IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

Volume 15 | Issue 1 | 2019

Special Issue – Privacy in the Digital Economy

[Cite as: 15 IJLT, < page no. > (2019)]

NATIONAL LAW SCHOOL OF INDIA UNIVERSITY
BANGALORE

Price: Rs. 900 (in 2 issues)

The mode of citation for this issue of The Indian Journal of Law and Technology, 2018 is as follows:

15 IJLT, <page no.> (2019)

Published by:

Student Bar Association
National Law School of India University
Nagarbhavi, Bangalore – 560072
Website: www.ijlt.in
Email: ijltedit@gmail.com or editorialboard@ijlt.in

Distributed exclusively by:

Eastern Book Company
34, Lalbagh, Lucknow - 226 001
U.P., India
Website: www.ebcwebstore.com Email: sales@ebc.co.in

IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

WWW.IJLT.IN

Volume 15 | Issue 1 | 2019

IJLT | THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

Volume 15 | Issue 1 | 2019

Contents

ARTICLES

SPECIAL REPORT

The *Aadhaar* Verdict and the Surveillance Challenge

Ananth Padmanabhan & Vasudha Singh***

Abstract *Conventional responses to privacy protection, such as the notice-and-consent framework, are inapposite to a datafied world where ubiquitous data collection is facilitated by a range of advanced technologies. Such traditional frameworks also commonly vest the State with more leeway than private companies to access personal data, which amplifies privacy harms in case of State use of data. Despite the ominous possibility of State surveillance, the Indian judiciary has thus far grappled with the right to privacy through a narrow lens focused on individual privacy risks rather than structural moves towards a surveillance society. This article explores a different viewpoint by studying the structural effects of the Aadhaar project on privacy, which drastically differ from the individual harms that Indian privacy jurisprudence is equipped to address. It first introduces the Supreme Court's engagement with the right to privacy through prior verdicts. It then explores the surveillance concerns raised by the petitioners in the Aadhaar verdict. This part examines the Supreme Court's response to these surveillance challenges and its failure to address structural inroads on privacy through architectural design choices that deliberately prescribe low baseline protection. Finally, the article contrasts this approach with the more holistic perspective on citizen-State interaction evident in Justice Chandrachud's minority view.*

* Dean, Daksha Fellowship.
** Advocate, Delhi High Court.

I. Introduction

Informational privacy[1] has become a fiercely contested dimension of privacy in recent times due to the trade-offs between ceding such privacy on the one hand and obtaining several benefits on the other. How societies handle data, be it in the realm of market behaviour or State functionalities, lies at the heart of this debate. Data can reshape market needs through personalised products and services, turn elections, and empower the State to track its citizens.[2] Standard responses such as the notice-and-consent framework do not appear robust enough to protect personal information in a datafied world.[3] This is often the case because the meaning and implications of elaborately worded privacy policies are lost on even legal experts. Additionally, this framework is ill-suited to the ubiquitous data gathering facilitated by more recent advances such as internet-of-things, radio frequency identification sensors, and commercial drones.[4]

These harms are amplified when it comes to the use of citizen data by the State. To begin with, the State is given more leeway than private companies when accessing data. A recent example of this differential treatment is seen in the case of Personal Data Protection Bill, 2019, which provides sweeping exemptions to the State for non-consensual data processing.[5] Most rely on larger public interest and State necessity as the foundational basis to do away with the consent requirement as well as, arguably, with other important privacy principles including data minimisation, purpose limitation, and

---

1 This branch of privacy, closely linked to the idea of 'informational self-determination', conceptualises individuals as rights-bearers with the authority to control their personal information and to determine how and when such information is communicated to others. *See*, Alan F Westin, *Privacy and Freedom* (1st edn, Athenum, 1967) 7. For a critique of this sole focus on control over personal information, *see*, Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087, 1109-1115. Solove argues for a bottom-up approach to define the concept, one that looks at specific technology-enabled intrusions and other encroachments into the personal information domain and the kind of harms that society desires to guard against. *See*, Solove (n 1) 1154-55.

2 Gautam Bhatia, 'Gautam Bhatia Dreams of Genuine Data Protection in India' (*LiveMint*, 11 August 2018) <https://www.livemint.com/Leisure/RuHOGczbrpt33v5ijP987M/Gautam-Bhatia-dreams-of-genuine-data-protection-in-India.html> accessed 19 June 2019.

3 Rishab Bailey and others, 'Disclosures in Privacy Policies: Does 'Notice and Consent' Work?' (2008) National Institute of Public Finance and Policy Research Paper No. 246 <https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf> accessed 19 June 2019; Aleecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 I/S: A Journal of Law and Policy for the Information Society 543, 565.

4 Ananth Padmanabhan and Anirudh Rastogi, 'Big Data' in Devesh Kapur and Madhav Khosla (eds), *Regulation in India: Design, Capacity, Performance* (Oxford: Hart Publishing 2019).

5 Personal Data Protection Bill 2019, cls 35 and 91(2).

transparency.[6] Unfortunately, the risks arising from such dilution of meaningful safeguards are more pronounced when the might of the State is drawn into the equation.

David Lyon discusses the possibility of 'surveillance societies' that are orchestrated through a combination of technologies that monitor or intercept personal information. Lyon points out that we usually understand State surveillance as a monolithic, centralised panopticon. However, in reality, surveillance societies assemble several "*audio-visual protocols*" that converge "*discrete systems of surveillance*."[7] Moreover, in extreme cases, citizens and private actors are even enlisted by the State to collaborate in such mass surveillance.[8] The role of technology is central to the ominous possibilities that this new form of State power entails, as noted by Justice Sanjay Kishan Kaul in *K.S. Puttaswamy* v. *Union of India* (***'Puttaswamy'***).[9] Here, the learned judge rightly observed that "*surveillance is not new, but technology has permitted surveillance in ways that are unimaginable*."[10]

Protective legal frameworks have been a standard response to the interception of private communications by the State, though the nature of the response varies across jurisdictions.[11] Most such responses entail some form of judicial involvement in the interception of private communications by law enforcement authorities. For example, under Australian law, a warrant from a judge or a nominated member of the Administrative Appeals Tribunal is required to intercept private communications. But the procedure does not envisage any form of contestation over the grant of such warrant, perhaps

---

6 Madhav Khosla and Ananth Padmanabhan, 'Draft Data Protection Bill Pays Little Attention to the Dangers of State Power' (*ThePrint*, 30 July 2018) <https://theprint.in/opinion/draft-data-protection-bill-pays-little-attention-to-the-dangers-of-state-power/90511/> accessed 19 June 2019.

7 David Lyon, 'Surveillance, Power and Everyday Life' in P Kalantzis-Cope and K Gherab-Martín (eds), *Emerging Digital Spaces in Contemporary Society* (Palgrave Macmillan 2010) 107, 108-09.

8 Alexandra Ma, 'China is Building a Vast Civilian Surveillance Network – Here are 10 Ways it could be Feeding its Creepy 'Social Credit System'' (*Business Insider*, 29 April 2018) <https://www.businessinsider.in/China-is-building-a-vast-civilian-surveillance-network-here-are-10-ways-it-could-be-feeding-its-creepy-social-credit-system/articleshow/63959324.cms> accessed 19 June 2019. This is not a new phenomenon, as borne out by a historical examination of exercise of State power in several diverse situations in the past, and resort to legislative and executive action to pry into the lives of citizens. *See*, Westin (n 1).

9 *KS Puttaswamy v Union of India* (2017) 10 SCC 1 *(Puttaswamy)*.

10 ibid 618.

11 *See*, '2017 Surveillance Law Comparison Global' (*Baker Mckenzie*, 2017) <https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/2017_surveillance_law.pdf?la=en> accessed 19 June 2019.

with the intent of preserving the efficacy of this exercise of state power.[12] But these safeguards do not apply when monitoring metadata,[13] which is highly useful to combat crimes but equally powerful as a surveillance instrument. Contrast this framework with Germany, which permits surveillance by specific agencies like the Federal Intelligence Service without a prior judicial warrant sanctioning the same.[14] They must follow certain procedures while undertaking surveillance and intercepting communication but barring that, the collected information can be used to share intercepted intelligence for criminal prosecutions.

'Surveillance societies' defy even these standard safeguards because of mass surveillance programs facilitated through advanced snooping technologies. The Snowden leaks can be considered a watershed moment in our understanding of modern surveillance because it brought to public glare the enormous privacy intrusions that such programs could achieve through strikingly opaque means. Even when judicial orders are legally mandated before undertaking these exercises, courts have often granted such orders without any meaningful scrutiny, raising doubts over the efficacy of constitutional and legal safeguards against surveillance in the digital age. In India, surveillance is carried out through various methods, including telephone-tappingas authorised under the Indian Telegraph Act, 1885 and the amended Telegraph Rules, 1951. This legal framework allows interception of a "*class of messages*" sent to or from a "*class of persons*", thereby technically permitting mass surveillance so long as the other safeguards are satisfied.[15]

But most mass surveillance programs came about in the aftermath of the 26/11 Mumbai terror attacks that shook the nation. Prominent among these are the Central Monitoring System ('**CMS**') that acts as an automated centralised portal granting direct access to all communication data (including voice calls over mobile and landline, internet messaging, and metadata

---

[12] Surveillance Devices Act 2004, sub-ss 4 and 16.

[13] Broadly defined as "*data about data*", metadata includes basic information about any piece of data such as the name of the author, dates of creation and modification of files, file-size, search engine metatags, call records and tower location details. *See*, Bryce Clayton Newell and Joseph T Tennis, 'Me, My Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs' (iConference, Berlin, March 2014) <https://www.ideals.illinois.edu/bitstream/handle/2142/47299/109_ready.pdf> accessed 19 June 2019.

[14] *See*, the Act on Restrictions on the Secrecy of Mail, Post and Telecommunications (G-10 Act).

[15] Indian Telegraph Rules 1951, R 419 A(4). Prior judicial approval has not been a feature in this framework, which relies on bureaucratic approval mostly from senior home ministry officials based on exigencies of the situation, when directing telecom service providers to intercept communications over their network.

on calls and internet usage) to security agencies of the State,[16] the National Intelligence Grid ('**NATGRID**'), the Crime and Criminal Tracking Network & Systems, and the Network Traffic Analysis System.[17] These programs have relied, for their legal basis, on amendments carried out in 2008 to the Information Technology Act, 2000, and IT rules that operationalised these newly conferred powers. But this framework mostly mimics the protective regime against unauthorised telephone-tapping,[18] which is realistically equipped, at best, to address individual privacy risks rather than regressive structural moves towards a surveillance society. As explained below, structural inroads on privacy involve a consciously low protection baseline through architectural design choices, and differ from case-by-case exemptions for State surveillance. The judicial engagement with surveillance in India, however, has mostly been within the latter context, one where the harms are again more immediately perceived than constituting themselves in the long run.

The recent verdict of the Supreme Court of India ('**Supreme Court**') in *K.S. Puttaswamy* v. *Union of India* ('***Aadhaar* verdict**') and its consideration of the plea that the Aadhaar project could enable mass surveillance by the State, must be appreciated with this background in mind.[19] The Aadhaar database, built up through practically non-consensual data gathering, envisages seeding Aadhaar numbers in multiple databases and thereby eases on-demand access to biometric and other sensitive information by State authorities. The project also entails authentication of subjects at various end-points to avail services and benefits, with records of such authentication events potentially offering a comprehensive account of a subject's interaction with the State and

[16] For a comprehensive discussion of this project, *see,* Addison Litton, 'The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression' (2015) 14 Washington University Global Studies Law Review 799.

[17] For an overview of these mass surveillance programs, *see*, Udbhav Tiwari, 'The Design and Technology behind India's Surveillance Programs' (*The Centre for Internet and Society*, 20 January 2017) <https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes> accessed 19 June 2019.

[18] *See*, Rishab Bailey et al, 'Use of Personal Data by Intelligence and Law Enforcement Agencies' (*The National Institute of Public Finance and Policy*, 1 August 2018) <http://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf> accessed 19 June 2019. Bailey identifies three important aspects in which interception powers under the IT Act and Rules exceed similar powers in the Telegraph Act; Madhav Khosla and Ananth Padmanabhan, 'Both BJP and Congress are Complicit in Expanding State Surveillance without Legal Basis' (*ThePrint*, 24 December 2018) <https://theprint.in/opinion/both-bjp-and-congress-are-complicit-in-expanding-state-surveillance-without-legal-basis/168084/> accessed 19 June 2019.

[19] See, *KS Puttaswamy v Union of India* (2019) 1 SCC 1 (*Aadhaar verdict*).

even private entities.[20] These fears motivated the petitioners' constitutional challenge to the Aadhaar project as being, *inter alia*, violative of Article 21 because it presents the ominous possibility of a surveillance State.

Part II explores the nature of individual privacy risks that the Supreme Court has come to address through prior verdicts. Part III then proceeds to detail the specific surveillance concerns raised by the Aadhaar project and highlighted by the petitioners in this case. The Aadhaar challenge raised concerns that drastically differed from the individual harms that Indian privacy jurisprudence was equipped to address, as demonstrated here. This part then examines how the Supreme Court's majority opinion dealt with the surveillance challenge, and the gaps resulting from its lack of prior experience in dealing with mass surveillance. The final part contrasts this with the more holistic and structural perspective on citizen-State interaction evident in Justice Chandrachud's minority view. It concludes that a more robust review is required in cases of mass surveillance. Not only are the harms and consequences more long-term in nature, these cases usually involve technology design that pegs the privacy baseline at undesirably low levels.

II. Surveillance and the Supreme Court

The Supreme Court's understanding of privacy and surveillance has evolved through the years. But even in this progressive journey, judicial verdicts have primarily dealt with the right to privacy within the context of existing individual harms rather than architectural interventions and mass surveillance technologies that structurally altered the power balance between the repositories and recipients of State power. In *M.P. Sharma* v. *Satish Chandra*,[21] acts of search and seizure, carried out in pursuance of powers vested with investigative authorities under the Code of Criminal Procedure, were challenged on the basis that they violated the fundamental right to acquire, hold and dispose of property[22] and the fundamental right against self-incrimination.[23] When dealing with the right to privacy within this narrow setting, the court held that this right could not be imported to Indian jurisprudence

---

[20] For a comprehensive critique, *see*, Ananth Padmanabhan, 'The Three Sins of Aadhaar' (*Open Magazine*, 4 August 2017) <www.openthemagazine.com/article/essay/the-three-sins-of-aadhaar> accessed 19 June 2019.

[21] *MP Sharma v Satish Chandra* AIR 1954 SC 300.

[22] Constitution of India 1950, art 19(1)(*f*) — before it was deleted from the bouquet of fundamental rights vide the Constitution (44th Amendment) Act, 1978.

[23] Constitution of India 1950, art 20(3).

through a process of strained construction.[24] Though this was not a case of surveillance, its adjudicatory structure is no different from many others that followed, where the court determined the status or scope of the right to privacy under the Indian Constitution through a balancing of immediate individual harms against specific State goals rather than through an evaluation of systemic surveillance projects with long-term consequences.

This is evident from the very next case in this line of precedents dealing with the right to privacy. In *Kharak Singh* v. *State of U.P.*,[25] the Supreme Court dealt with the constitutionality of police surveillance that included 'domiciliary visits' from local police officials to the petitioner's house at night authorised *vide* Regulation 236(b), Chapter XX of the Uttar Pradesh Police Regulations. A six-judge bench of the Supreme Court invalidated this provision as violating Articles 19 and 21. However, the remaining provisions authorising 'surveillance' such as secret picketing of the residence of the "*history sheeter*" and maintaining a report of his habits, associations and movements, were upheld because "*the right of privacy is not a guaranteed right under our Constitution, and therefore the attempt to ascertain the movements of an individual is merely a manner in which privacy is invaded and is not an infringement of a fundamental right*." While the Supreme Court has now wholly discarded this view on the status of the right to privacy as borne out by the categorical and unanimous view to the contrary in *Puttaswamy*, the point we make here still holds. As Gautam Bhatia has pointed out, "*the State argued - and the Court endorsed - the basic idea that what makes surveillance reasonable … is the very fact that it is … targeted at individuals who are specifically suspected of being a threat to society because of a history of criminality*."[26] Thus, the adjudicatory structure was one calling into question the balance between immediate individual harms and state necessity.

Similarly, in *Malak Singh* v. *State of P&H*,[27] inclusion of the petitioners' names into a surveillance order was challenged because it was solely motivated by extraneous reasons rather than the prevention of crime as required under law. The petitioners relied on the right to privacy to contend that they ought to have been heard prior to their inclusion in this order. The Supreme Court disagreed, despite locating the right to privacy within the concept of individual dignity embedded in Article 21. It framed the dispute as involv-

---

[24] Gautam Bhatia, 'State Surveillance and the Right to Privacy in India : A Constitutional Biography' (2014) 26 National Law School of India Review 127, 128.

[25] *Kharak Singh v State of UP* AIR 1963 SC 1295.

[26] Bhatia (n 24) 129.

[27] *Malak Singh v State of P&H* (1981) 1 SCC 420 *(Malak Singh)*.

ing the extent to which the citizen's right to be let alone could be "*invaded by the duty of the Police to prevent crime*."[28] The court then proceeded to reason that a close watch over suspects was required to effectively combat organised crime.[29] Because effective surveillance had to be discrete, the court struck the balance in favour of the larger social goal of policing and disentitled the petitioners to a right of prior hearing.[30] The court also underscored provisions in the Police Rules that safeguarded individuals against unbridled exercise of surveillance power, and the option of judicial recourse against specific instances of such exercise.[31] Structural changes to the surveillance architecture were neither petitioned for nor *suo moto* considered in any of these cases.

The only case in this line of precedent that initially comes across as one where the Court addressed a structural problem is the verdict in *People's Union for Civil Liberties* v. *Union of India*[32] ('***PUCL***'). Here, a public interest litigation was initiated against the abuse of political power perpetrated through unchecked and illegal telephone tapping. The constitutional validity of Section 5(2) of the Indian Telegraph Act, 1885 was challenged. The Supreme Court declined to go into the constitutional validity of this provision, instead proceeding to discuss the executive's role in adhering to statutory pre-requisites such as the pre-conditions of 'occurrence of any public emergency' or situations that involved 'the interest of public safety' for the issuance of an interception order. Thus, on closer reading, this case similarly involved the balancing of unjustifiable immediate harms against justifiable state goals. The court's tackling of the matter through detailed directives did address some structural defects but was mostly a check on arbitrariness in the issuance of telephone tapping orders in specific cases. These directives demanded specificity of State action, be it the communications, persons or addresses intercepted, the exhausting of alternate and less intrusive ways to acquire the information before activating interception, and limiting intercepted material to the necessary minimum.

However, the existing technology at that point did not permit mass surveillance in the way that CMS and NATGRID now enable, thereby limiting judicial imagination of threats and consequences that went beyond immediate harms to the individual. Accordingly, these directives are inconsistent with mass surveillance and the kind of safeguards required to protect

---

[28] ibid 421.
[29] *Malak Singh* (n 27) 424.
[30] *Malak Singh* (n 27) 425-26.
[31] *Malak Singh* (n 27) 426.
[32] *People's Union for Civil Liberties v Union of India* (1997) 1 SCC 301.

innocent citizens in such cases.[33] Mass surveillance, especially the kind citizens are subject to in the present day and age, usually relies on technology design that keeps the baseline of privacy protection low, rather than on State action that makes use of exceptions to access data architecture or communication modes that are otherwise private. To illustrate, a directive that end-to-end encryption must not be deployed, or that the encryption key length must be kept low, is a vehicle for mass surveillance because it keeps privacy baseline low as a technological feature. The technology specifications become a part of any new product or service that is on offer because it is integrated as a design feature. Thus, such directives and measures have surveillance-by-design as their driving agenda, unlike telephonic communications where the inventor neither applied his mind to questions of surveillance or the best form of design that would enable such surveillance, nor was he compelled to do so by the State. By default, the design itself favoured and valued privacy and anonymity, with limited exceptions emerging with time.[34]

In similar fashion, requesting decryption assistance in individual instances – again a power that can be abused – would remain an exception to a system where the privacy baseline is still high. These examples are akin to telephone tapping because they do not address the core design principles in the technology itself, thereby conceding at a fundamental level that the design is in favour of privacy and anonymity and then devising exceptions to the workings of this design in suitable cases. In any case, they do not qualify as surveillance-by-design because the possibility of surveillance is not integrated as a design feature in the technology at hand. The *PUCL* directives were geared only to tackle the abuse of such exceptions, and not to evaluate technology design *vis-à-vis* the optimal privacy baseline for citizens and communities.[35] The court did not provide any guidance on assessing the design principles for any new technology that enables communications between individuals, for the straightforward reason that that was not the issue at hand.

Finally, in the most important verdict on the right to privacy in recent times, *Puttaswamy*, a nine-judge bench of the Supreme Court held privacy to be an expression of human dignity and therefore a vital part of fundamental rights guaranteed under the Indian constitution. This verdict is also important because of its focus on informational privacy, a dimension that

---

[33] *See*, Bhatia (n 24) 144.

[34] Edgar A Whitley et al, 'From Surveillance-by-Design to Privacy-by-Design: Evolving Identity Policy in the United Kingdom' in Kees Boersma et al (eds), *Histories of State Surveillance in Europe and Beyond* (Routledge 2014).

[35] For a comprehensive discussion on how many of the mass surveillance tools compromise the general level of privacy in electronic communications, *see*, Bailey (n 18) 16-17.

had not come to the forefront in a major way in earlier Supreme Court cases.[36] The court, for instance, recognised how people are increasingly spending more time on the internet and as a consequence, their digital footprints can "*reveal patterns, trends and associations, especially relating to human behaviour and interactions.*"[37] The court observed that this information can be used as a tool to exercise control over people and "*have a stultifying effect on the expression of dissent and difference of opinion, which no democracy can afford.*"[38]

But here too, the court's engagement with the right has been mostly focused on the balance between immediate individual harms and larger social goals. This is despite the broader context of structural surveillance under the Aadhaar program, which thus provided the Court ample opportunity to examine both the individual and structural aspects of privacy. Even its articulation of the limitations on privacy through proportionality assessments bears the strong imprint of this balancing exercise between individual rights and social goals. Justice Chandrachud's opinion articulated exceptions benefiting big data analytics for better governance, revenue utilisation, law enforcement and other social benefits.[39] However, it failed to probe deeper into the structural ramifications of such analytics in terms of the incentives they create, the manageability of such projects, and the essential line-drawing between responsible and unsafe innovation. For instance, Justice Kaul recognises that we are no longer contending with new forms of data alone, but also new methods to analyse and use such data with more effective algorithms and enhanced computational powers.[40] His opinion then registers reality as one where, in suitable cases, the collection and processing of big data would be legitimate and proportionate even when invasive of individual privacy, due to the ability of big data models to promote public interest.[41] At the same time, however, these models could very easily be made to work together to facilitate an undesirable 'surveillance society' in the future. The court failed to articulate any suitable legal safeguards to protect against these slightly more futuristic, yet quite real, harms. This in turn illustrates

---

[36] *See*, *R Rajagopal v State of TN* (1994) 6 SCC 632; *X v Hospital Z* (1998) 8 SCC 296; *Sharda v Dharmpal* (2003) 4 SCC 493. These cases, though dealing with privacy of personal information, were not constitutional cases in a real sense. The Supreme Court had erroneously constitutionalised these cases, which involved privacy intrusions by private individuals rather than the State. A possible exception is the verdict in *District Registrar & Collector v Canara Bank* (2005) 1 SCC 496, where the Stamp Act authorised the District Collector to access the confidential bank records of private individuals.

[37] *Puttaswamy* (n 9) 619.

[38] *Puttaswamy* (n 9) 620.

[39] *Puttaswamy* (n 9) 505.

[40] *Puttaswamy* (n 9) 619-20.

[41] *Puttaswamy* (n 9) 620.

how 'surveillance societies' often shape themselves in slow and discreet ways without raising immediate or obvious constitutional concerns.

In fact, a notable instance where the Supreme Court responded to some of these more long-term consequences was the verdict in *Shreya Singhal* v. *Union of India*,[42] a case dealing with free speech and not directly with the right to privacy. Here, the police had invoked section 66-A of the Information Technology Act, 2000 against some Facebook users for expressing their displeasure at a city-wide shutdown in Mumbai in the wake of Shiv Sena supremo Bal Thackeray's death. Striking down this provision as being unconstitutional for its chilling effects on the freedom of speech and expression, the court opened doors to the possibility of evaluating structural power imbalances brought on by vaguely worded criminal offences. Chilling effects can occur when the citizen apprehends that the State is watching her activities. While immediate criminal consequences may not necessarily follow, the mere existence of vague and overreaching criminal liabilities could restrain individuals from expressing themselves due to the fear of attracting such consequences. As the court reasoned,

> Section 66-A is cast so widely that virtually any opinion on any subject would be covered by it, as any serious opinion dissenting with the mores of the day would be caught within its net. Such is the reach of the section and if it is to withstand the test of constitutionality, the chilling effect on free speech would be total.[43]

The court did not even consider reading down the provision, instead striking it down in its entirety.

While we do not argue here that the 'chilling effects' doctrine is a perfect mechanism to scope out the limits of state authority when undertaking mass surveillance, the verdict in *Shreya Singhal* demonstrated the need to evaluate possible long-term consequences of State action. To do so, the judiciary must necessarily go beyond immediate cases of rights infractions to a critical scrutiny of the architecture put in place, be it legal or technological. This is not a point exclusively limited to rights reviews. Even cases involving the dilution of judicial independence through the formation of tribunals, for instance, demand similar outlook. As do instances of colourable exercise of power such as law-making on a regular basis through ordinances. In all these situations, the State's usual defence that the scope for abuse is no ground to strike down an executive or legislative action, stands weakened. These are

---

[42] *Shreya Singhal v Union of India* (2015) 5 SCC 1 *(Shreya Singhal)*.
[43] *Shreya Singhal* (n 42) 167.

all architectural questions, ones that have a bearing on even the basic structure of the Constitution, but not in the same way that surveillance orders against history sheeters or individual instances of telephone tapping impinge on individual rights. But as the Aadhaar verdict reveals, courts are both less inclined and less equipped to make the evaluations that such architectural changes necessitate.

III. Aadhaar's Surveillance Risks and the Judicial Resolution

The petitioners in the *Aadhaar* challenge raised several concerns regarding the effect of this project on fundamental rights and the future of democracy. The collected information sufficiently indicated, in their view, the religion, class, social status, income, education, medical history, and other sensitive personal information relating to an individual and a further analysis of such data could even throw light on her habits, preferences and behaviour. Thus, it completely altered the balance of power between the State and its citizens.[44] The need for an Aadhaar database was justified by the State as primarily an exercise to ensure deliveries of subsidies and benefits to deserving beneficiaries through a de-duplication of fraudulent identities and a reliable process of identity verification.[45] The Aadhaar project worked through the gathering of vital pieces of information – biometric information including fingerprints, iris scans; demographic information including photograph, name, age, address, sex, mobile number, e-mail address, family members and their Aadhaar numbers; transaction metadata such as the frequency and purpose of authentication, the frequency of failure of authentication, and the device ID of the biometric capture device used for authentication; information to which the Aadhaar number was linked or seeded including bank accounts, income tax returns, scholarships, licences, voter card, etc.– though not all such information resided in a single database. The Unique Identification Authority of India ('**UIDAI**') submitted before the court that the project was built on the principles of minimal data, optimal ignorance, unidirectional linkage, and federated databases.[46] In simpler terms, the technology design was such that no central authority including the UIDAI had access to all the purposes for which the Aadhaar number was used. Thus, mere access to Aadhaar numbers did not provide knowledge on how citizens

---

[44] *Aadhaar verdict* (n 19) 437-38.
[45] *Aadhaar verdict* (n 19) 369-70.
[46] *Aadhaar verdict* (n 19) 227.

availed of other systems in which these numbers were seeded – tax, banking, pension, employment, to name a few.

Even assuming the UIDAI's contentions to be true, the challenge here was as much to the Aadhaar project as the Aadhaar Act and regulations thereunder.[47] Viewed from this lens, the wider project had spawned the creation of State Resident Data Hubs ('**SRDHs**') by various state governments, presenting the perfect tool to conduct mass surveillance. These data hubs, information pertaining to which was and still is mired in opacity, envisioned linking Aadhaar numbers with almost every state-sponsored scheme or payment from the state exchequer. They helped offer a 360-degree view of state residents, as publicly claimed by the State governments – Haryana, Andhra Pradesh, Tamil Nadu, Madhya Pradesh and others – that instituted such SRDHs.[48] While the SRDHs utilised Aadhaar information as their foundation, they failed to extend data protection and privacy safeguards envisaged under the Aadhaar act, to their operation.[49] Thus, even a basic enquiry into the procedures and systems in place with respect to the SRDHs made it evident that the aggregation of data from different silos, profiling, and consequential surveillance of residents was no longer in the realm of conjecture. Unique Aadhaar numbers made the findability of information much more convenient by serving as a unifying link for information held across various government departments and databases.[50]

To articulate this threat in legal terms, the petitioners relied on important decisions of the European Court of Justice ('**ECJ**') that appreciated state-sponsored surveillance systems as a separate class when coming up for judicial review. In most such cases, the applicant could not establish special harm or even conclusively demonstrate being subjected to any surveillance. Yet, in *Kennedy* v. *The United Kingdom*,[51] the ECJ held that the general

---

[47] *See*, the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act 2016.

[48] Anand Venkatanarayanan, 'The 360 Degree Database' (*Medium*, 5 December 2017) <https://medium.com/@venkatanarayanan.anand/the-360-degree-database-17a0f91e6a33> accessed 19 June 2019.

[49] All these databases are governed in the same manner as any welfare measure i.e. strictly through executive orders and resolutions, without appreciating the privacy risks that place them on a separate footing. *See*, Aman Sethi, 'Why State Data Hubs Pose a Risk to Aadhaar Security' (*Hindustan Times*, 13 March 2018) <https://www.hindustantimes.com/india-news/why-state-data-hubs-pose-a-risk-to-aadhaar-security/story-Klyl3yT5MkFk6Szg2yGg9N.html> accessed 19 June 2019.

[50] Annexure A, Submission of Ms Meenakshi Arora, Senior Advocate on behalf of the petitioners, *VickramCrishna v UIDAI* Transfer Case (Civil) No. 152 of 2013 decided on 26-9-2018 (SC) and *SG Vombatkere (SC) v Union of India* WP(C) No. 797 of 2016 decided on 26-9-2018.

[51] *Kennedy v United Kingdom* 2010 ECHR 682.

approach that denied individuals the right to challenge a law in the abstract based on its potential for abuse would not apply where secret surveillance took place. In such situations, courts had to apply a stricter standard, one that evaluated the availability of domestic remedies to effectively challenge acts of surveillance. The ECJ concluded so because in its view, "*the menace of surveillance can be claimed in itself to restrict free communication…, there by constituting … direct interference with the right guaranteed by Article 8*."[52]

Similarly, regarding substantive limits on surveillance programs, the ECJ provided adequate guidance, a point relied on by the petitioners in the *Aadhaar* challenge. Minimum legal safeguards were spelt out in *Roman Zakharov* v. *Russia*,[53] a case that challenged Russia's system of surveillance of mobile communications. These are:

> the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed.[54]

Evaluating Russian surveillance law against these benchmarks, the ECJ found that technical details pertaining to surveillance were not generally accessible to the public, despite impacting their right to privacy. The law suffered from overreach, permitting interception in respect of "*a very wide range of criminal offences, including … pickpocketing*", as well as "*of a person who may have information about an offence or … relevant to the criminal case*."[55] It also legitimised withholding necessary information from review proceedings meant to assess the legality of contested surveillance orders, thereby stripping such review of its efficacy.

Russian telecom service providers also had to mandatorily install equipment facilitating direct law-enforcement access to all mobile telephone

---

[52] *Roman Zakharov v Russia* 2015 ECHR 1065. In this case, the European Court of Justice found Russia's surveillance framework as falling short of adequate safeguards and therefore violative of art 8 of the European Convention on Human Rights (ECHR). This provision in the ECHR provided every individual the right to respect for one's "*private and family life, his home and his correspondence*".

[53] ibid.

[54] *Zakharov* (n 52).

[55] *Zakharov* (n 52).

communications of all users.[56] The ECJ reasoned that this generality of surveillance power made it even more important for the domestic law to provide a robust mechanism of review and supervision of its exercise. In its absence, the Russian domestic law would violate Article 8. Employing this heightened yardstick, the ECJ found that the system of prosecutorial supervision envisioned in Russia fell short of ECHR requirements as prosecutors were not independent enough in their functioning from executive control. The ECJ also found to be problematic the fact that the direct access system did not maintain any logs or records of interception, thereby rendering it difficult to evaluate whether interceptions were indiscriminately undertaken to advance legally untenable purposes. This decision was relied on along with others from the ECJ,[57] the European Court of Human Rights,[58] and the German Federal Constitutional Court,[59] all of which considered mass surveillance programs to be overly broad and capable of causing fear in the minds of citizens that they were under constant monitoring by the State. In fact, all these verdicts appear to consider the certainty of information under State control as being better than State authorities possibly holding voluminous information about an individual, and without one being able to ascertain this fact for sure.

These cases focused considerably on the structural and architectural aspects of the respective surveillance programs under challenge in each of them. But the Supreme Court's response in the *Aadhaar* verdict to the contentions built on these decisions was qualitatively different from the very essence of the judicial reasoning employed in them. The court's response can, at best, be characterised a narrow balancing exercise between immediate individual harms and social goals. During this exercise, the majority held that authentication records and 'authentication transaction data' can only be retained for a six-month period and must be deleted thereafter unless there is a judicial order authorising prolonged data retention.[60] It also limited the metadata that may be gathered to "*process metadata*" that helps identify when and where authentication may have taken place for purposes of subsequent dispute resolution and not any other categories of metadata that indicates the purpose served by such authentication and other transaction

---

[56] Ministry of Communications Order No. 70, issued on 20 April 1999.

[57] *Maximillian Schrems v Data Protection Commr* 2016 QB 527; *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* 2015 QB 127: (2014) 3 WLR 1607; *Tele 2 Sverige AB v Post-ochtelestyrelsen* 2017 QB 771: (2017) 2 WLR 1289.

[58] *Szabó and Vissy v Hungary* 2016 ECHR 579.

[59] *Proceedings on the Constitutional Complaints Against §§ 113a and 113b of the Telecommunications Act* (2010) judgment in 1 BvR 256/08 & Ors (BVerfG).

[60] *Aadhaar verdict* (n 19) 351.

details.[61] While not a point directly relating to surveillance, the majority ordered that the power to direct disclosure of Aadhaar data on grounds of national security be vested in a higher-ranking official than the joint secretary level specified in Section 33(2) of the Act.[62] In other situations of data disclosure, the court vested the data subject with a right to be heard by the district court sanctioning such disclosure.[63] It also extended the right to data subjects to directly raise grievances against data leakages and other offences, rather than rely on UIDAI and its authorised officers as stipulated in Section 47.[64]

While these may be considered quick fixes for any immediate harms that the court saw as arising from the workings of Aadhaar, they hardly address the long-term consequences of SRDHs and other potential applications of Aadhaar for big data analytics and profiling. In fact, the majority chose to not reference SRDHs despite the petitioners pointing out that when combined with multiple databases, the view that these data hubs offer about a citizen could be extremely potent. The majority observed that the averment of a "*surveillance state created by the Aadhaar project is not well founded, and in any case, taken care of by the diffluence exercise carried out with the striking down of certain offending provisions in their present form*."[65] There are significant strands in the majority's reasoning when dealing with surveillance that endorse the State's position based on the UIDAI's submissions that it has strengthened the security systems in place to avoid data leaks. This is particularly disconcerting because secure systems simultaneously double up as extremely sophisticated surveillance machineries. Instead, the majority would have done well to follow the various European court decisions that consistently opposed state-of-the-art mass surveillance architectures because their long-term consequences, while not fully ascertainable, made them even more worrisome and intrusive. But to do so, the majority should have appreciated, at both conceptual and factual levels, the distinc-

---

[61] *Aadhaar verdict* (n 19) 350.

[62] *Aadhaar verdict* (n 19) 423.

[63] *Aadhaar verdict* (n 19) 420-21.

[64] *Aadhaar verdict* (n 19) 424. It needs special mention here that many of these 'directives' are expressed as options and preferences for the State rather than mandatory orders. For instance, the majority *hopes* that "*if considered fit*," s 47 would be amended. Similarly, it concludes that a judicial officer may *preferably* function alongside a high-ranking bureaucrat to direct disclosure of Aadhaar data under s 33(2). As seen with the recent Aadhaar (Amendment) Ordinance 2019, the State has conveniently handpicked some of these options while ignoring the rest. *See*, Madhav Khosla and Ananth Padmanabhan, 'What the Aadhaar Amendment Bill Fails to Address' (*ThePrint*, 7 January 2019) <https://theprint.in/opinion/what-the-aadhaar-amendment-bill-fails-to-address/173958/> accessed 19 June 2019.

[65] *Aadhaar verdict* (n 19) 359.

tion between surveillance exceptions and surveillance-by-design. *PUCL* and other previous instances concerned the former, but the *Aadhaar* challenge demanded understanding the latter. The majority failed to draw this distinction, thereby applying a reasoning frame that was flawed to begin with.

IV. In Conclusion: The Need for More Robust Review

Behemoth adventures like the Aadhaar project spring up from a strong idea of technology solutionism. To its proponents and supporters, many of whom are senior bureaucrats and prominent business leaders, the biometric solution can be waved seamlessly like a magic wand to cure the State of all its ills. To some extent, the biometric solution may work in weeding out duplicate identities and fraudulent practices. However, the metrics put forth – the scale and pace of enrolment, the low cost per identity, the savings to the public exchequer – all pale when juxtaposed against the normative problems highlighted here. As experiences with the on-the-ground rollout of the Aadhaar project reveal, there have been leaks galore and misuse of Aadhaar data by both private and public entities within a limited period.[66] While no technical solution is ever fool-proof, any identity linked with such vast and varied facets of an individual's life are bound to elevate the cause for consternation. In a datafied world, vesting a significant number of personal data points within State custody is a recipe for abuse and potential profiling disasters. It also lowers, in a structural sense, the baseline of privacy protection that citizens must necessarily have against the State.[67]

This aspect is reflected in Justice Chandrachud's dissent in the *Aadhaar* case. Unlike the majority, he accounts for the structural reality that post-Aadhaar interactions between citizens and the State shall never be the same as in the pre-Aadhaar era. In a fine example of inductive reasoning, the dissent begins this exploration from what lies at the core of this project

---

[66] Srinivas Kodali, 'Forensic Probe Into Aadhaar Data Controversy in Andhra Pradesh Raises Troubling Questions' (*TheWire*, 15 April 2019) <https://thewire.in/government/andhra-pradesh-stolen-aadhaar-data> accessed 19 June 2019; Apoorva Mandhani, 'Prof. Shamnad Basheer Moves Delhi HC Against Aadhaar Data Leak; Demands Exemplary Damages' (*LiveLaw*, 18 May 2018) <https://www.livelaw.in/prof-shamnad-basheer-moves-delhi-hc-against-aadhaar-data-leak-demands-exemplary-damages/> accessed 19 June 2019.

[67] Whitley (n 34). Here, the authors argue that modern identity policy involves a complex socio-technical system that relies intensely upon technology while also altering the relationship between the individual and the State. Thus, choices such as biometric identities, use of a single identification number across government and the private sector, and an 'audit trail' that records details of every instance when an identity is verified against information stored on the register, can qualify as surveillance-by-design because of the extensive collection and use of personal information being proposed, as well as the expansive purposes for which the system would be used.

– biometric technology.[68] He notes that the deployment of this technology eradicates features such as anonymity and "*privacy by obscurity*" which, though not always desirable, bring some balance to the power dynamic between State and citizens.[69] He also rightly observes that this technology architecture, once compromised, cannot be secured again precisely because of the unique biometric features that make the project valuable in the first place.[70] This part of the discussion, and the impact of biometric solutions on privacy and exclusion as discussed in the dissent, are outside the scope of this article. Yet, they reveal a judicial approach that assesses the technology design in a deeper way than the majority did.

Proceeding further, the dissent assesses the overall technology solution to be legally disproportionate because "*an entire population cannot be presumed to be siphoning huge sums of money in welfare schemes or viewed through the lens of criminality, and therefore, considered as having a diminished expectation of privacy.*"[71] Justice Chandrachud examines the authentication architecture from the time biometric information is captured at point-of-sale devices, to conclude that extensive authentication transaction data vests with the UIDAI. This fact, coupled with the lack of transparency and inadequate grievance redressal mechanisms, "*exacerbate the overall risk associated with data retention*," including potential surveillance activities using the Aadhaar database.[72] Third parties can access biometric authentication information, link it with other information, and erode the personal control that an individual has over her information – a systemic harm arising from big data applications.[73] He also underscores the profiling risks in making Aadhaar numbers the "*central unifying feature that connects the cell phone with geo-location data, one's presence and movement with a bank account and income tax returns, food and lifestyle consumption with medical records*," thereby starting a "*causal link between information which was usually unconnected and was considered trivial.*"[74] This opinion, which conclusively shuts down the project, has been recently followed by

---

[68] *Aadhaar verdict* (n 19) 763.
[69] *Aadhaar verdict* (n 19) 767.
[70] *Aadhaar verdict* (n 19) 768-69.
[71] *Aadhaar verdict* (n 19) 835.
[72] *Aadhaar verdict* (n 19) 936.
[73] *Aadhaar verdict* (n 19) 845. Justice Chandrachud factually substantiates this point by exploring the contractual arrangement between UIDAI and the private vendor that licensed the biometric storage solutions software, and concluding that the vendor was given unfettered access to the Aadhaar database.
[74] *Aadhaar verdict* (n 19) 854, 856. Subsequently, the dissent notes: "*When Aadhaar is seeded into every database, it becomes a bridge across discreet data silos, which allows anyone with access to this information to reconstruct a profile of an individual's life. It must be noted while s. 2(k) of the Aadhaar Act excludes storage of individual information related*

the Jamaican Supreme Court in *Julian Robinson* v. *Attorney General of Jamaica*[75] to invalidate the national identification and registration statute.

To conclude, the majority verdict in *Aadhaar* ought to have developed a test along the lines of the 'chilling effects doctrine' to evaluate the long-term harms of the project rather than confine its enquiry to the immediate harms and solutions associated with such architectures. It should also have developed sounder judicial models for assessing technological design and structural features against the optimal privacy baseline in a democratic society. As we showed earlier, part of the majority's failure to do so can be attributed to the long history of privacy jurisprudence in India that evolved in the context of such balancing between immediate harms and larger social goals. But we still cannot ignore the fact that the court had received considerable instruction from the bar through judicial precedents and scholarship that tackled similar concerns arising from architectural interventions. Shyam Divan and other counsel appearing for various petitioners had relied on the idea of limited government, one that went beyond individual harms as narrowly framed to a more structural sense of what the power balance between the State and the citizen ought to be for democracy to survive. The majority chose not to address these submissions in an appealing manner, instead taking an easier route of reading in procedural safeguards. Through this choice, the majority let go of a valuable opportunity to engage with the kind of long-term harms and structural imbalances that any democratic society must be prepared to confront in the age of emerging technologies and big data analytics.

---

to race, religion, caste, tribe, ethnicity, language, income or medical history into CIDR, the mandatory linking of Aadhaar with various schemes allows the same result in effect."

[75] 2019 JMFC Full 04. *See*, Madhav Khosla and Ananth Padmanabhan, 'How Jamaican Supreme Court has Killed India's Hope of Selling Aadhaar to the World, for Now' (*ThePrint*, 22 June 2019) <https://theprint.in/opinion/how-jamaican-supreme-court-has-killed-indias-hope-of-selling-aadhaar-to-the-world-for-now/252199/> accessed 19 June 2019; Gautam Bhatia, 'The Afterlife of the Aadhaar Dissent: The Jamaican Supreme Court Judgment Quashing NCID' (*LiveLaw*, 14 April 2019) <https://www.livelaw.in/columns/jamaican-sc-national-biometric-identification-system-144269> accessed 19 June 2019.

Web 2.0 and the Concept of 'Data Controller': Recent Developments in EU Data Protection Law

Maria Berger & David Eisendle***

Abstract *In order to operationalise the fundamental right to privacy, as reaffirmed by the Supreme Court in the landmark K.S. Puttaswamy judgment, the Indian government has recently introduced a draft data protection legislation. The present draft is inspired — to a considerable extent — by the EU's GDPR and defines numerous key notions in largely identical terms. In view of these similarities, this paper seeks to examine the recent developments in the EU regarding the concept of 'data controller' and its application to what may be termed as a 'Web 2.0 setting'. The paper commences with a review of the obligations imposed on controllers under the GDPR. Next, it introduces the 'Web 2.0 setting' and traces the evolution of the 'data controller' concept with the emergence of the internet. The paper then turns to a substantive analysis of the understanding of data controllers in a Web 2.0 context by examining the case of Wirtschaftsakademie Schleswig-Holstein, which concerns the potential joint controllership of Facebook and the administrator of a Facebook fan page. The final section challenges the interpretations of the concept previously adopted by the ECJ and provides suggestions to better realise the objectives of data protection law.*

* Honorary Professor at the University of Vienna School of Law – Department of European, International and Comparative Law, Austria; former Judge at the Court of Justice of the European Union, Minister of Justice of the Republic of Austria and Member of the European Parliament.

** Legal Secretary (*référendaire*) in the Chambers of Judge Andreas Kumin at the Court of Justice of the European Union, prior to that in the Chambers of Judge Maria Berger and Advocate General Juliane Kokott; law and business studies in Vienna (Austria), Hong Kong and St. Gallen (Switzerland); LL.M, B.Sc., LL.B.

I. Introduction

From a European and judicial perspective, it is both valuable and enriching to keep an eye on key developments taking place in the case-law of top courts in other parts of the world. In that respect, the recent seminal judgment rendered by the Indian Supreme Court on 24 August 2017 in *K.S. Puttaswamy* v. *Union of India* deserves particular attention, for it ruled, in essence, that the right to privacy is protected as a fundamental right under the Constitution of India.[1] As the Supreme Court noted in memorable terms, privacy is the "*constitutional core of human dignity*" and subserves, at a normative level, "*those eternal values upon which the guarantees of life, liberty and freedom are founded*".[2] It went on to observe that while the negative content of privacy "*restrains the state from committing an intrusion upon the life and personal liberty of a citizen*", its positive content "*imposes an obligation on the state to take all necessary measures to protect the privacy of the individual.*"[3] Mindful of the challenges inherent to the network society and the information age that we live in, the Supreme Court rightly emphasised in this context that informational privacy is a facet of the right

---

1 *KS Puttaswamy v Union of India* (2017) 10 SCC 1 (*Puttaswamy*); *See*, for a presentation of the judgment, M Guruswamy, 'Justice K.S. Puttaswamy (Retd) and Anr v Union of India and Ors' (2017) 111 American Journal of International Law 994; further, on the evolution of the right to privacy in India, *see*, A Pillai and R Kohli, 'A Case for a Customary Right to Privacy of an Individual: A Comparative Study on Indian and other State Practice' (2017) Oxford University Comparative Law Forum 3 <https://ouclf.law.ox.ac.uk/a-case-for-a-customary-right-to-privacy-of-an-individual-a-comparative-study-on-indian-and-other-state-practice/> accessed 10 October 2019. It is interesting to note that the judgment was interpreted as having paved the way for another landmark decision of the Indian Supreme Court, of 6 September 2018, in *Navtej Singh Johar v Union of India* (2018) 10 SCC 1, concerning the decriminalisation of any consensual sexual relations among adults in private.

2 *Puttaswamy* (n 1) part T, para 3(E).

3 *Puttaswamy* (n 1) part T, para 3(I); *See also*, Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review 193. This ground-breaking article on the subject famously captured the essence of this negative content of the right to privacy by referring to the right "*to be let alone*". As regards EU law, any limitation on the exercise of the right to privacy, laid down in Article 7 of the Charter of Fundamental Rights of the European Union, must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others; *See*, to that effect, European Court of Justice (ECJ) judgment of 8 April 2014, Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* 2015 QB 127: [2014] ECR 238 (38).

to privacy, and that dangers to privacy in an age of information can originate not only from the state but from non-state actors as well.[4]

In order to give effect to the right to privacy, the Indian government was thus directed to examine and put into place a robust regime for data protection. Subsequently, the committee established in response to the judgment and entrusted with the task of elaborating such a legal framework under the direction of retired Justice Srikrishna ('**Srikrishna Committee**') prepared a draft bill for a comprehensive Personal Data Protection Act.[5] In the Committee's explanatory report,[6] this bill – which is likely to be introduced in the Indian Parliament in June 2019 – is described as representing a fourth path, distinct from the approaches to data protection in the US, the EU and China.[7] However, as is apparent from both its structure and content, the bill is inspired to a considerable extent by the EU General Data Protection Regulation ('**GDPR**'),[8] which became applicable as of 25 May 2018. In particular, processing personal data requires a lawful basis – which is, first and foremost, consent – and the individuals whose data is being processed are conferred specific rights such as the right to confirmation of data and access to data, the right to data portability, the right to correction of data and the right to be forgotten, though these rights may differ in scope compared to the GDPR.[9] What is more, key notions of both the draft bill and the GDPR are defined in largely identical terms. This holds true not only for 'personal data' and 'processing', but also for 'data subjects' and 'data controllers', even though, in respect of the two latter notions, the terminology differs as the draft bill refers to 'data principals' and 'data fiduciaries'.[10]

---

4 *Puttaswamy* (n 1) part T, para 5.

5 The Draft Personal Data Protection Bill 2018 (*Draft Bill*). For an analysis of the bill, *see*, Lothar Determann and Chetan Gupta, 'Indian Personal Data Protection Act, 2018: Draft Bill and its History, compared to GDPR and California Privacy Law' (2018) UC Berkeley Public Law Research Paper <https://dx.doi.org/10.2139/ssrn.3244203> accessed 10 October 2019.

6 Committee of Experts under Justice BN Srikrishna, *A Free and Fair Digital Economy—Protecting Privacy, Empowering Indians* (2018) <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> accessed 10 October 2019.

7 ibid 14.

8 Regulation (EU) 2016/679 of 27 April 2016 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC(2016) OJ L119/1 (GDPR).

9 *See*, Draft Bill, chs III and VI.

10 As is pointed out at pages 7 and 8 of the Srikrishna Committee's report (n 6), in a regulatory framework where the rights of the individual with respect to her personal data are respected and the existing inequality in bargaining power between individuals and entities that process such personal data is mitigated, the individual must be the *data principal* since she is the focal actor in the digital economy. By contrast, entities collecting personal data

In view of these similarities, it appears to be of interest from a comparative legal perspective for this Journal's readers in India and beyond to shed light on recent developments in EU data protection law with regard to the concept of data controller. This concept plays a crucial roles since it determines responsibility for compliance with data protection rules. In this contribution, we first provide a brief overview on the definition of data controller under EU law and the case-law of the European Court of Justice ('**ECJ**') on this concept's application in the context of the Internet. We then examine how this concept is applied in what can be called a 'Web 2.0 setting'. For this purpose, we focus on the recent judgment rendered by the Grand Chamber of the ECJ in the case of *Wirtschaftsakademie Schleswig-Holstein*[11] concerning the question of data protection responsibility in relation to a fan page on the social network Facebook.

II. The Concept of 'Data Controller' in EU Data Protection Law

A. Principles

In EU data protection law, data controllers take on a central role. As it has previously been held in the ECJ's case-law, controllers must ensure, within the framework of their responsibilities, powers and capabilities, that the data processing in question meets the legal requirements in order that the guarantees laid down by law may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.[12] Under the regime of the GDPR, this is reflected most fundamentally in Article 24(1), according to which the controller is tasked to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the regulation. The provisions in Chapter III of the GDPR, which concern the rights of the data subject, are essentially directed at the controller and define obligations incumbent on him. It is therefore the controller's responsibility to provide transparent information to the data subject concerning collected personal data relating to him, to grant access to the personal data, and to

have a duty of care to deal with such data fairly and responsibly for purposes reasonably expected by the principals, which makes such entities *data fiduciaries*.

[11] C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (2019) 1 WLR 119 (ECJ, 5 June 2018) (*Schleswig-Holstein*).

[12] C-131/12 *Google Spain SL and Google v Agencia Española de Protección de Datos* (AEPD) 2014 QB 1022: (2014) 3 WLR 659 (ECJ, 13 May 2014) paras 38 and 83 (*Google Spain*).

ensure rectification of inaccurate personal data or its erasure. Furthermore, under Article 82(1) GDPR, any person who has suffered damage as a result of an infringement is entitled to receive compensation from the controller, and under Article 82(2), any controller involved in processing shall be liable for the damage caused by processing data in violation of the regulation.

According to Article 4(7) GDPR, 'controller' is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.[13] This definition corresponds to the one retained in Article 2(d) of the original EU Data Protection Directive[14] ('**DPD**'), which was adopted in 1995 and repealed by the GDPR. For analysing the notion of controller, valuable guidance has been provided by a detailed study[15] carried out by the Article 29 Data Protection Working Party, an independent advisory board set up by the DPD and comprising, in particular, representatives from the EU Member States' national data protection authorities.[16] As the Working Party pointed out, the concept of controller has, fundamentally speaking, a wide and dynamic meaning and scope, for it relates to activities reflecting the life cycle of information from the point of its collection to its destruction.[17] Furthermore, it is a functional concept intended to allocate responsibilities where the factual influence is, and is thus based on a factual rather than a formal analysis.[18]

The definition of controller includes three central elements. Besides the *personal* aspect ("*natural or legal person, public authority, agency or any other body*") and the possibility of *pluralistic control* ("*alone or jointly with others*"), it is the *substantive* element (determination of the "*purposes and means of the processing of personal data*") that deserves particular attention, as it is this part that allows one to distinguish the controller from other actors. According to the Working Party's findings, determining the purposes and the means amounts to determining respectively the *why* and the *how* of

---

[13] By way of comparison, cl 13(3) of the Draft Bill defines 'data fiduciary' as "*any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data*."

[14] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L281/31 (DPD).

[15] Article 29 Working Party (WP 29), *Opinion 1/2010 on the concepts of 'controller' and 'processor'* (2010) 00264/10/ENWP 169 (Opinion 1/2010).

[16] As of 25 May 2018, the WP 29 has been replaced by the European Data Protection Board; *See*, GDPR, arts 68-76.

[17] Opinion 1/2010 (n 15) 3.

[18] Opinion 1/2010 (n 15) 9. It is stated, in this connection, that one should look at the specific processing operations in question and understand who determines them, by replying in a first stage to the questions "*why is this processing taking place? Who initiated it?*".

certain processing activities. While determination of the purpose of the processing would in any case trigger the qualification as controller, determining the means implies, in their view, control merely over the essential elements of the processing. By contrast, as regards technical or organisational questions, the determination of the means of processing can be delegated by the controller.[19]

B. The Concept's Application in the Context of the Internet

It must be borne in mind that the foundations of EU data protection law, and the definition of data controller included in this legal framework, date back to a time at which the Internet – here understood in the sense of the World Wide Web – was still in its infancy.[20] This framework, originally established by the DPD and now carried forward to the GDPR, has been characterised as a *linear model*, fitting well for an environment of centralised data processing with independent relationships between data subjects and data controllers. In such a setting, the controller is the main architect of the information system, exercising full control and responsibility.[21] Given that both the DPD and the GDPR were drafted in a technology neutral manner, it presented no particular difficulties to clarify that, in principle, data protection rules fully apply to data processing taking place on the Internet as well. Thus, in its early landmark case *Lindqvist*, the ECJ ruled that the DPD applied to a situation where elements of personal data are published on a web page on the Internet.[22]

Subsequently, in *Google Spain and Google,* the ECJ was called upon to examine a situation where an Internet search engine provided search results

---

[19] Opinion 1/2010 (n 15) 13 and 15. The WP 29 identifies aspects such as "*which data shall be processed?*", "*for how long shall they be processed?*", or "*who shall have access to them?*" as essential elements.

[20] In effect, the EU Commission's original proposal for the EU Data Protection Directive (DPD) was presented in 1990, when the World Wide Web had not even existed yet and the epoch-making changes it would induce could barely be foreseen.

[21] *See*, Omer Tene, 'Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws' (2013) 74 Ohio State Law Journal 1219; Rene Mahieu, Joris van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World – on the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe' (2018) 10 Journal of Intellectual Property, Information Technology and E-Commerce Law 85 <https://dx.doi.org/10.2139/ssrn.3256743> accessed 10 October 2019.

[22] C-101/01 *Bodil Lindqvist v Aklagarkammareni Jönköping* 2004 QB 1014: (2004) 2 WLR 1385 (ECJ, 6 November 2003). The case concerned a church worker in Sweden who published, on her personal internet website, information about other parish members, such as their names, hobbies and phone numbers, without having obtained those individuals' prior consent.

which direct the engine's users to the source web page. The question was, inter alia, whether the operator of such a search engine had to be regarded as a data controller in respect of the processing of personal data that it carried out. It was argued that the operator did not meet the definition of data controller, given that it did not exercise control over the personal data published on the web pages of third parties.[23] The Court explicitly rejected this argument, pointing out that the concept of controller must be interpreted broadly, with a view to ensure effective and complete protection of data subjects, and that it was not necessary, in order to be regarded as a controller, to have complete control over all aspects of data processing.[24] The Court further considered that the processing of personal data carried out in the context of the activity of a search engine could be distinguished from, and was additional to, that carried out by publishers of websites, consisting in loading those data on an Internet page.[25] For it is the search engine operator which determines the purposes and means of its activity and thus of the processing of personal data that it itself carries out within the framework of that activity. Consequently, the search engine operator had to be regarded as the data controller in respect of that processing.[26]

One cannot but realise, however, that in comparison to the factual circumstances which the two cases outlined above were based on, contemporary technological reality is immensely more sophisticated. This reality is characterised by multi-tiered structures and complex, interactive relationships between individual actors. New features have emerged and continue to expand rapidly; including social networks, hosted services and web applications – developments that are commonly referred to as being part of and forming *Web 2.0*. A typical situation is that an information provider's interactive web presence is integrated in another provider's platform. Think, for instance, of blogs or of merchants offering goods on Amazon Market place or Ebay. Visitors to theses web pages are faced with at least two different information providers. From a data protection point of view, the question thus arises as to how one must apply data protection rules in these settings. In particular, in addition to establishing data protection responsibility, it

---

[23] *Google Spain* (n 12) para 22.
[24] *Google Spain* (n 12) para 34.
[25] *Google Spain* (n 12) para 35.
[26] *Google Spain* (n 12) para 33. By contrast, in his opinion rendered in this case, Advocate General Jääskinen argued that Internet search engine service providers merely supply an information location tool without exercising control over personal data included on third-party web pages. As they cannot in law or in fact fulfil obligations of a controller in relation to the personal data on source web pages, they should not generally be considered as having that position.

must be determined how responsibility is to be allocated between the individual information providers.[27]

III. Data Control in a Web 2.0 Setting – the *Wirtschaftsakademie Schleswig-Holstein* Case

A. Facts of the Case

The ECJ was recently called upon to address precisely this issue in a case concerning a fan page hosted on the social network Facebook. Such a fan page can be set up, by individuals or businesses registered with Facebook, who can then use the platform, for instance, to introduce themselves to their users and to communicate with them. Additionally, operating the fan page entails the possibility to obtain, by means of a function called *Facebook Insights*, 'anonymous' statistical information on visitors to the page. This feature, which can be categorised as a form of *online behavioural tracking*,[28] is made available by Facebook free of charge under non-negotiable conditions of use. Information is collected by means of evidence files (cookies), which each contain a unique user code and remain active for two years while they are stored by Facebook on the fan page visitor's computer hard disk or other media. The user code is collected and processed when the fan pages are opened. Consequently, Facebook receives, registers and processes the information stored in the cookies when a person visits its services.

The German-based company Wirtschaftsakademie Schleswig-Holstein ('**Wirtschaftsakademie**') operates a fan page hosted on Facebook, by means of which it offers educational services. In November 2011, Wirtschaftsakademie

---

[27] *See*, P Hacker, 'Mehrstufige Informationsanbieterverhältnisse zwischen Datenschutz und Störerhaftung' (2018) 21 Multimedia und Recht 779; Bernd Wagner, 'Disruption der Verantwortlichkeit: Private Nutzer als datenschutzrechtliche Verantwortliche im Internet of Things' (2018) Zeitschrift für Datenschutz 307, 308; S Schulz, 'Case Comment Wirtschaftsakademie Schleswig-Holstein' (2018) Zeitschrift für Datenschutz 357, 364.

[28] Such tracking consists in recording and collecting data linked to an individual visiting the internet over a period of time in order to gain information on this individual. *See*, G Skouma and L Léonard, 'On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection' in S Gutwirth et al (eds), *Reforming European Data Protection Law* (Springer 2015) 35; Mireille Hildebrandt, 'Profiling: From Data to Knowledge – The Challenges of a Crucial Technology' (2006) 30 Datenschutz und Datensicherheit 548, 549; *See also*, Claude Castelluccia, 'Behavioural Tracking on the Internet: A Technical Perspective' in S Gutwirth et al (eds), *European Data Protection: In Good Health?* (Springer 2012). Behavioural tracking used for advertisement purposes is referred to as *behavioural advertising*. In this context, characteristics of online behaviour are tracked to develop a specific profile of users in order to provide tailored advertisement; *See*, WP 29, *Opinion 2/2010 on online behavioural advertising* (2010) 00909/10/ENWP 171 4, 5.

was ordered by a German data protection authority to deactivate the fan page it had set up, on the ground that visitors to the fan page were not informed that Facebook, by means of cookies, collected and processed personal data concerning them. Wirtschaftsakademie brought a complaint against that decision, arguing, in essence, that it was not responsible under data protection law for the processing of the data by Facebook or the cookies which the latter installed. By contrast, the data protection authority took the view that, by setting up the fan page, Wirtschaftsakademie had made an active and deliberate contribution to the collection by Facebook of personal data relating to visitors to the fan page, from which it profited by means of the statistics provided to it by Facebook. Subsequently, Wirtschaftsakademie turned to the Administrative Court which annulled the data protection authority's decision and found that the administrator of a fan page on Facebook, such as Wirtschaftsakademie, cannot be considered as controller and therefore cannot be the addressee of a measure such as to deactivate its fan page.[29] The Higher Administrative Court confirmed this view, stating that Wirtschaftsakademie was not a responsible entity in relation to the data collected by Facebook. Facebook alone decided on the purpose and means of collecting and processing personal data used for the Facebook Insights function, whereas Wirtschaftsakademie only received anonymised statistical information.[30]

The data protection authority appealed to the German Federal Administrative Court which, in line with the courts of lower instance, also held that Wirtschaftsakademie could not itself be regarded as responsible for the data processing.[31] It considered that while Wirtschaftsakademie, as a result of setting up a fan page, objectively provided Facebook with the possibility of using cookies when the fan page is retrieved and collecting data via these cookies, this could not lead to the inference that Wirtschaftsakademie was able to influence, administer, design or otherwise control the nature and scope of the processing by Facebook of its users' data. The conditions of use for the fan page did not give Wirtschaftsakademie any rights to influence or control this aspect. The unilaterally imposed conditions of use of Facebook were not the result of a process of negotiation and did not give Wirtschaftsakademie the right to prohibit Facebook from collecting and processing data of users of its fan page. Thus, Wirtschaftsakademie had

---

[29] *Rechtsanwälte A v Das Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (2013) 8 A 14/12 (Verwaltungsgericht Schleswig).

[30] *Rechtsanwälte A v Das Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (2014) 4 LB 20/13 (Schleswig-Holsteinisches Oberverwaltungsgericht).

[31] BVerwG (Federal Administrative Court, Germany), decision of 25 February 2016 1 c 28.14 para 16.

no decision-making, design or control powers. Accordingly, without any legal or actual influence on the decision about how personal data is processed, it could not be regarded as a controller. Furthermore, the Federal Administrative Court noted that while there was a legal relationship between Wirtschaftsakademie and Facebook to provide a fan page, this user relationship did not mean that Wirtschaftsakademie had commissioned Facebook to collect and process the data of the users of its fan page on its behalf.

However, the Court wondered whether, under such circumstances, the monitoring and intervention powers available to the data protection authority may relate solely to the data controller (i.e., in the present case, Facebook) or whether there nonetheless remained scope for responsibility of an entity that does not control the data processing, like Wirtschaftsakademie, when choosing the operator for its information offering. It took the view that in information provider relationships in which providers use an infrastructure such as that offered by Facebook, where they do not themselves control the processing of personal data by the infrastructure provider, it is necessary to also include the information provider itself within the scope of responsibility. This is essential to ensure the effective protection of the users of the information. This data protection responsibility would then relate to the careful choice of the operator of the infrastructure used for the information provider's own offering. Therefore, having in mind the objective of effective protection of the right to privacy, the Federal Administrative Court decided to stay the proceedings. It referred to the ECJ the question of whether the notion of data controller in EU data protection law definitively and exhaustively defines liability and responsibility for data protection infringements, or whether scope remains, in multi-tiered information provider relationships such as in the setting at issue, for responsibility of an entity that does not control the data processing, when it chooses the operator of its information offering.[32]

B. The ECJ's Judgment

Recalling the necessity to ensure, through a broad definition of the concept of data controller, effective and complete protection of the persons concerned, the ECJ considered – as was undisputed in the present case – that Facebook had to be regarded as the controller, for it primarily determined the purposes and means of processing the personal data of users of Facebook

[32] Other questions referred to the ECJ by the Federal Administrative Court, concerning inter alia the division of competences between data protection authorities of different EU member States, are not relevant here.

and persons visiting the fan pages hosted on Facebook.[33] However, the Court emphasised that that concept did not necessarily refer to a single entity and may concern several actors taking part in the processing of personal data. It thus went on to examine whether and to what extent Wirtschaftsakademie *itself*, as the administrator of a fan page on Facebook, may also be regarded as a controller, inasmuch as it contributes in the context of that fan page in determining, jointly with Facebook, the purposes and means of processing the personal data of the visitors to the fan page.[34]

The Court answered in the affirmative. First of all, it noted that the processing of personal data at issue was:

> intended in particular to enable Facebook to improve its system of advertising transmitted via its network, and to enable the fan page administrator to obtain statistics produced by Facebook from the visits to the page, for the purposes of managing the promotion of its activity, making it aware, for example, of the profile of the visitors who like its fan page or use its applications, so that it can offer them more relevant content and develop functionalities likely to be of more interest to them.[35]

While, in the Court's view:

> the mere fact of making use of a social network does not make its user a controller jointly responsible for the processing of personal data by that network, […] the administrator of a fan page hosted on Facebook, by creating such a page, gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page, whether or not that person has a Facebook account.[36]

Moreover,

> the creation of a fan page on Facebook involves the definition of parameters by the administrator, depending inter alia on the target audience and the objectives of managing and promoting its activities, which has an influence on the processing of personal data for the purpose of producing statistics based on visits to the fan page. The administrator may, with the help of filters made available by Facebook, define the criteria in accordance with which the statistics are to be drawn up and even designate the categories of persons whose personal data is to be made use of by Facebook. Consequently, the administrator of a fan

---

[33] *Schleswig-Holstein* (n 11) paras 28 and 30.
[34] *Schleswig-Holstein* (n 11) para 31.
[35] *Schleswig-Holstein* (n 11) para 34.
[36] *Schleswig-Holstein* (n 11) para 35.

> page hosted on Facebook contributes to the processing of the personal data of visitors to its page.[37]

The Court added that

> the administrator of the fan page can ask for and thereby request the processing of — demographic data relating to its target audience, including trends in terms of age, sex, relationship and occupation, information on the lifestyles and centres of interest of the target audience and information on the purchases and online purchasing habits of visitors to its page, the categories of goods and services that appeal the most, and geographical data which tell the fan page administrator where to make special offers and where to organise events, and more generally enable it to target best the information it offers.[38]

In contrast, the fact that the audience statistics compiled by Facebook were transmitted to the fan page administrator only in anonymised form was not deemed decisive, given that the production of those statistics was based on the prior collection and processing of the personal data of those visitors for such statistical purposes.[39] Furthermore, the Court explicitly held that the use of a platform like the one operated by Facebook could not exempt a fan page administrator from compliance with data protection rules, given that a Facebook user account is not a precondition for being able to access the page. Rather,

> the fan page administrator's responsibility for the processing of the personal data of those persons appears to be even greater, as the mere consultation of the home page by visitors automatically starts the processing of their personal data.[40]

Therefore, the Court concluded that the administrator of a fan page hosted on Facebook, such as Wirtschaftsakademie, must be regarded as taking part in the determination of the purposes and means of processing the personal data of the visitors to its fan page and must thus be categorised, jointly with Facebook, as a controller responsible for that processing.[41]

---

[37] *Schleswig-Holstein* (n 11) para 36.
[38] *Schleswig-Holstein* (n 11) para 37.
[39] *Schleswig-Holstein* (n 11) para 38.
[40] *Schleswig-Holstein* (n 11) para 41.
[41] *Schleswig-Holstein* (n 11) para 39.

IV. Analysis

A. The Court's *leitmotif*: Effective and Complete Protection

Historically speaking, the enactment of a common EU legal framework on data protection was primarily driven by the desire to facilitate free movement of personal data within the EU.[42] It was expressly emphasised in Article 1(1) of the original DPD that the fundamental rights of individuals, in particular their right to privacy with respect to the processing of personal data, shall be protected.[43] This is repeatedly echoed in the case-law of the ECJ when it is noted that the DPD seeks to ensure a high level of protection.[44] In respect of Wirtschaftsakademie, which was an addressee of an injunctive order issued by a data protection authority, the courts in Germany initially dealing with the matter were well aware of this objective of EU data protection law. In their view though, only Facebook but not Wirtschaftsakademie could be regarded as responsible entity, given that, in essence, the latter was not deemed to exercise any influence on the processing of personal data. It was precisely in order to avoid gaps in protection that the German Federal Administrative Court considered whether the administrator of a Facebook fan page like Wirtschaftsakademie could nonetheless, even if to a lesser extent than a data controller, be made held responsible due to the (poor) choice of the operator of its information offering.[45]

Neither the ECJ, nor its Advocate General tasked with delivering a reasoned opinion on the case prior to the judges' deliberations, agreed with the premise that the German courts had based their reasoning on. Advocate General Bot pointed out that, most fundamentally, the data processing at issue was preconditioned by the decision of the fan page administrator to create and operate the page. Not only does that administrator have a decisive

---

[42] *See*, DPD, Recitals 3, 8 and 10; Case C-518/07 *Commission v Germany* 2010 ECR I-1885 (ECJ, 9 March 2010) para 20; Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof v Österreichischer Rundfunk and Others* and *Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk* 2003 ECR I-4989 (ECJ, 20 May 2003) paras 39 and 70.

[43] Under the regime of the GDPR, Article 1(2) provides that the Regulation "*protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*."

[44] *See*, *Google Spain* (n 12) para 66; C-362/14 *Maximillian Schrems v Data Protection Commr* 2014 QB 527 (ECJ, 6 October 2015) para 38; C-473/12 *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert* (2014) 2 CMLR 297 (ECJ, 7 November 2013) para 28.

[45] *See*, F Jotzko, 'Case Comment Wirtschaftsakademie Schleswig-Holstein' (2018) 73 Juristenzeitung 1154, 1160.

influence over the commencement of the processing of the visitors' personal data, but it also lies in its hands to end that processing by closing the page down.[46] He further argued that, by using a tool like Facebook Insights, a fan page administrator participates in the determination of the purposes and means of the processing of the personal data of visitors to its page.[47] The administrator is able to influence the specific way in which that tool is put to use by defining the criteria for the compilation of the viewing statistics, thus playing a predominant role in how that data is processed by Facebook and exerting a de facto influence over it.[48]

The ECJ followed this approach and relied less on a textual analysis of the definition of data controller when interpreting the concept and applying it to the case at hand. Instead, it placed emphasis on teleological considerations. In effect, rather than analysing individually the purpose(s) and the means of the data processing induced by the creation of a fan page on Facebook, the Court noted with reference to *Google Spain and Google* that the objective of the provision defining the notion of data controller was to ensure, through a broad definition of that concept, effective and complete protection of the persons concerned. It went on to distinguish between three aspects: First, by creating the fan page, its administrator *enables* data processing by Facebook. Second, the administrator contributes itself to the data processing through defining *parameters* according to which statistics on the page's visitors are produced. Third, the administrator can *request* demographic data relating to its target audience, without it being relevant that this information is transmitted by Facebook only in anonymised form or that the administrator does not have (complete) access to the relevant data. Thus, an entity can meet the requirements for being qualified as data controller if it exerts, to a sufficient degree, influence over the data processed. While the first argument that the Court referred to in this context (*enabling*) would, taken alone, be particularly wide-ranging, it appears that the crucial element is the possibility to define parameters.[49] In fact, the Court concluded that precisely due to the definition of parameters, the administrator of a fan page must be regarded as "*taking part in the determination of the purposes and means*" of processing the personal data of the visitors to its fan page.[50] By contrast, joint responsibility needs to be distinguished from situations in which two or more actors

[46] *Schleswig-Holstein* (n 11) para 56.
[47] *Schleswig-Holstein* (n 11) para 55.
[48] *Schleswig-Holstein* (n 11) para 57.
[49] *See*, J Marosi and L Matthé, 'Case Comment Wirtschaftsakademie Schleswig-Holstein' (2018) Zeitschrift für Datenschutz 357, 362.
[50] *Schleswig-Holstein* (n 11) para 39.

simply collaborate in the processing of personal data, each processing taking place within its own sphere.

Through its broad approach, the Court primarily addresses the risk inherent to multi-tiered information provider relationships where the actors involved circumvent data protection rules and shuffle off responsibility elsewhere, to the detriment of the individuals whose personal data is processed.[51] As the Advocate General pointed out in his Opinion, a narrow interpretation might provide an incentive for an undertaking to have recourse to the services of a third party in order to escape its data protection obligation. In a setting such as the one at issue, an information provider like the fan page administrator could use a platform which might infringe data protection rules, but nonetheless escapes responsibility. In order to achieve a high level of protection, it must therefore be ensured that operators are not able to evade data protection compliance, by using a hosting service for their information offering.[52] In addition, the approach taken is also likely to produce a ripple effect with respect to all the information providers involved. First, operators are called upon to exercise care and diligence in choosing their platform provider and, if necessary, refrain from using its services. Consequently, the platform provider itself is encouraged to comply with data protection rules in order not to jeopardise its commercial success.[53] It is therefore to be seen in light of these aspects that the Court concluded that in a situation such as the one at issue, recognition of joint responsibility in relation to the processing of personal data contributes to *ensuring more complete protection* of the rights of data subjects.[54]

B. One Step Further? The Pending Case *Fashion ID*

To what extent the ECJ's judgment will set a precedent for the assessment of similar situations involving two or more information providers is not fully foreseeable at this point, given that the facts of the case are characterised by certain particularities. In fact, creating and operating a Facebook fan page inevitably entails the use of the platform provided by Facebook and, consequently, the processing of personal data by it. Visitors to the fan page cannot avoid their data being processed by Facebook, except by refraining from accessing the page altogether. The spheres of responsibility of Facebook and

---

[51] *See*, Jotzko (n 45) 1160.

[52] *See*, *Schleswig-Holstein* (n 11) paras 62 and 64.

[53] *Schleswig-Holstein* (n 11) para 4. *See*, to that effect, Nicolas Blanc, 'Wirtschaftsakademie Schleswig-Holstein: Towards a Joint Responsibility of Facebook Fan Page Administrators for Infringements to European Data Protection Law?' (2018) 4 European Data Protection Law Review 120, 124.

[54] *Schleswig-Holstein* (n 11) para 42.

the fan page administrator thus seem inextricably intertwined.[55] Therefore, the judgment must be considered as being directly relevant for settings in which entities using a platform for their information offering (can) exert a certain influence on purposes and means of the data processing performed by the platform provider.

As outlined above, in the present case, this influence appeared to be established for the Court primarily due to the fact that fan page administrators defined parameters and criteria according to which statistics were drawn up, thereby contributing to the processing of the personal data of the visitors. It remains to be seen, however, whether such kind of interference effectively presents a minimum level. In *Fashion ID*, a case currently pending before it, the ECJ has the opportunity to provide further clarifications.[56]

Fashion ID is a German-based online retailer which sells fashion items on its website. The retailer embedded a plugin, the so called 'Like-button', provided by Facebook, on its website. When a visitor accesses the site on which the button appears, this visitor's Internet Protocol address and browser string are automatically sent to Facebook, irrespective of whether the visitor even clicked on it. A consumer protection association brought legal proceedings and sought an order to force Fashion ID to cease integrating the plugin on its website, on the grounds, essentially, of failure to inform about the purpose of the data collection and the use of the data and to obtain the visitors' consent for the transmission of their data. The question arising in this context is whether someone who has embedded a plugin on a website which transmits personal data to a third party is to be considered a data controller, even without being in a position to influence the subsequent processing of the data obtained by that third party.[57]

Unlike in the *Wirtschaftsakademie* case, it does not appear that Fashion ID determines the parameters of any information about its website's visitors which would then be returned to it. The purpose of embedding the 'Like-button' rather consists in optimising advertisement of the products offered by the retailer, by being able to make them visible on Facebook. While the ECJ has not yet rendered its judgment in the case, Advocate General Bobek opined that the crucial criterion for an entity to be considered a data controller, was that that entity made it possible for personal data to be collected and

---

[55] *See*, F Moos and T Rothkegel, 'Case Comment Wirtschaftsakademie Schleswig-Holstein' (2018) 21 Multimedia und Recht 591, 599.

[56] C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* (2020) 1 WLR 969 (ECJ, 26 January 2017) *(Fashion ID)*, initiated by a request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Higher Regional Court Düsseldorf, Germany) .

[57] Oberlandesgericht Düsseldorf, decision of 19 January 2017 I-20 U (40/16).

transferred, without it being necessary that specific input as to the parameters is provided. In his view, (co-)determining the parameters of the data collected already takes place through the simple act of embedding the plug-in, which itself provides parameters of the personal data to be collected.[58]

C. Joint Control – Joint Liability?

In the light of this, it has been critically remarked that by setting the bar low as to the necessary extent of an entity's actual influence on determining the means and purposes of the processing of personal data, there is a risk of over stretching the concept of data controller.[59] In connection with Facebook fan pages, it has been noted in particular that the page administrator has usually no influence at all on the platform's architecture and key features, but is limited to use its services under non-negotiable terms – take it or leave it.[60] A wide understanding of (joint) control might inevitably go along with expanding liability beyond a limit that can be deemed reasonable.

The Court's considerations in *Wirtschaftsakademie* suggest awareness of this tension, given that it is expressly pointed out that "*the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data*." Rather, "*those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case*."[61] However, the Court did not further elaborate on this aspect, given that it was not called upon to examine in more detail the practical consequences of joint responsibility.

Stressing the need for a reasonable correlation between power, control and responsibility, Advocate General Bobek argues that the issue of control is to be assessed with regard to the concrete operation in question. A (joint) controller should therefore be deemed responsible for that operation or set of operations for which it shares or co-determines the purposes and means as far as a given processing operation is concerned.[62] By contrast, liability cannot spill over into any subsequent stages of data processing,

---

[58] Opinion of Advocate General Bobek in *Fashion ID* (n 56) paras 67-69.

[59] Opinion of Advocate General Bobek in *Fashion ID* (n 56) para 71; Hacker (n 27) 779-780; Schulz (n 27) 364; D Klein, 'Case Comment Wirtschaftsakademie Schleswig-Holstein' (2018) Zeitschrift für Internationales Wirtschaftsrecht 224, 226.

[60] *See*, Blanc (n 53) 124.

[61] *Schleswig-Holstein* (n 11) para 43.

[62] Opinion of Advocate General Bobek in *Fashion ID* (n 56) paras 91 and 99-101.

if such processing occurs outside an entity's control and knowledge.[63] In the Advocate General's view, in the case of the Facebook 'Like-button', the relevant stage of the processing corresponds to the collection and transmission of personal data, occurring by means of the plugin.[64] In the same vein, Schroers argues for limiting responsibility of joint controllers to joint processing. In the case of a Facebook fan page such as the one at issue in *Wirtschaftsakademie*, she notes that joint processing will likely relate to the collection of data from visitors of the fan-page and to the processing of this data for statistical purposes for Wirtschaftsakademie, but not to the use of the data by Facebook for Facebook's own analysis and advertising unrelated to Wirtschaftsakademie. Wirtschaftsakademie would therefore need to comply with the responsibilities incumbent on a controller with regard to this processing.[65] However, it has been pointed out that this interpretation might not respect the principle of effective and complete protection of data subjects as emphasised in the ECJ's case-law.[66] In that regard, one feasible option would consist in excluding the external liability of individual controllers in cases in which it can objectively be ascertained that a controller, due to a lack of actual decision-making power, is not in a position to comply with certain legal obligations which, in principle, would result from the classification as controller.[67] Such an interpretation is supported by the ECJ's finding in *Google and Google Spain* according to which a data controller must ensure, "*within the framework of its responsibilities, powers and capabilities*", that data processing complies with data protection rules.[68] In other words, *qui habet commoda, ferre debet onera* must be limited to the extent that *ultra-posse nemo obligatur*: while information providers who take advantage of using the services of a platform or embedding a plugin must also bear the burdens resulting therefrom, i.e. (joint) data protection responsibility vis-à-vis the users, they cannot be obligated beyond what they are able to do.[69] This includes, however, that they could be required to cease operating a fan page or embedding a plugin if such a measure is necessary to ensure effective and complete protection of the interests and rights of data subjects.

---

[63] Opinion of Advocate General Bobek in *Fashion ID* (n 56) para 107.

[64] Opinion of Advocate General Bobek in *Fashion ID* (n 56) para 102.

[65] Jessica Schroers, 'The Wirtschaftsakademie Case: Joint Controllership' (*KU Leuven Centre for IT and IP Law*, 14 August 2018) <https://www.law.kuleuven.be/citip/blog/the-wirtschaftsakademie-case-joint-controllership/> accessed 10 October 2019.

[66] Mahieu and others (n 21) 18. The authors refer to a hypothetical cookie notice saying, "*We collect your IP-address and Browser-ID and transfer this personal data to Facebook. We do not know what Facebook does with the data. Click here to accept and proceed*", which evidently would not amount to meaningful transparency in practice.

[67] *See*, Hacker (n 27) 780.

[68] *Google Spain* (n 12) paras 38 and 83; *See*, Mahieu and others (n 21) 19.

[69] *See*, C-115/16 *N Luxembourg 1 and Others v Skatteministeriet* (ECJ, 26 February 2019) para 143.

It is important to note in this context that both the *Wirtschaftsakademie* and *Fashion ID* cases concern the old DPD and the definition of data controller as retained therein. Nonetheless, given that the notion of data controller is identically defined in both the DPD and the new GDPR, it can reasonably be assumed that the Court's interpretation will in principle remain valid in a GDPR context as well. Unlike the DPD, however, the GDPR explicitly addresses the case of joint controllers. Under Article 26(1), where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. In that case, they are obliged to determine, in a transparent manner and by means of an arrangement between them, their respective responsibilities for data protection compliance in particular as regards the exercise of the rights of the data subject and their respective duties to provide information. According to Article 26(2) GDPR, the arrangement chosen shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects and its essence shall be made available to the data subject. If joint controllers fail to determine their respective responsibilities by means of an arrangement, they risk administrative fines under Article 83(4)(a) GDPR.[70]

However, what is crucial is that according to Article 26(3) GDPR, irrespective of the terms of the arrangement concluded between joint controllers, data subjects may exercise the rights conferred to them under the GDPR "*in respect of and against each of the controllers*." Moreover, under Article 82(4) GDPR, where more than one controller is involved in the same processing and where they are responsible for any damage caused by processing, "*each controller shall be held liable for the entire damage*" in order to ensure effective compensation of the data subject. Despite this, according to Article 82(5), a controller is entitled to claim back from the other controllers involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage when he has paid full compensation for the damage suffered.[71] The principle of joint and several liability anchored in Article 26(3) and Article 82(4)GDPR appears to be at odds with the Court's statement in *Wirtschaftsakademie* that the existence of joint responsibility does not necessarily imply equal responsibility.[72] It is possible, though, that the latter might be construed as foreshadowing a restrictive interpretation of

[70] Violations may be subject to administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

[71] In response to the ECJ's judgment in *Wirtschaftsakademie*, German data protection authorities were quick to make clear that, as joint controllers, Facebook fan page administrators must take care of compliance with data protection rules in order not to risk regulatory measures, and that it will not suffice to refer to the responsibility of Facebook.

[72] Moos and Rothkegel (n 55) 597.

the two provisions mentioned, which, however, remains to be verified in the ECJ's future case-law.

V. Conclusion

As is evidenced by the recent case-law of the ECJ, Web 2.0 and the emergence of multi-tiered information provider relationships represent specific challenges to data protection law. The ECJ addresses these challenges by interpreting broadly the concept of data controller, with a view to ensuring effective and complete protection of individuals whose personal data is processed. An entity which exerts, to a sufficient degree, influence over the data processed and therefore participates in determining the purposes and means of the data processing can be considered a (joint) data controller, without it being required that that entity has complete access to the data. However, this extensive interpretation gives rise to questions concerning the allocation of responsibility between joint controllers. While the Court has held that joint responsibility does not necessarily imply equal responsibility, it remains to be seen in future case-law how more specific criteria for the practical implementation of this statement are to be defined and reconciled with the principle of joint and several liability of joint controllers as laid down in Article 26(3) and Article 82(4) GDPR. While the currently discussed Indian Personal Data Protection Bill also provides, through the definition of *data fiduciary*, for the possibility of joint data control, it appears that it does not include specific provisions with regard to the legal consequences arising from such a situation. The recent developments in EU data protection law as outlined in this article may offer an occasion to reflect on the opportunity to further develop the draft bill in that sense.

The Weight of Secrets: Assessing the Regulatory Burden for Informational Privacy in India

*Lalit Panda**

Abstract *Given the galloping pace at which information technology continues to develop and penetrate our lives, it is inevitable that the aspirations of data protection will sometimes appear like hollow promises that the law cannot keep. This makes it essential to study the precise regulatory conditions that can allow for the effective enforcement of legal protections for informational privacy. This Article provides a holistic account of the likely breadth and regulatory burden of an effective data protection regime and attempts to flesh out various regulatory tools that can go into the design of a Data Protection Authority for India so as to account for the weighty duties it must bear. Touching on the proposals of the Srikrishna Committee while drawing on the experiences of other jurisdictions, it justifies the idea of a unified, cross-sectoral data protection regulator with a broad mandate, examines the limits of sectoral regulation, and clarifies the significance of and outlook for models such as co-regulation and responsive regulation, as well as the role of the much-vaunted principle of accountability. In assessing the enforcement burdens created by the substantive rights and duties of data protection, the article also provides pointers as to what we should expect from a privacy watchdog in India and how these expectations can best be met in practice.*

* Research Fellow, Vidhi Centre for Legal Policy. The author would like to thank Damini Ghosh, Senior Resident Fellow, Vidhi Centre for Legal Policy, for her guidance and inputs.

I. Introduction

A number of engaging legal problems in the emerging field of data protection require careful scrutiny as we grapple with questions regarding how to treat personal data, how to characterise the relationship between such data and the data principal/subject, how to identify the legitimate situations in which other persons may use such data, and what persons using such data must do to safeguard the interests of data principals/subjects. As India moves to adopt a governance framework for informational privacy, it is appropriate to closely analyse the substantive rights and duties that are put into place in relation with personal data, whose unique characteristics result in unique reasons to value it.

Even as the contours of various solutions to these problems emerge, the means by which to enforce data protection law equally require close study. The designs of the enforcement mechanisms for informational privacy also have a wide range of correlations with the unique characteristics of personal data and the structure of data protection law. As will emerge in the discussion below, these correlations mean that the design of the regulatory mechanism must proceed simultaneously with the design of the substantive law. The central argument of this article is that the regulatory scheme for data protection must closely match the regulatory burden it entails a burden shaped by the dizzying variety of contexts in which personal data is processed, the volume of such data being processed, the number of entities that process such data, the ease with which such data can change hands, the ease with which the use of the data can be modified, the ease with which possession and use can be obfuscated, and the subtle ways in which the observation of a person can harm them.

The problems related to regulatory burden in data protection are alluded to in the following section though they are further elucidated later in the Article. The third section then relates questions of capacity with two structural choices for a data protection regulator: first, whether to have the regulatory burden shouldered by a single, specialised regulator or have it shared amongst sectoral regulators, and second, whether to have the regulatory burden borne exclusively by the regulator or whether to allow regulated entities to participate in the regulatory process. After explaining why these choices have sparked debate in the context of data protection, the section argues in favour of the appropriate structures that need to be adopted in each case. The fourth section then turns the focus to two further concepts in data protection regulation: accountability and responsive regulation. Both these concepts are broken down and explained and the need for their adoption in data protection is linked, once again, to the unique regulatory burdens of the

field. The fifth and final section concludes with a few additional remarks. The focus throughout will be on the Draft Personal Data Protection Bill, 2018, released by the Srikrishna Committee of Experts on Data Protection ('**Srikrishna Committee**').[1] A new Bill with a number of modifications has since been tabled in Parliament,[2] and while the general regulatory approach discussed in this Article has remained the same, certain notable points of departure worth scrutinising have been identified below.

II. Enforcement Challenges, Old and New

A. A Legacy of Low Capacity

Rights and duties in practice have always depended on the regulatory structures by which they are given life. In India, for example, a recurring theme in regulatory policy is the limitation on capacity: the promises of the law remain unfulfilled because the regulatory structures that effectuate them can be poorly designed, under-staffed, and lacking in good governance incentives and procedures.[3] There can often be infrastructural shortcomings and lack of technical know-how.[4] Since it would be difficult to quickly build up capacity in the early days of a law's implementation, some argue that regulatory structures can collapse under pressure, fall back onto formalistic posturing or fail to follow due process requirements.[5] It is easy enough to say that inad-

---

1 Draft Personal Data Protection Bill, 2018, <https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf> accessed 21 March 2020 (Draft PDPB, 2018).

2 Personal Data Protection Bill, 2019, <http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf> accessed 21 March 2020 (PDPB, 2019).

3 *See*, for instance, Shubho Roy and others, 'Building State Capacity for Regulation in India', in Devesh Kapur and Madhav Khosla (eds), *Regulation in India: Design, Capacity, Performance* (Hart Publishing, 2019) 359 (arguing, on a number of bases, that "*Regulators have … been plagued by poor State capacity.*"); Devesh Kapur and others (eds), 'Introduction' in *Rethinking Public Institutions in India* (OUP, 2017) 5-8 (bemoaning lack of capacity due to the Indian State's "*relatively small size*" and due to its being "*as over-bureaucratized as it is under-staffed*".)

4 This issue is only exacerbated in the digital context. *See*, Geoffrey G. Parker and others, *Platform Revolution: How Networked Markets are Transforming the Economy — and How to Make Them Work for You* (W.W. Norton & Company, 2016) 255 (advising that future models of regulation for digital platforms across the world, including for data protection, will require "*significant talent upgrades on the part of government agencies*".); *See also*, Ananth Padmanabhan and Anirudh Rastogi, 'Big Data', in Devesh Kapur and Madhav Khosla (eds), *Regulation in India: Design, Capacity, Performance* (Hart Publishing, 2019) 272-273 (warning of how big data creates "*new challenges that demand the rapid upgrading of skills from the regulator's end*").

5 Suyash Rai, 'Comment on the White Paper of the Committee of Experts on a Data Protection Framework for India' 1-6 <http://macrofinance.nipfp.org.in/PDF/data_protection_comments_suyash.pdf> accessed 15 February 2019.

equacies in the level of enforcement are to be accepted for budgetary reasons or lack of expertise. However, this under emphasises the effects of deficits in regulatory capacity. Apart from a regulator's posturing and due process failures, the overall effect on the rule of law caused by unenforced rules and unaddressed violations should be recognised as a significant concern, though it may be difficult to measure.

B. Challenges in the Information Age

In addition to the legacy of issues surrounding state capacity in India, there are a number of additional burdens that are likely to emerge in the context of digital governance. One prime consideration is the pace of innovation in data processing techniques. Rule-based governance requires some stability of circumstances if the criteria embedded in the rule are to continue to be relevant and effective. If innovation is extremely fast-paced, the processes for the modification of rules will have to keep up. Governance institutions are already falling behind on many fronts and it seems apparent that this trend will continue.[6] In the realm of data protection, for example, this is apparent in such schemes for privacy protection as anonymizsation.[7] Another aspect of the innovation question is the public interest in actually promoting it. All the fruits of technological advancement have been borne due to the culture of innovation that the tech industry has promoted and the continued channelling of such benefits would require that this culture not be throttled by *ex ante* regulatory schemes like licensing and permissions.[8]

If the speed of change creates one set of problems from a dynamic view, the complexity, context-specificity and opacity of data-related processes

---

[6] William D. Eggers and others, 'The Future of Regulation: Principles for Regulating Emerging Technologies', (*Deloitte Insights*, 19 June 2018) <https://www2.deloitte.com/insights/us/en/industry/public-sector/future-of-regulation/regulating-emerging-technology.html> accessed 23 February 2019 ("*As new business models and services emerge … government agencies are challenged with creating or modifying regulations, enforcing them, and communicating them to the public at a previously undreamed-of pace.*"); for general discussion on the 'ossification' of traditional rulemaking, *See*, Richard J. Pierce, Jr., 'Rulemaking Ossification is Real: A Response to Testing the Ossification Thesis' (2012) 80 George Washington Law Review 1493; Jason Webb Yackee and Susan Webb Yackee, 'Testing the Ossification Thesis: An Emperical Examination of Federal Regulatory Volume and Speed, 1950-1990' (2012) 80 George Washington Law Review 1414; Aaron L. Nielson, 'Optimal Ossification' (2018) 86 George Washington Law Review 1209.

[7] Jules Polonetsky and others, 'Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification' (2016) 56 Santa Clara Law Review 593, 594 ("*Computer scientists and mathematicians have come up with a re-identification tit for every de-identification tat.*")

[8] Parker (n 4) 230 ("*There is a significant tension between the social goals of promoting innovation and economic development, which argue for a relatively laissez-faire approach to regulating platforms, and the social goals of preventing harm, encouraging fair competition, and maintaining respect for the rule of law.*")

constitute another such set even if we discount change. The very use of information technology exponentially increases the difficulty in detection of violations and makes many kinds of sustained investigations considerably tricky. Issues related to the number of users, physical accessibility of devices, remote access to digital assets, transnational dimensions, speed of data exchange, anonymity and encryption, automation etc. do not all surface simultaneously in non-digital governance areas.[9] The power of platforms to constrain competition, the growth of unmanageably voluminous information flows, and systemic threats with uncertain future realisation constitute further challenges to the existing paradigm for regulatory constructs.[10] As a result of these issues, regulators are looking to bolster various facets of their investigative powers.[11] Even short of investigation, regulators must worry about the appropriateness of their rulemaking. Any regulations issued by a regulatory body should not run slip-shod over the differentiated circumstances in which privacy interests arise.[12] What is more, data protection law in particular must face up to unique issues including the level of regulatory discretion needed to strike the right balance in fair rulemaking or adjudication while coping with the transaction-intensive nature of personal data transfers across industries.[13] Further, key regulatory concerns in data protection linked to context-sensitivity, the ease of change of purpose for process-

---

[9] For a detailed view of such issues, *see*, International Telecommunication Union, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (September 2012) <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf> accessed 23 February 2019, at 22-23, 75-81, 227-33, 239-43 (for example, the report notes how investigative agencies were able to meet the challenges of child pornography while it was still transported through the postal services but struggle to do so now); *See also*, for some of the traditional techniques used by violators, Larry Greenemeier, 'Seeking Address: Why Cyber Attacks are So Difficult to Trace Back to Hackers' (*Scientific American*, 11 June 2011) <https://www.scientificamerican.com/article/tracking-cyber-hackers/> accessed 23 February 2019.

[10] Julie E. Cohen, 'The Regulatory State in the Information Age' (2016) 17 Theoretical Inquiries in Law 369, 375, 395.

[11] Oscar Williams, 'Exclusive: Government Considering Boosting ICO's Powers Amid Cambridge Analytica Scandal' (*New Statesman Tech*, 26 March 2018) <https://tech.newstatesman.com/news/government-ico-powers-cambridge-analytica> accessed 23 February 2019); *See also*, Carole Cadwalladr, 'Elizabeth Denham: 'Data Crimes are Real Crimes' (*The Guardian*, 15 July 2018) <https://www.theguardian.com/uk-news/2018/jul/15/elizabeth-denham-data-protection-information-commissioner-facebook-cambridge-analytica> accessed 23 February 2019 (for a view on the kind of personnel required for a large data protection investigation as well as the reliance on journalists, civil society and whistleblowers for bringing forward evidence).

[12] For a leading theory on the contextual approach to privacy, *see*, Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79(1) Washington Law Review 119; for a further view on the contextual nature of digital interfaces in different areas, *see*, Stephen R. Miller, 'First Principles for Regulating the Sharing Economy' (2016) 53 Harvard Journal on Legislation 147, 151, 153.

[13] Rai (n 5) 3-5.

ing, and the diffused nature of privacy harms play equally significant roles in shaping the regulatory burden under study and will be elaborated upon in appropriate sections below.

It is in the face of such legacy and emerging issues that a regulatory framework for data protection must be built up. How far privacy law sees active implementation will depend on the way these challenges are dealt with.

III. The Structural Choices for a Privacy Watchdog

There is a broad consensus across jurisdictions that data protection regulation benefits from the existence of regulatory bodies instead of just legislations implemented by government departments and courts.[14] Setting this question aside, there are some further standard questions on regulatory structure that must be answered at the threshold - whether regulation can be better done by a specialised, unified regulator or by sectoral regulators acting in their specific sectors, and how far can private entities be trusted to share regulatory burdens. Both questions are dealt with in turn below. However, they have one common theme animating the concerns over whether a regulator will be able to bear its regulatory burdens all by itself. The amelioration of such concerns may seem to necessitate solutions involving some form of 'decentralisation' of regulatory controls. However, not all of these forms of sharing of burdens are equally appropriate and the manner in which these approaches can go wrong is elaborated upon below in justifying particular structural choices.

A. The Perils of a Worm's-Eye View

As discussed above, our preferences regarding our own personal information can be strikingly contextual. What we are willing to reveal or communicate regarding ourselves depends on who we are talking to and who else can hear us. Taken to its logical end, this line of reasoning would suggest that the best rules for the regulation of personal information flows must be developed within the different walks of life in which we operate. Would it then not be appropriate for there to be sectoral regulators handling data protection questions in their respective sectors? Finance, health, news media, social

[14] The kinds of problems that necessitate specialised regulatory bodies include the inability of legislatures to keep up with dynamic areas of law and their lack of intricate industry knowledge coupled with the fact that government departments have a similar lack of expertise and specialisation, weak processes to absorb market feedback, a continued culture of central planning, the potential politicisation of individual transactions due to direct ministerial control, and conflicts of interest where departments own elements of the production process. *See*, for an instance of this listing, Roy (n 3).

media, governmental agencies, legal proceedings etc. can each have different standards for privacy with agencies dedicated for these areas handling data protection issues according to the in-depth understanding of their field.

However, even a cursory glance at developments in other jurisdictions dispels this notion. The move towards comprehensive privacy legislations has been gradual but decisive, with comparative experiences in implementation playing a key role. Even the EU's shift from the 1995 Data Protection Directive to the recent General Data Protection Regulation ('**GDPR**') was largely driven by concerns regarding fragmentation in the implementation of data protection law in different European jurisdictions.[15] The US is a prominent outlier on this front with the applicability of key federal legislations being restricted only to specific types of data and specific types of entities. However, such a focus on a limited set of identified contexts of information use results in gaps in coverage. Enforcement actions are constantly forced to proceed only after threshold determinations are first made regarding the applicability of legislation to a particular situation.[16] This means that every time privacy rules are sought to be enforced, the legal process must first ascertain whether certain, specific rules are applicable to particular entities - a determination made on the basis of how a sectoral law defines the entities it seeks to regulate or otherwise specifies its own applicability, eg a law on financial privacy will often have to delineate which financial organisations it will apply itself to. States also chip in with laws for their own territories, adding to the already veritable patchwork such that there is reduced clarity, increased complexity and sometimes even conflicts between the different laws in a fragmented regime.[17]

The examples of the health and telecommunications sector in the US have been used to indicate that the definitions used to identify the relevant players in the industry or the definition of specific kinds of information fail to address even those privacy concerns that relate to that industry, often because the said definitions are confusing or inadequate. This is in the nature of the ease of modification of data use and is especially troublesome given the increased big data analytics practices that lack fixed purposes and allow data to break sectoral silos.[18] As noted privacy scholar Daniel Solove notes,

---

[15] *See*, General Data Protection Regulation (EU) 2016/679, Recital 9.

[16] Paul M. Schwartz, 'The Value of Privacy Federalism' in *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Roessler & Mokrosinska eds.) (2015).

[17] Nuala O'Connor, 'Reforming the US Approach to Data Protection and Privacy' (*Council on Foreign Relations*, 30 January 2018) <https://www.cfr.org/report/reforming-us-approach-data-protection> accessed 28 March 2019.

[18] Kirk J. Nahra, 'Is the Sectoral Approach to Privacy Dead in the U.S.?' (*Privacy and Security Law Report*, 2016) 15 PVLR 153.

the sectoral regime in the US has resulted in widespread uncertainty regarding the protections available for different kinds of personal data, a resultant lack of respect for US privacy law, failure in the law keeping up with sectoral shifts, and persistence of gaps where data remains unprotected.[19]

In sum, it is relevant to keep in mind that informational flows have never respected sectoral barriers as personal data can be easily transposed for the creation of value across industries. Not only does data flow across sectors but private entities also span across multiple industries allowing them to freely shuffle around datasets internally if left unchecked. As Cohen notes:[20]

> Understanding economic power and its abuses in the era of informational capitalism requires discussions about the new patterns of intermediation and disintermediation that information platforms enable, and about the complexity and opacity of information-related goods and services.

Bewildering as the information age is, one solution may lie in constitutionalism. In advising that India follow the EU route for a strong, comprehensive legislation instead of the US sectoral/self-regulatory route to data protection regulation, Greenleaf points out the significance of privacy being a fundamental right:[21]

> The position in India … is in general principle the same as the EU: privacy is a fundamental inalienable right, with the ability of governments to derogate from it requiring considerable justification … [Data protection in India] will have to meet standards approximating those of EU laws if it is to constitute the background environment within which particular legislative interferences with privacy can be justified.

This does, of course, depend on the extent to which one sees fundamental rights like privacy being applicable in the context of the activities of private entities, either directly or in the form of a duty of the state to intervene and protect individuals from such entities.[22] While concerns may exist regarding

---

[19] Daniel Solove, 'The Growing Problems with the Sectoral Approach to Privacy Law' (*TeachPrivacy*, 13 November 2015) <https://teachprivacy.com/problems-sectoral-approach-privacy-law/> accessed 28 March 2019.

[20] Cohen (n 10) 375.

[21] Graham Greenleaf, 'Data Protection: A Necessary Part of India's Fundamental Inalienable Right of Privacy – Submission on the White Paper of the Committee of Experts on a Data Protection Framework for India' UNSW Law Research Paper No. 18-6 (2018) 4.

[22] For studies on the 'horizontal' applicability of fundamental rights, *see*, Stephen Gardbaum, 'The "Horizontal Effect" of Constitutional Rights' (2003) 102(3) Michigan Law Review 387; Mark Tushnet, 'The Issue of State Action/Horizontal Effect in Comparative Constitutional Law' (2003) 1(1) International Journal of Constitutional Law 79; Stephen Gardbaum, 'The Indian Constitution and Horizontal Effect' in *The Oxford Handbook*

the unclear position of a unified data protection regulator in its relations with various other sectoral or statutory authorities, these are not intractable issues and should be viewed in light of the increasing need for formal coordination mechanisms between different public agencies. This requirement has notably been addressed in the Draft Bill released by the Srikrishna Committee by inserting a requirement for the proposed Data Protection Authority ('**DPA**') to consult other regulators and authorities and a power to enter into agreements with them.[23]

B. Between a Public Devil and a Private Deep Sea

The potential for involvement of private organisations in processes for their own regulation is an old theme in data protection policy discourse and has been agitated in the past in the context of the divide between the US and the EU in their approaches. The debate generally outlines three different models for regulation: command-and-control, self-regulation and co-regulation.[24] The first variety refers to governmental regulation, often with a rule-based mechanism for determining how the conduct of the regulated entities should look like. It thus constrains market behaviour through enforcement and sanctions handled by a governmental authority. On the other hand, self-regulation involves private organisations creating and enforcing standards themselves, often by enhancing the conditions for market exchange. Thus, in the context of data protection, some argue that businesses have various incentives to protect privacy since they would lose customers if they didn't. In contrast with both the above, co-regulation involves sharing of responsibility between public agencies and industry for drafting and enforcing regulatory standards.[25] While this combines elements of governmental regulation with elements of self-regulation, some claim that it can be "*typified by a specific combination of state and non-state regulation*".[26] The possibility of such combinations indicates that a system of regulation with a few limited but significant elements of non-state regulation would still be considered co-regulation. The essential aspects of state regulation, including approval and oversight of the non-state actions, need not be sacrificed. What

of the Indian Constitution (OUP, 2016), ch 33; *See also*, for a leading case touching upon horizontal effects in the context of the right to education, *Society for Unaided Private Schools of Rajasthan v Union of India* (2012) 6 SCC 1, especially paras 126, 159 and 222.

[23] Draft PDPB 2018, cl 67.

[24] Dennis D. Hirsch, 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?' (2011) 34 Seattle University Law Review 439.

[25] ibid 441.

[26] Hans-Bredow-Institut for Media Research, Final Report: Study on Co-Regulation Measures in the Media Sector (2006) 17, <https://www.hans-bredow-institut.de/uploads/media/default/cms/media/cd368d1fee0e0cee4d50061f335e562918461245.pdf> accessed 10 March 2019 (emphasis added).

limited non-state aspects may be retained? A well-understood co-regulatory mechanism is for "*[government] agencies [to] collaborate with industry groups or other third parties to develop detailed substantive rules … [which] may then become enforceable law, frequently (though not always) subject to some approval or ratification by government regulators*."[27] In a world where privacy interests can be contextual, the development of 'codes of conduct' embodying best practices through collaboration with industry bodies can provide necessary sectoral adaptation where comprehensive legislations and agency-driven regulation-making are likely to fall short. What is important is that while these codes may draw upon the inputs and even the drafts of private entities, the exact form of the code that is finally approved is still the decision of the government.

At the outset, it is appropriate to note that the Report of the AP Shah Group of Experts in 2012 had endorsed the use of co-regulation in the context of privacy governance. It envisaged self-regulatory organisations voluntarily adopting standards not lower than certain national privacy principles, thus allowing "*for both high level principles to be achieved and for specific privacy standards to be enforced*".[28] Similarly, the White Paper released by the Srikrishna Committee for consultation purposes also endorsed co-regulation as "*an appropriate middle path that combines the flexibility of self-regulation with the rigour of government rulemaking*".[29] Notably, discussion of this provisional view is absent in the Committee's final Report.[30] Further discussion of the responsive regulatory model endorsed in the final Report is in the fourth section of this article. However, the adoption of a regulatory scheme that is responsive does not prevent sharing of regulatory burdens through co-regulation. Suffice it to say that the questions raised by the White Paper may still require close attention.

Whatever calls for self-regulation existed in the context of privacy have seen a decided cutback over the last two decades. In its White Paper, the

---

[27] William McGeveran, 'Friending the Privacy Regulators' (2016) 58 Arizona Law Review 959, 980; Ira Rubinstein, 'Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes' (2011) 6 I/S: A Journal of Law & Policy for the Information Society 356, 383.

[28] Report of the Group of Experts on Privacy (Chaired by Justice A.P. Shah, Former Chief Justice, Delhi High Court) (2012) <http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf> accessed 10 March 2019 at 57, 69 and 75.

[29] White Paper of the Committee of Experts on a Data Protection Framework for India (2017) <https://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf> accessed 10 March 2019 at 145-146.

[30] *See*, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018) ch 9 <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf> accessed 10 March 2019 (Srikrishna Committee Report).

Srikrishna Committee couched the debate regarding regulatory approaches as being largely captured in an EU-US binary - the distinction between a comprehensive legislation with strong regulatory powers and a market-oriented, sectoral model.[31] On the other hand, in his submissions to the Committee in response to the White Paper, Greenleaf argued that this was "*a considerable understatement and misunderstanding*" and outlined the variety of jurisdictions that had adopted privacy standards, largely in the form of comprehensive laws with high-powered regulators in the European mould. The US approach thus appears to have fallen terribly out of step with global practice[32] despite official calls for a strict, general law issuing at least as early as 2000.[33] With it, self-regulation has increasingly appeared an infeasible mode of privacy governance.[34] Even conceptually, the prospect of self-regulation in data privacy is fraught with problems given that it is unable to overcome significant market failures as a result of collective action problems (because of shared interest in personal information) information asymmetries ("*[I]ndividuals today are largely clueless about how personal information is processed through cyberspace*").[35]

The prospect for co-regulation, on the other hand, has been more promising. In the context of the US, given the initial dependence on self-regulation, Rubinstein views co-regulatory measures, including privacy safe harbours, as an effective and flexible policy instrument if well designed. She points to a holistic approach for privacy protection that relies on organisational data governance systems and internal privacy methodologies as well as reliance on best practices: a greater reliance on internal policy over state-heavy prescription.[36] Some argue that it may be appropriate for developing economies

---

[31] White Paper of the Committee of Experts on a Data Protection Framework for India (n 29) 10-14.

[32] Greenleaf (n 21) 3-4.

[33] *See*, for instance, Federal Trade Commission, 'Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress' (May, 2000), <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf> accessed 10 March 2019.

[34] Robert Gellman and Pam Dixon, 'Many Failures: A Brief History of Privacy Self-Regulation in the United States' (*World Privacy Forum*, 14 October, 2011) <http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf> accessed 10 March 2019; Ryan Moshell, 'And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection' (2005) 37(2) Texas Tech Law Review 357; Morey E. Barnes, 'Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive' (2006) 27 Northwestern Journal of International Law & Business 171.

[35] Jerry Kang, 'Information Privacy in Cyberspace Transactions' (1998) 50 Stanford Law Review 1193, 1253.

[36] Rubinstein (n 27) (safe harbour provisions seek to encourage participation in self-regulatory programs by treating an entity that has complied with the program guidelines as

to consider co-regulatory models even before adopting national legislations. The approach may best capture the benefits of a growing e-commerce sector. While one justification is that developing countries may have substantial budgetary constraints in meeting desired privacy objectives, another is that they may lack technical expertise and effective judicial systems. The stifling of innovation may be a further concern for an economy that is eager to grow.[37] In India particularly, apart from the 2012 Report of the AP Shah Group of Experts mentioned above, others have also called for the adoption of co-regulatory initiatives for data protection.[38]

In describing how regulatory institutions have been changing in recent years, Cohen characterises the models as "*procedurally informal, mediated by networks of professional and technical expertise that define relevant standards, and financialized*".[39] The rise of informal guidance, non-binding interpretations, and the development of and reliance on best practices are thus to be viewed alongside the growth of collaborative proceedings that result in consensus-based standards that may require private enforcement. While these developments align well with the unique regulatory challenges of the information age, they also create new transparency and accountability problems.[40] Greenleaf does not see any successes emerging from co-regulation efforts at all and considers them to be of no significance in Asian data privacy laws. While it had been considered a key part of Australia's regulatory approach to privacy, it appears to have been discontinued. The most significant concern is the risks involved in any scheme that allows vested interests in industry bodies to gain control over privacy regulation-making.[41] A weak track record on transparency, complaints handling and the failure in the revocation of privacy marks constitute further corroboration of general concerns.[42]

---

having complied with statutory requirements).

37 Tiffany Curtiss, 'Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies' (2016) 12 Washington Journal of Law, Technology & Arts 95.

38 Rahul Matthan and others, 'A Data Protection Framework for India: In response to the White Paper released by the Justice Srikrishna Committee' (*Takshashila Policy Advisory 2018-01*, February 2018) <http://takshashila.org.in/wp-content/uploads/2018/02/TPA-Data-Protection-Framework-for-India-RM-MV-AP-2018-01.pdf> accessed 28 March 2019, 65; Amber Sinha, 'India's Data Protection Regime must be Built through an Inclusive and Truly Co-Regulatory Approach' (*The Wire*, 1 December 2017) <https://thewire.in/business/inclusive-co-regulatory-approach-possible-building-indias-data-protection-regime> accessed 28 March 2019 (favouring an inclusive and participatory approach to rule-making, including in relation with the conduct of the Srikrishna Committee itself).

39 Cohen (n 10) 395.

40 ibid.

41 Greenleaf (n 21) 22.

42 Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2017) 524, 525.

Concerns of this nature are appropriate in light of the hazards of self-regulation. Co-regulation can easily appear like an official channel allowing for the systematic compromise of public agencies. However, it is not appropriate to define our concepts on the basis of potential outcomes that we do not like. Co-regulation as a coherent concept and regulatory approach is based on the idea of sharing regulatory burdens with private bodies and there need be no presupposition as to how much or what kind of burdens are to be shared. The EU's GDPR is seen as a very promising standard for stricter privacy protections[43] but it is easily recognisable that it contains co-regulatory features as well.[44] If one is not frightened by the very use of the term 'co-regulation', it should be accepted that well-designed elements such as the formal assessment and approval of best practices through codes of conduct, the utilisation of privacy marks or scores, mandated organisational complaints redressal systems, and reliance on private entities like data protection officers and auditors can reduce much of the regulatory burden of data protection without compromising on integrity.[45] Significant conditions for the efficacy of co-regulation are the maintenance of transparency in the approval of codes

[43] Dr. Sebastian Golla, 'Is Data Protection Law Growing Teeth? The Current Lack of Standards in Data Protection Law and Administrative Fines under the GDPR' 8(1) Journal of Intellectual Property, Information Technology and E-Commerce Law (2017) <https://www.jipitec.eu/issues/jipitec-8-1-2017/4533> accessed 28 March 2019; as described by UK's Information Commissioner: "*The new European law – the GDPR – has a global pedigree. Regulatory instruments and practices developed elsewhere in the world were embedded in its DNA during its drafting. We in the EU made vigorous efforts to learn from abroad and embrace policy instruments that were pioneered in other countries. Fair information practices and breach notification originated in the US; accountability and Privacy by Default and Design in Canada; Codes of Practice from the UK and New Zealand; and innovation measures from East Asia*." (Elizabeth Denham, Speech to the International Privacy Forum, 50th Asia Pacific Privacy Authorities Forum, Wellington, New Zealand (4 December 2018) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/12/international-privacy-forum-forum/> accessed 2 April 2019.

[44] Irene Kamara, 'Co-regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation "mandate"' (2017) 8(1) European Journal of Law & Technology <http://ejlt.org/article/view/545> accessed 28 March 2019 (noting the shift from pure command-and-control regulation to co-regulatory approaches, with the example of the development of standards for privacy management); Hirsch (n 24) (citing the scheme for codes of conduct under the EU 1995 Data Protection Directive as an instance of co-regulation worth studying further); Greenleaf (n 21) 22 (referring to and endorsing the EU GDPR's scheme for codes of conduct under Arts. 40 and 41 as "*a very highly-regulated approach*" for the introduction of "*elements of co-regulation*").

[45] Such features may be noted in the Srikrishna Committee's Draft PDPB, 2018, <https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf> accessed 28 March 2019 (*see*, cls 35, 36, 39, and 61); *See also*, Padmanabhan and Rastogi (n 4) 268 (maintaining that "*the Expert Committee veers towards co-regulation*"); in this view, it may be too quick to say that the Bill 'prohibits' co-regulation as some have noted (*see*, 'Assessing India's Proposed Data Protection Framework: What the Srikrishna Committee could Learn from Europe's Experience' (*Access Now*) 15 <https://www.accessnow.org/cms/assets/uploads/2018/10/Assessing-India%E2%80%99s-proposed-data-protection-framework-oct18.pdf> accessed 28 March 2019. The most appropriate label to employ

of conduct and opportunity for appeal from tardy complaints redressal mechanisms.[46] Such features can ensure that co-regulatory rulemaking and enforcement are being adequately overseen and checked by the state and data subjects/principals respectively. They should definitely be integrated into any implementation of the model.

IV. Accountability and Responsive Regulation

Under the Srikrishna Committee's Draft Personal Data Protection Bill, the proposed DPA is endowed with a dizzying array of powers and functions ranging from specifying 'reasonable purposes' under Clause 17 to identifying residuary categories of sensitive personal data under Clause 22, from managing data auditors to registering significant data fiduciaries, from monitoring cross-border flows of data to responding to data security breaches, from raising awareness to handling and adjudicating on complaints, and from issuing codes of practice on a host of subjects under Clause 61 to making regulations on an equally numerous set of subjects under Clause 108.[47] The substantive bases for liability on data fiduciaries also enter into considerable detail with various broad principle-based duties like purpose specification and privacy by design existing side by side with specific obligations like data breach notification and data portability. Some rights, such as the right to be forgotten, require the proposed DPA's adjudicating officers to enter into a balancing act guided by a nuanced set of criteria.[48] The sharing of burdens across alternative regulatory tracks such as co-regulation forms only one response. Two further solutions, accountability and responsive regulation, are discussed below.

A. Accountability: The Real Measure of Responsibility

In describing the contours of privacy (including decisional privacy) and assessing an anti-totalitarian conception of the right vis-à-vis state power,

---

for the Committee's model would probably be "command-and-control with co-regulatory features.")

[46] *See*, Draft PDPB 2018, cls 39 and 61 (2), (3) and (4); a crucial method by which to ensure that regulation is not controlled by regulated entities is to also involve public interest and consumer protection groups in the regulation-making process in a system of 'tripartism' (*see*, Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP, 1992), 55, 56).

[47] Draft PDPB 2018, cl 60.

[48] Draft PDPB 2018, cl 27; commentators have noted that data protection law requires intensive, detailed and discretionary regulatory action due to the large number of transactions that require regulatory decisions as well as the imperfect and incomplete information available for such decisions [*See*, Rai (n 5) 3-4].

Solove argues that we must view it as not only involving prohibitions against intrusions but also active protections:[49]

> In fact, privacy is both a positive and negative right; it is not just a freedom from the state, but a duty of the state to protect certain matters via property rights, tort law, criminal law, and other legal devices. Without protection against rape, assault, trespass, collection of personal information, and so on, we would have little privacy and scant space or security to engage in self-definition. To preserve people's ability to engage in self-definition, the state must actively intervene to curtail the power of customs and norms that constrain freedom.

This powerful account of the evolution of privacy jurisprudence draws on the steady movement that the concept has seen from negative rights as prohibitions to positive duties of protection and advancement. Though it is argued in relation with state power, this evolution is also very much in line with how we may see private power in the context of personal information. The development of data protection law, policy and regulation are core parts of the state's positive duties towards informational privacy. What form of positive duties can private entities have under data protection? These duties should appropriately be designed with a keen eye for the systemic threats created by the information age. In Cohen's astute analysis of the risk and information-oriented regulatory responses to the growing recognition of systemic threats, she finds:

> As societal understandings of harm have evolved to encompass more long-term and systemic effects of development, regulatory methodologies have evolved as well. The contemporary toolkit includes constructs oriented toward measuring, demonstrating, and responding to harms that are nascent and systemic, and those constructs are themselves predominantly informational. … As threatened future harms have become more abstract, diffuse, and technologically complex, disputes about appropriate regulatory response have become struggles for control over the modeling and representation of systemic threats and over the burden of proof required to justify regulatory actions.

The probabilistic and diffused nature of certain kinds of privacy harms is an important aspect of study relevant to data protection, with one scholar distinguishing 'subjective' and 'objective' privacy harms and even analogising them with assault and battery respectively (the former is an apprehension

---

[49] Daniel J. Solove, 'Conceptualizing Privacy' (2002) 90(4) California Law Review 1087, 1120.

or threat of the latter).[50] These informational considerations mean that individuals have considerably reduced abilities to safeguard themselves against harm through privacy self-management. This situation is considerably aggravated due to what is variously called 'infoglut'[51] or informational overload and the consequent occurrence of 'consent fatigue' due to which individuals find themselves with a surplus of material making it difficult for them to identify points of information relevant to their choices.[52] From the perspective of those handling personal data, the 'data deluge' caused by the increased availability and transfer of large quantities of data also multiplies the risk of grave data breaches.[53]

At the same time, it also means regulatory authorities have reduced abilities to detect, investigate and conclusively fix liability for the creation of diffused harms and systemic threats. Ordinary concepts of liability relying on chains of causation can be difficult to work with when proofs regarding remotely-caused harm from opaque operations lie only in ephemeral digital objects and processes. Equally, subjective harms (dependent upon a feeling of being observed, for instance) do not lend themselves to quantification and concrete evidence, making the harm component difficult to prove as well.

This is the context in which we must understand the principle of accountability. The term itself is a very mundane one, used in common parlance with little regard for any technical meaning that it could have. One may argue that it is a bit superfluous to speak of accountability as a separate coherent legal concept at all given how implicit it can be in the context of any and every legal duty. For example, consider the specific provision embedded in the GDPR regarding accountability. In Article 5(2), the principle is formulated with two prongs: first, that a data controller "*shall be responsible*" for compliance with the data protection principles in sub-article (1) of the same Article, and second, that the controller shall "*be able to demonstrate*" the said compliance.

In the context of a legal duty, the first prong can appear somewhat redundant. Isn't a regulated entity 'responsible' for compliance with its legal duties anyway? Isn't the allocation of responsibility through the concept of liability

---

[50] M. Ryan Calo, 'The Boundaries of Privacy Harm' (2011) 86 Indiana Law Journal 1131.

[51] Mark Andrejevic, *Infoglut: How Too Much Information is Changing the Way We Think and Know* (Routledge, 2013).

[52] Daniel Solove, 'Privacy Self-management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880; B. W. Schermer and others, 'The Crisis of Consent: How Stronger Legal Protection may Lead to Weaker Consent in Data Protection' (2014) 16(2) Ethics and Information Technology.

[53] Article 29 Data Protection Working Party, Opinion 3/2010 on the Principle of Accountability (2010), para 6.

the very reason why we have laws at all?[54] We should understand this formulation, however, in the context of the recent developments in the course of which it came to be adopted. For one matter, it is certainly not a new concept in data protection law. Accountability has featured in prior legal instruments and had been discussed and put into practice under the EU's 1995 Data Protection Directive before official advisories and negotiations resulted in its explicit inclusion as a provision in the GDPR.[55] Why was there a need for such an explicit inclusion? It is difficult to understand the reasoning for the first prong but it is likely traceable to the generalised anxiety created by the prospect of a 'post-privacy' age or the 'death of privacy'. As noted by the Srikrishna Committee in its White Paper:[56]

> The processing of personal data entails an increase of power (in terms of knowledge and its consequent insights) of the data controller vis-à-vis the individual. Data protection regulations are a means to help protect individuals from abuses of power resulting from the processing of their personal data. The method by which this protection was traditionally sought to be achieved was using notice and consent, offering the individual the autonomy to decide whether or not to allow her data to be processed … the concept of privacy self-management is coming under pressure given the complexity of the trade-offs between the benefits and the harms of modern technology. To offset the flaws of the notice and choice model, a key principle that has emerged is of accountability …

Accordingly, we can understand the first prong best as an attempt to rebalance power structures and the allocation of responsibility in the digital economy given the shortcomings of privacy self-management. In grappling with the problem of how to ensure the full measure of responsibility on the part of data controllers/fiduciaries, the law has come face to face with society: its intention is to *directly* demand a culture of privacy and thereby

---

[54] Thus, one finds statements such as, "*Arguably, all GDPR requirements require some accountability on the part of the controller and operational policies and procedures to give effect to the legal obligations*." (Centre for Information Policy Leadership, 'The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society' Discussion Paper 1 (of 2) (23 July 2018), 11 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf> accessed 30 March 2019).

[55] *See*, Article 29 Data Protection Working Party, Opinion 3/2010 (n 53), para 2 (for reference to the Working Party's proposals regarding explicit inclusion of the principle) and paras 16-20 (for prior precedents); *See also*, Canada's Personal Information Protection and Electronic Documents Act 2000, sch 1, para 4.1.

[56] White Paper of the Committee of Experts on a Data Protection Framework for India (n 29) 147.

engender trust in the digital economy.[57] This may have become necessary as such a privacy culture was not emerging naturally, through market competition or assortments of specific legal duties. The focus on changing cultures and mindsets may become more apparent once we start unpacking the first prong and examining what the general principle could look like in practice.

Most sources point to a similar (non-exhaustive) set of obligations that form part of the principle - the establishment of internal procedures such as review and impact assessment mechanism, written and binding internal privacy policies, identification of all data processing operations, appointment of data protection officers and executive oversight, offering data protection training to staff, establishment of internal complaints handling mechanisms, procedures in the event of security breaches etc. as well as the complete internalisation of privacy in processing operations through privacy by design and default.[58] Nonetheless, the legal nature of the obligation poses a characteristic question - if this list is non-exhaustive, how do regulated entities know what constitutes an adequate adoption of accountability measures? One assessment of the complete legal meaning of accountability under the GDPR assigns accountability components to many of its provisions, viewing the principle as one that pervades the Regulation as a whole.[59] It must be accepted that the nature of this legal rule is not the same as ordinary rules given that it is, after all, a principle. Most of its requirements in practice can be collapsible into specific obligations, just as in the case of the principle of transparency.[60] It is difficult to gauge the likelihood of residual, as-yet-unidentified obligations arising from the principle without allowing for further developments in practice and before courts.

---

[57] *See*, for instance, Centre for Information Policy Leadership (n 54) 19 (viewing accountability measures as "*essential prerequisites for trust in technology, systems and the digital market place*"); *See also*, Sebastian le Cat, 'GDPR Top Ten: #2 Accountability Principle' (*Deloitte*) <https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-accountability-principle.html#> accessed 30 March 2019 ["*(Accountability) implies a cultural change which endorses transparent data protection, privacy policies & user control, internal clarity and procedures for operationalising privacy and high level demonstrable responsibility to external stakeholders & data protection authorities.*"].

[58] Article 29 Data Protection Working Party, Opinion 3/2010 (n 53), para 41; UK Information Commissioner's Office, 'Accountability and Governance' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/> accessed 30 March 2019.

[59] Nymity, 'GDPR Accountability Handbook 2018' 8-67, <https://info.nymity.com/hubfs/Landing%20Pages/GDPR%20Handbook/Nymity-GDPR-Accountability-Handbook.pdf> accessed 30 March 2019 (tabulating a complete view of potential accountability measures for all relevant GDPR obligations).

[60] Srikrishna Committee Report (n 30) 58, 59 (noting that transparency is incumbent throughout the lifecycle of any data processing activity but also identifying specific obligations such as notice, acknowledgement of requests and publication of privacy policies).

This brings us to the second prong of the accountability principle and possibly the focal point of the obligation as a whole: the ability to demonstrate compliance. As has been discussed at length above, the entire regulatory approach for data protection must be seen in light of the unique informational considerations involved in establishing the incidence of harm (which can be in the form of uncertain, diffused threats) and further tracing the causation for the harm to the relevant entities handling personal data (which can often be done in digital format with ephemeral traces). If the first prong of the accountability principle is about the creation of a culture of privacy across and inside organisations, the ability to detect the growth or stunting of this culture is not an easy regulatory burden for any public agency to carry.

The significance of the second prong can thus be encapsulated in this statement: "*[r]esponsibility and accountability are two sides of the same coin and both essential elements of good governance. Only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed.*"[61] In a running theme from the discussion of co-regulation in the section above, one may note that a significant method of demonstrating compliance with the broad principles of a general data protection law is to adopt and comply with a specialised code of practice (eg compliance with a code of practice for the insurance sector on data storage can elaborate on a general rule in a data protection law that data may be stored for as long as is 'necessary' for a specified and legal purpose). Thus, various provisions of the GDPR explicitly state that "*adherence to approved codes of conduct… may be used as an element by which to demonstrate compliance…*".[62] It would appear that the demonstration of compliance can involve various aspects. A key first step to compliance would be the identification of specific standards that are applicable in one's industries since it might be a more fraught enterprise to go about demonstrating compliance with a broad vague standard or principle as are found throughout general data protection laws. The formulation and adoption of internal policies may also go some way in demonstrating the seriousness with which an organisation has gone about aligning its specific processing operations and priorities with data protection requirements. At the very least, it demonstrates application of mind as to the ways in which the general legal rules relate to the specific contexts of

---

[61] Article 29 Data Protection Working Party, Opinion 3/2010 (n 53) para 21 (in discussing the choice of 'accountability' for the terminology for the principle).

[62] *See*, GDPR, arts 24(3), 28(5), 32(3) and 35(8). In contrast, the Srikrishna Committee Draft Bill uses a cautious negative phrasing: "*Non-compliance … with any code of practice … may be considered … while determining whether … [a] data fiduciary or data processor has violated the provisions of this Act.*" (*See*, Draft PDPB 2018, cl 61(7).

processing by the organisation, aiding official interpreters of the rules along the way. Finally, it is clear that accountability must involve the maintenance of documentation or records. As one source declares, following the explicit inclusion of accountability in the GDPR, organisations are to "*[m]aintain more extensive records of their processing activities*" and that"*[t]his should include the purposes of the processing, the nature of the data, categories of recipients, the categories of data subjects, any transfers of personal data abroad, including documentation of suitable safeguards, timelines for erasure of data, and a general description of the technical and organizational security measures applied to the processing activities*".[63]

Viewed in this manner, the second prong does indeed look like a cross between a record-keeping requirement and a superadded burden of proof rule. This is precisely the way the Srikrishna Committee came to view the provision and this is despite there being explicit references (in the Committee's Draft Bill) to a burden of proof on the data controller/fiduciary only in the context of consent requirements.[64] After all, if compliance with the accountability principle itself ever comes up for adjudication, the evidentiary processes involved in establishing the ability to demonstrate compliance may in practice be very similar to evidentiary rules regarding a burden to prove compliance. However, what constitutes the satisfaction of this burden may at times appear unclear until there is further judicial development in the precision of our understanding of this general principle.

In light of the foregoing discussion regarding the significance of informational burdens and the difficulty of detection of data protection violations, it is considerably unfortunate that the new Bill tabled in Parliament has entirely omitted the second prong of accountability, retaining only the first prong.[65] This is certainly troubling because it may mean that the ordinary rules regarding burden of proof in evidence law for civil disputes would be applicable in data protection as well. The actual outcome of any litigation would likely be very different under the new Bill's version of accountability. If any account is taken at all as to which party has better access to evidence in a data protection dispute, some obligation regarding the ability to demonstrate compliance must be put in place.

---

[63] Hannah Crowther, 'The GDPR's Accountability Principle: A Shift in Mindset' (*Dropbox*, 20 March 2018) <https://blog.dropbox.com/topics/product-tips/gdpr-accountability-principle> accessed 2 April 2019.

[64] Srikrishna Committee Report (n 30) 164; *See also*, Draft PDPB 2018, cl 12(4) (for the provision regarding burden of proof for consent).

[65] PDPB 2019, cl 10; the Draft Bill from the Srikrishna Committee had specified that the data fiduciary "*should be able to demonstrate that any processing undertaken by it or on its behalf is in accordance with the provisions of this Act*" [Draft PDPB 2018, cl 11(2)].

B. Responsive Regulation

In critiquing the idea of co-regulation many commentators have held up an alternative model for regulation which also received the Srikrishna Committee's stamp of approval - responsive regulation.[66] However, as has been explained above, co-regulation needn't involve any significant abdication of state functions at all and may only be a method of remaining sensitive to industry practices and nuances while relying on private resources for enforcement. Responsive regulation, as shall be described below, can easily complement and act in synergy with a system containing limited co-regulatory features.

Over a couple of decades the concept of responsive regulation has received a considerable fillip as it has gained greater recognition and application.[67] The core idea behind the approach is that "*governments should be responsive to the conduct of those they seek to regulate in deciding whether a more or less interventionist response is needed*".[68] Most accounts of the theory visualise a pyramid or hierarchy of enforcement tools lying on a spectrum of strictness along which a regulator can escalate so as to ensure that "*[t]he magnitude of escalation and the punitive effect of the regulatory response corresponds to the nature of default*".[69] Thus, a one-time, inadvertent and minor breach can be dealt with quite differently from a grave and intentional violation affecting key rights or large numbers. In escalating order, the regulator can seek information, provide informal guidance, require audits, direct mitigation measures, publicly 'name and shame' an entity, demand undertakings, cause investigations and apply penalties or initiate criminal action.

Since none of the tools in the regulator's toolkit are supposed to be legally excluded in the context of any regulatory action, proponents see the approach as a key method to target enforcement actions effectively. The theory has many merits. For one, it has close linkages to robust democratic ideals of deliberative accountability. Braithwaite argues that responsive theories bring

---

[66] *See*, for forceful defences of the responsive approach for India, Greenleaf (n 21) 22-23; Beni Chugh and others, 'Effective Enforcement of a Data Protection Regime: A Model for Risk-Based Supervision Using Responsive Regulatory Tools' Dvara Research Working Paper Series No. WP-2018-01 (July 2018) <https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf> accessed 2 April 2019.

[67] For one survey of applications of the theory in practice in Australia and the rest of the world, *see*, Mary Ivec and Valerie Braithwaite, 'Applications of Responsive Regulatory Theory in Australia and Overseas: Update' RegNet Research Paper No. 2015/72 (March 2015).

[68] John Braithwaite, 'Responsive Regulation and Developing Economies' (2006) 34(5) World Development 884, 886.

[69] Chugh (n 66) 9.

democracy to bear on a larger swathe of the population, ensuring that the interpretation of rules is done within a system of "*networked governance*".[70] Similarly, the idea of responsive regulation also appeals to our deepest intuitions regarding justice and align well with the principle of proportionality in areas as diverse as constitutional, commercial and criminal law.[71]

However, in the context of the present study, a significant feature of responsiveness is the manner in which it streamlines regulatory action so as to target and respond to violations with a solid system of prioritisation in place at the outset. The regulatory state is not usually in the business of regulating cultures but when it does descend to fiddling around in such matters, it needs at hand an appropriate theory of regulation that provides it with the ability to credibly and legitimately create the threat of strict measures without actually imposing the same unless the situation warrants. Otherwise, the burden of welding together a privacy culture may prove too heavy for an effective attempt to even be made. As pointed out by Ayres and Braithwaite:[72]

> A fundamental principle for the allocation of scarce regulatory resources ought to be that they are directed away from companies with demonstrably effective self-regulatory systems and concentrated on companies that play fast and loose.

The ideas and concepts behind responsive regulatory theory have already filtered through into data protection far deeper than one might at first imagine. McGeveran enthusiastically points out that responsive regulation in the context of privacy holds many benefits including the retention of flexibility to deal with changing technology, the cost-effective discharge of

---

[70] Braithwaite (n 68) 884-886 (Braithwaite views different actors in a system of regulation acting in "*reflexively related systems*" that affect each other's behaviour simultaneously and finds that abuse of power is "*best checked by a complex plurality of many separated powers*", whether private, public or a hybrid of the two).

[71] See, *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1, para 310 ("*Proportionality is an essential facet of the guarantee against arbitrary State action because it ensures that the nature and quality of the encroachment on the right Is not disproportionate to the purpose of the law.*"); *Excel Crop Care Ltd. v CCI, Competition Commission of India* (2017) 8 SCC 47, para 92 ("*[T]he penalty cannot be disproportionate and it should not lead to shocking results. That is the implication of the doctrine of proportionality which is based on equity and rationality.*"); Andrew von Hirsch, 'Proportionality in the Philosophy of Punishment' (1992) 16 Crime and Justice 55; proportionality also features prominently in data protection law in the context of the various balancing tests that it envisages [*see*, for instance, discussions in Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC (2014)].

[72] Ayres and Braithwaite (n 46) 129 (discussing this advantage in the context of "*enforced self-regulation*"); *See also*, Braithwaite (n 68) (providing serious discussion of responsive regulatory theory in the context of capacity deficits in the developing world).

oversight duties and the consequent improvement of real world data practices.[73] Similarly, the UK's Information Commissioner's Office, arguably the leading data protection regulator in the world, makes clear in its regulatory action policy that a system of prioritisation and pragmatism is key to how it sees its own effective functioning:[74]

> [A]s issues or patterns of issues escalate in frequency or severity then we will use more significant powers in response. This does not mean however that we cannot use our most significant powers immediately in serious or high-risk cases where there is a direct need to protect the public from harm. Our approach will also encourage and reward compliance. Those who self-report, who engage with us to resolve issues and who can demonstrate strong information rights accountability arrangements, can expect us to take these into account when deciding how to respond.

In light of these developments around the world, including in developed countries with considerable state capacity, it may be justified for India to also adopt a responsive approach to data protection regulation. Indeed, the Srikrishna Committee has approved of the approach in its Report.[75] Understandably, though the Committee's Draft Bill does not contain any explicit legal mandate for the proposed regulator to take a responsive approach, the entire toolkit of powers that may be applied by the regulator appears to have been provided for.[76]

One matter that we must remain cognizant of is that a responsive approach carries with it a requirement that the regulatory authority be granted adequate discretion to be able to carry out the dynamic, context-sensitive enforcement actions that such a method entails. While the perils of regulatory discretion are well known, there is also evidence to suggest that it is a key requirement in the context of limited regulatory capacity.[77] Such findings

---

[73] McGeveran (n 27).

[74] UK Information Commissioner's Office, Regulatory Action Policy, 13 <https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf> accessed 2 April 2019; similarly, the UK Information Commissioner has declared: "… *I hope by now you know that enforcement is a last resort. I have no intention of changing the ICO's proportionate and pragmatic approach after 25th of May. Hefty fines will be reserved for those organisations that persistently, deliberately or negligently flout the law.*" [Denham (n 43)].

[75] Srikrishna Committee Report (n 30) 156-158.

[76] Power has even been specifically provided to engage in reputational sanctions through a 'name and shame' approach [Draft PDPB 2018, cl 60(2)(*w*)].

[77] *See*, Esther Duflo and others, 'The Value of Regulatory Discretion: Estimates from Environmental Inspections in India' (*MIT Economics*, 10 March 2018) <https://economics.mit.edu/files/10335> accessed 2 April 2019 (finding, in the context of environmental regulation, that random inspections reveal fewer extreme violators than inspections on the

are also corroborated in the context of other regulatory fields with broad coverage. As it happens, the growth of prioritisation approaches may also be seen in that other significant cross-sectoral regulatory mandate - competition regulation.[78]

It is understandable that we should be wary of unguided discretion in any context but the essential take away from the above discussion must be that we have to create workable systems for granting regulatory discretion in data protection while maintaining systems by which to check and guide this discretion. This is a core enterprise for Indian administrative law which seems to have had an over-emphasis on flexibility, pragmatism and adaptation and a concomitant failure to consolidate into a unified legislation with minimum standards for administrative processes such as in the US Administrative Procedure Act.[79]

An allied area of study is the question of the independence and functional integrity of a data protection regulator. This has been an important area of debate in the context of any proposed Data Protection Authority for India[80] and while it is not the subject matter of this Article, it is nonetheless a crucial problem that scholars and practitioners should direct their energies towards. For the purposes of our discussion on responsive regulation, however, one may see significant need for statutory checks on the most significant discretionary functions of a data protection regulator. In this matter, a data

---

basis of a regulator's discretion and noting the resonance of their findings with literature on limited regulatory capacity at n 6).

78 Raeesa Vakil, 'Indian Administrative Law and the Challenges of the Regulatory State' in Devesh Kapur and Madhav Khosla (eds), *Regulation in India: Design, Capacity, Performance* (Hart Publishing, 2019) 51.

79 Raeesa Vakil, 'Indian Administrative Law and the Challenges of the Regulatory State' in *Regulation in India: Design, Capacity, Performance* (Kapur & Khosla eds.) (Hart Publishing, 2019) 51.

80 Key to the debate have been the provisions in Draft PDPB 2018, cls 68 and 98 (on the appointment of adjudicating officers and government directions to the proposed regulator); to add to these problematic provisions, the new Bill tabled in Parliament has acceded even more control to the Government by allowing it to have exclusive control over surveillance activities and a stranglehold on the selection committee of the DPA [PDPB 2019, cls 35 and 42(2)] (for examples of concerns regarding of the same, *see*, Graham Greenleaf, 'GDPR-Lite and Requiring Strengthening – Submission on the Draft *Personal Data Protection Bill* to the Ministry of Electronics and Information Technology (India)' UNSW Law Research Paper No.18-83 (2018), at 2, 3 and 11; UK India Business Council, 'Data: The Foundation of Intelligent Economies' (March 2019) 29 <https://www.ukibc.com/data-the-foundation-of-intelligent-economies/> accessed 2 April 2019; *Access Now* (n 45) 10; Amba Kak, 'The Emergence of the Personal Data Protection Bill, 2018: A Critique' (2018) LIII (38) Economic & Political Weekly 12, 14-15); *See also*, for European case law on the level of independence required for data protection authorities, *European Commission v Federal Republic of Germany*, 2010 ECR I-1885, C-518/07 (CJEU) and *European Commission v Republic of Austria*, C-614/10 (CJEU).

protection statute can be seen as a contract that serves to manage the relationship between an independent regulatory authority and an elected government that is directly subject to democratic accountability.[81] One may thus note the attempts made in the Srikrishna Committee's Draft Bill to guide the discretionary functions of the DPA through various prescriptive criteria, for example, in provisions regarding consent and explicit consent (Clauses 12(2) and 18(2)), reasonable purposes (Clause 17(1)), the designation of further categories of sensitive personal data (Clause 22(2)), the right to be forgotten (Clause 27(3)), the classification of significant data fiduciaries (Clause 38(1)), and the determination of penalties and their amounts (Clause 74(4)), as well as through an illustrative list defining the concept of a privacy harm (Clause 3(21)). Other mechanisms that may appear less principle-based but potentially effective are to embed clear mechanisms by which to carry out cost-benefit analyses that are reviewable by courts on a consistent basis.[82] The merits of systematically studying the varieties of privacy harms may be of great significance here, including the recognition of diffused and cumulative harms that are easy to undervalue.

There will be no easy answers to questions regarding how we can balance the grant of discretion and independence with the requirements of constraining executive action for public good and ensuring democratic accountability. Cohen describes navigating the tension as "*charting a course between the Scylla of regulatory capture and the Charybdis of bureaucratic inefficiency*".[83] If and when regulatory practice on data protection proceeds in India, a close eye will have to be kept to ensure that decisions are made with adequate and explicit reasons that are themselves consistent across measures, sectors, entities and individuals. This kind of scrutiny of the functioning of our regulatory authorities may be the only way to marry discretion with efficiency and the protection of our rights.

V. An Eye to the Future

This study has sought to elaborate on the key unique considerations involved in designing a scheme for data protection regulation that can adequately

---

[81] For a detailed view of the considerations involved in taking this view, *see*, Roy (n 3) (treating the legislature represented by the executive as the principal and the regulatory agency as the agent in a classic principal-agent problem in which the necessary discretion of the agent needs to be constrained by employing optimal information and incentive structures).

[82] Eric A. Posner, 'Controlling Agencies with Cost-Benefit Analysis: A Positive Political Theory Perspective' (2001) 68 University of Chicago Law Review 1137; Michael A. Livermore, 'Cost-Benefit Analysis and Agency Independence' (2014) 81 University of Chicago Law Review 609.

[83] Cohen (n 10) 392.

match up to the weighty task at hand. Even after one considers all the exemptions that a data protection law usually provides for, there remains a vast array of entities that any future regulator will have to engage with. In all likeliness, data protection regulation has the widest regulatory mandate in terms of the coverage of entities and volume of transactions and functions that any regulator has ever had to take on, even considering authorities in financial and competition regulation. A successful attempt at taming the roving eyes of public and private surveillance will need more than just clever ideas, however. The project requires a serious look at the unique characteristics of personal data, informational flows and privacy harms. As has been argued above, the most significant regulatory considerations in the regulation of personal information will be informational considerations - answers to the problem of how best an agency can gather the regulatory information needed to protect personal information.

One set of information that will be needed is on-ground awareness of the ordinary practices that computer professionals employ when operating in the information economy. Apart from developing ecosystems and networks of privacy professionals with whom a regulator may engage, an important method of creating a credible threat of the detection of violations may be the initiation of schemes for whistle-blowers who may be willing to call out the illegalities of their organisation as well as the formal institution of whistle-blower awards.[84] Other avenues for the amelioration of informational concerns include the development of awareness regarding data protection amongst individuals generally and the growth of a body of research around how best to create technical safeguards for privacy as well as develop technological solutions to regulatory problems. Unlike in many other instances of Indian regulatory practice, there cannot be any devaluation of regulatory functions like awareness generation and research.

Active support and encouragement must also be given to public interest or consumer interest groups willing to organise and examine the data economy from vantage points other than commercial ones. If we want to look forward to a future where data principals/subjects in India are ready and able to defend their own privacy, the sharing of enforcement burdens cannot just be with regulated entities but also with the persons who are to be protected under the law. Illiteracy, innumeracy and the lack of technical knowledge on data processing may always be concerns going forward but

[84] For a robust scheme developed in this regard in the field of securities regulation (a field with similar difficulties in detection and investigation), *see*, U.S. Securities and Exchange Commission, Office of the Whistleblower <https://www.sec.gov/whistleblower> accessed 2 April 2019.

the entire project of data protection can be streamlined towards the activation of individuals themselves. The evolution of regulatory practice appears to be moving from prescriptive rules, certification and gatekeeping towards the promotion of innovation in an environment of data-driven transparency and accountability.[85] While the traditional scheme of paternalistic regulation seemed appropriate for a time when information was *scarce*, regulatory action can today be bolstered not just with co-regulation but also with collaborations riding on consumer and citizen activism so long as the individual is allowed to know about the future they are being thrust into. This must mean transparency on the part of regulated entities but it also requires the systematic and comparative presentation of the information needed to allow for good choices in a data economy inundated with *too much* information. Hopefully, systems such as data trust scores and consent dashboards can play a role here.[86]

A word of caution is appropriate. While the anxieties of the information age are appropriately regarding the dangers that our liberties face against the unending storm of technological innovation, it is possible that we are anxious only because we do not yet understand what we are dealing with. In 1865, the British Parliament demanded that automobiles travel at 4 miles per hour on highways and 2 miles per hour in towns and villages, that they be manned by crews of at least three persons and that one person walk 60 yards ahead of the vehicle with a red flag to warn everyone of what was coming. Though the time the law was repealed in 1896, the development of automobiles had been stifled as a result.[87] While the anxiety provoked by change is understandable, the method by which we build a society that can trust technology should not strangle innovation to death either.

And yet, as data protection law develops, it may not end up looking anything like what we might see in most areas of legal and regulatory practice. We should be ready to live with such uncertainty but we should accept change only where it promotes human welfare. Cars may carry the weight of our bodies and computers the weight of our secrets, but no one can claim that both weigh the same.

---

[85] Parker (n 4) 253-256.
[86] Srikrishna Committee Report (n 30) 36.
[87] Eggers (n 6).

Law Enforcement Access to Data in India: Considering the Past, Present, and Future of Section 91 of the Code of Criminal Procedure, 1973

*Tarun Krishnakumar**

Abstract *Developments in modern technology and the Internet have resulted in vastly greater quantities of information being stored in electronic form. In addition to gains for convenience, innovation, and the economy, this trend also means that law enforcement and other government agencies are required to increasingly turn to the digital domain to gather evidence for investigative or enforcement purposes. In the Indian context, this usually means having to rely on pre-digital era procedural powers such as Section 91 the Code of Criminal Procedure, 1973. Drawing from existing literature, case law, and developments in policy, this article seeks to conduct an analysis of Section 91 with a view towards adding to the discourse surrounding calls for its reform. It concludes that, in its current form, the provision neither adequately accounts for privacy concerns nor provides clear and certain procedures for law enforcement agencies to compel production of evidence stored in electronic form. Several principles which have developed around the provision are no longer relevant in the digital age, others have the potential to excessively invade privacy, while several others internally conflict. It would be in the interests of both individuals and law enforcement agencies to seek timely review and reform of this provision to account for modern realities.*

* Tarun Krishnakumar is a lawyer admitted to practice law in India and the United States (California). He is a graduate of the National Law School of India, Bangalore. All views expressed are personal. The developments surveyed in this article are current as of June 2019.

I. Introduction

The proliferation of the Internet, smartphones, and other digital devices has meant that an increasing amount of information – including information considered private[1] – is found in electronic form. Trends in digitisation, automation, computing, and the emergence of data-centric revenue models mean that vastly more quantities and entirely new categories of information are being generated, collected, and processed; previously transient datapoints are being stored more permanently; and there is increasing convergence of services which involve data collection. All this means that, in today's world, it is exceedingly difficult to not leave a digital footprint in ordinary course.[2]

While having positive implications for innovation, commerce, governance, and convenience, these developments also mean that an increasing amount of information relevant for law enforcement and investigative purposes is found in electronic form.[3] Alongside the availability of vastly more types and quantities of evidence for use for investigative purposes by law enforcement agencies ('**LEA**'), this data 'revolution' also raises novel questions from the points of view of personal privacy, due process, and civil liberties.[4] In several jurisdictions, this duality has triggered vigorous debates surrounding the legal standards for LEA[5] to compel production of data stored by individuals or the ubiquitous intermediaries[6] (and service providers) that process and store data on their behalves. Often these debates centre around the procedural safeguards which apply to the ability of LEA to compel production – including issues such as evidentiary standards, proportionality of production

---

1 In this context, 'private' information may be understood to include information that is personal as well as other kinds of information that is considered sensitive including trade secrets and confidential commercial information.

2 *See generally*, Bernard Marr, 'How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read' (*Forbes*, 21 May 2018), <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#52cd124260ba> accessed 19 October 2019.

3 For a balanced discussion, *see*, Matt Olsen and others, 'Don't Panic: Making Progress in the 'Going Dark' Debate' (Berk*man Center for Internet and Society*, 1 February 2016) 12 <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf> accessed 19 October 2019.

4 Olsen and others (n 3) 1.

5 For the purposes of this paper, LEA refers to police and other regulatory/enforcement agencies regulated by statute. It does not include intelligence agencies which – in India – are not created by or governed under statute.

6 For the purposes of Indian law, intermediaries are defined by s 2(*w*) of the Information Technology Act in the following terms: "'*Intermediary' with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes*".

orders, protections against self-incrimination, and the need for judicial oversight or authorisation.[7]

While several stakeholders in India have expressed concerns relating to the inadequacy of the procedural framework governing LEA access to data, the debate has been fragmented. Although significant discussion has taken place surrounding a legal framework for privacy and data protection in India,[8] there is scope for deeper examination of LEA powers under Indian criminal procedure law. Where discussions have taken place on this issue, they have largely been at the policy-level and have not deeply engaged with historical trends in caselaw or applicable legal doctrine.

Against this backdrop, this paper aims to contribute to the discourse around these issues by engaging in a legal survey of powers available to LEA under Section 91 of the Code of Criminal Procedure, 1973 ('**Cr.PC**' or '**1973 Code**') – a provision commonly used to compel production of data.[9] In addition to surveying existing research and judicial precedent, this paper attempts to draw from these principles and several related domestic and international developments – to highlight why it is timely to begin considering reforms to this provision and the mechanism under it.

II. Statutory Framework

The Indian legal regime for LEA access to data comprises a patchwork of procedural provisions from frameworks including general criminal procedure law,[10] special criminal law,[11] sectoral

---

[7] For example, in the Indian context, *see*, Rishab Bailey and others, 'Use of Personal Data by Intelligence and Law Enforcement Agencies' (2018) National Institute for Public Finance and Policy Working Paper <http://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf> accessed 19 October 2019; *See also*, Rahul Matthan, 'The Government and Big Tech Need to Meet Halfway" (*LiveMint*, 11 June 2019) <https://www.*LiveMint*.com/opinion/columns/opinion-the-government-and-big-tech-need-to-meet-halfway-1560247166819.html> accessed 19 October 2019.

[8] Most recently, these debates have centred around the Personal Data Protection Bill 2019 which is soon to be enacted by the Government of India.

[9] For example, *see*, Sahil Makkar, 'Are Private Detectives Prying on Personal Details?' (*Rediff.com*, 18 November 2013) <https://www.rediff.com/news/report/are-private-detectives-prying-on-personal-details/20131118.htm> accessed 19 October 2019; Dheeraj Fartode, 'Now, RPF can monitor Call Data Records for Probe' (*TheHitavada*, 28 April 2016) <https://www.nagpurrailwaypolice.gov.in/sites/default/files/5_11.pdf> accessed 19 October 2019.

[10] As mainly contained in the Code of Criminal Procedure 1973 (CrPC).

[11] For example, the Narcotics Drugs and Psychotropic Substances Act 1985 (NDPS Act) contains specialised procedures for search and seizure. However, where not inconsistent with provisions of the NDPS Act, provisions of the CrPC governing search and seizure will continue to apply (NDPS Act, s 51).

regulations,[12] and information technology law.[13] The framework applicable to a particular case depends on the criminal conduct that is at issue and the authority empowered to investigate it. It important to note that, in most cases, there are no specific carve-outs for access to evidence stored in digital form.[14] Powers relating to *physical* search and seizure – intended to apply to tangible objects and documents at the time of enactment – are applied in relation to electronic evidence.

Within this patchwork, this paper focuses on certain key provisions contained within the general criminal procedural framework, the Cr.PC. The reason for this scoping is two-fold. *First*, Cr.PC powers are most commonly used to compel production as they apply to the widest variety of criminal offences and are available to the widest number of authorities including police and specialised LEA. *Second*, many sectoral or special frameworks, rather than creating specialised procedures, tend to incorporate – by direct reference – provisions of the Cr.PC insofar as summons, search and seizure are concerned. While other frameworks may also provide mechanisms for LEA to access data, these provisions are not as commonly resorted to, usable only in narrowly defined circumstances (or in relation to specific offences), have onerous authorisation requirements on paper, or are available only to a small sub-set of LEA or other government authorities.[15]

Of particular relevance within the Cr.PC are provisions of Chapter VII which relate to "*Processes to Compel the Production of Things*". This Chapter is divided into two sub-chapters: "*Summons to Produce*" and – and where such summons is insufficient – "*Search Warrants*". Sections 91 and 92 pertain to summons, while Sections 93 to 98 pertain to search warrants. Sections 99 – 101 contain general guidance in relation to the manner in

---

[12] *See*, examples cited in Sunil Abraham and Elonnai Hickok, 'Government Access to Private-Sector Data in India' (2012) 2(4) International Data Protection Law 304 <https://doi.org/10.1093/idpl/ips028> accessed 19 October 2019.

[13] As mainly contained in the Information Technology Act 2000 (IT Act) as amended.

[14] A notable exception to this statement is the Income Tax Act 1961 which in its provisions governing search and seizure expressly applies to "*books of account or other documents maintained in the form of electronic record*" [Income Tax Act 1961, s 132(1)(*ii*)(*b*)]. Another example is the Information Technology Act 2000 – which principally applies to regulate conduct in the cyber domain.

[15] For example, s 69 of the IT Act authorises interception, monitoring, and decryption of any information *passing through any* computer resource in relation to a wide variety of matters. However, such powers are only exercisable upon issuance of orders by the Secretary of Home Affairs (Central Government) or the Secretary of the Home Department (State Government) to (currently ten) *agencies designated under the provision*. Only in very limited circumstances can very senior LEA officers themselves order interception under this provision. In this regard, *see*, the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009. Similarly, s 69B authorises monitoring and collection of traffic data only for cyber security linked purposes.

which searches are to be conducted. This paper will focus on Section 91 (and, to a lesser extent, Section 92) as it has been – and is likely to continue to be – the key focus of debates on LEA access to data. This is because the powers under these provisions, widely exercisable by most LEA around the country, are outdated in as much as they only apply to *physical* objects and also because Section 91 authorises LEA to *unilaterally* compel production – without the need for judicial authorisation or adversarial process.[16] To illustrate, they are extracted below (emphasis supplied):

> *91. Summons to produce document or other thing.—*
>
> (1) Whenever any Court or *any officer in charge of a police station* considers that the production of *any document or other thing is necessary or desirable for the purposes of any investigation*, inquiry, trial or other proceeding under this Code by or before such Court or officer, such Court may issue a summons, or *such officer a written order*, to the person in whose possession or power such document or thing is believed to be, requiring him to attend and produce it, or to produce it, at the time and place stated in the summons or order.
>
> (2) Any person required under this section merely to produce a document or other thing shall be deemed to have complied with the requisition if he causes such document or thing to be produced instead of attending personally to produce the same.
>
> (3) Nothing in this section shall be deemed—
>
> (a) to affect sections 123 and 124 of the Indian Evidence Act, 1872 (1 of 1872), or the Bankers' Books Evidence Act, 1891 (13 of 1891), or
>
> (b) to apply to a letter, postcard, telegram or other document or any parcel or thing in the custody of the postal or telegraph authority.

Section 92 addresses the procedure for seizure and detention of letters and telegrams in transit:

> *92. Procedure as to letters and telegrams.—*
>
> (1) If any document, parcel or thing in the custody of a postal or telegraph authority is, in the opinion of the District Magistrate, Chief Judicial Magistrate, Court of Session or High Court wanted for the

[16] For a general discussion of concerns associated with non-adversarial process to compel data production, *see*, James Orenstein, 'I'm a Judge. Here's How Surveillance is Challenging Our Legal System' (*The New York Times*, 16 June 2019) <https://www.nytimes.com/2019/06/13/opinion/privacy-law-enforcment-congress.html> accessed 19 October 2019.

> purpose of any investigation, inquiry, trial or other proceeding under this Code, such Magistrate or Court may require the postal or telegraph authority, as the case may be, to deliver the document, parcel or thing to such person as the Magistrate or Court directs.
>
> (2) If any such document, parcel or thing is, in the opinion of any other Magistrate, whether Executive or Judicial, or of any Commissioner of Police or District Superintendent of Police, wanted for any such purpose, he may require the postal or telegraph authority, as the case may be, to cause search to be made for and to detain such document, parcel or thing pending the order of a District Magistrate, Chief Judicial Magistrate or Court under sub-section (1).

On a bare reading, Section 91 enables either a court or police officer (of appropriate rank) to issue a summons or written order seeking production of any 'document' or 'thing' that is necessary or desirable for any investigative purpose. Expressly excluded from the scope of this provision are letters, postcards, telegrams, and 'other things' which are in custody of the postal or telegraph authority. Such items may only be seized by order of a judge under Section 92(1) of the Cr.PC. While Section 92(1) manifests a higher level of procedural safeguards in the form of judicial approval prior to issuance of summons, the powers under Section 91, in contrast, may be exercised by a police officer without the need for prior judicial approval.

Another distinction between the two provisions is scope. While Section 91 may be used to compel the production of seemingly anything qualifying as a 'document' or 'thing', Section 92 is more limited in scope – applying only to things in the custody of a postal or telegraph authority.

III. Setting Context: Section 91 and LEA access to Data in Practice

Despite the lack of any specific references to data or electronic evidence, Section 91 is commonly understood to be used by LEA to seek the production of data and other forms of electronic evidence in the possession of intermediaries and other persons.[17] Several authors have noted and com-

[17] Maria Xynou, 'Why 'Facebook' is More Dangerous than the Government Spying on You' (*The Centre for Internet and Society*, 19 November 2013) <https://cis-india.org/internet-governance/blog/why-facebook-is-more-dangerous-than-the-government-spying-on-you> accessed 19 October 2019; Vipul Kharbanda, 'Policy Paper on Surveillance in India' (*The Centre for Internet and Society*, 3 August 2015) <https://cis-india.org/internet-governance/blog/policy-paper-on-surveillance-in-india> accessed 19 October 2019; Elonnai Hickok and Vipul Kharbanda, 'An Analysis of the CLOUD Act and Implications for India' (*The Centre for Internet and Society*, 22 August 2018) <https://cis-india.org/

mented on this practice. For instance, Acharya has noted that the powers under Section 91 may be applied to obtain data at rest such as emails stored in an inbox or sent-mail folder.[18] Similarly, the Centre for Communication Governance has noted that Section 91 is used by LEA to access 'stored data', i.e. data at rest.[19]

While a comprehensive survey of all academic references to Section 91 is outside the scope of this paper, it may be generally acknowledged that several authors express concerns regarding the unilateral ability of LEA to access data under this provision.

In a comprehensive study, Iyengar examines this provision in the context of compelled disclosure of IP addresses. He also studies the relationship between Sections 91 and 92 and notes that it may be possible for Internet Service Providers to be considered as 'telegraph authorities' for the purposes of these provisions – entitling them to the higher standard of protection under Section 92. He also notes separately that "…*Despite their primary functions as email providers, it seems unlikely that any magistrate would interpret webmail providers like Hotmail and Google as "postal authorities" so as to be immune from police summonses under Section 91*…"[20] Overall, he concludes that – given the interpretational uncertainties involved – it would be appropriate to amend the Cr.PC to keep pace with technological developments.[21]

The Centre for Internet and Society too makes similar observations in relation to use of Section 91 to compel production of data.[22] As regards

---

internet-governance/files/analysis-of-cloud-act-and-implications-for-india> accessed 19 October 2019.

18 Bhairav Acharya, 'An Analysis of the Cases Filed under Section 46 of the Information Technology Act, 2000 for Adjudication in the State of Maharashtra' (*The Centre for Internet and Society*, 30 September 2013) <https://cis-india.org/internet-governance/blog/analysis-of-cases-filed-under-sec-48-it-act-for-adjudication-maharashtra> accessed 19 October 2019; *See also*, Amrita Vasudevan and others, 'Law Enforcement Agencies Perceptions of Gender-Based Cyber Violence – An Ethnographic Exploration of Bengaluru City Cyber Police' (*IT for Change*, January 2018) <https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Amrita-Anit-and-Nandini-.pdf> accessed 19 October 2019.

19 Centre for Communication Governance at National Law University, Delhi, 'Comments to TRAI's Consultation Paper on Cloud Computing' (2018) 17 <https://ccgdelhi.org/wp-content/uploads/2018/10/CCG-NLU-Comments-on-TRAIs-Consultation-Paper-on-Cloud-Computing.pdf> accessed 19 October 2019.

20 Prashant Iyengar, 'IP Addresses and Expeditious Disclosure of Identity in India' (2013) 9 Indian Journal of Law and Technology 1, 22.

21 ibid.

22 The Centre for Internet and Society and Privacy International, 'The Right to Privacy in India– Stakeholder Report' (27th Session — India, Universal Periodic Review, 2016) para 17 <https://privacyinternational.org/sites/default/files/2018-04/India_UPR_Stakeholder%20Report_Right%20to%20Privacy.pdf> accessed 19 October 2019.

Section 92 of the Cr.PC, a 2016 report by the organisation also briefly notes that "*…there is little judicial clarity on the subject but it may be argued that it is possible to interpret the provisions in a way that even private ISPs can be considered as postal or telegraph authorities and thus become subject to interception under this section.*"[23]

Separately, Abraham and Hickok make several notable observations about these provisions. For instance, they find that the powers under Sections 91 and 92 are exercised in preference to powers under sectoral frameworks that may also be available to certain LEA.[24] They also note that the breadth of Section 91 has meant that it has been used to request various types of communication data including the content (payload) of communications. In other words, LEA tend to ignore the heightened standards of Section 92 (which the authors suggest is more appropriate) and prefer to use generic Section 91 powers which do not require any form of prior judicial authorisation. Based on inputs from unnamed intermediaries, the authors also report that only basic subscriber information or meta-data is typically provided by intermediaries in response to Section 91 requests since 'communication data' requires a court order under Section 92. However, the authors acknowledge that it is unclear if all intermediaries follow such an approach.[25]

Within this context, in a submission made to the Madras High Court, a leading messaging platform stated that it provides basic subscriber information including "*phone number, name, device info, App version, Start date/time, connection status, last connection date/time/IP, E-mail address, Web client data*"[26] in response to Section 91 requests.

Swire, Hemmings and Srinivasan, among others, have briefly considered Section 91 in the context of cross-border data requests and the requirements of the Clarifying Lawful Use of Overseas Data Act ('**CLOUD Act**') – discussed below. In most such studies, there is general acknowledgement that Section 91 is a key provision under which LEA access to data is effected in India. Relevant to the present analysis, the authors note that "*law enforcement regularly makes use of this broad authority, even continuing to order the production of data under the Cr.PC despite stricter provisions in other specialised statutes like the IT Act and Telegraph Act.*"[27] According to them,

---

[23] ibid.

[24] Abraham and Hickok (n 12) 304.

[25] Abraham and Hickok (n 12) 304.

[26] *Antony Clement Rubin v Union of India* 2019 SCC OnLine Mad 11785 and *Janani Krishnamurthy v Union of India* 2019 SCC OnLine Mad 11785.

[27] Justin Hemmings, Sreenidhi Srinivasan and Peter Swire, 'How Stricter Procedures in Existing Law May Provide a Useful Path for Cloud Act Executive Agreements'

case law suggests "*that this authority has typically been used by the accused, complainants, and prosecutors who would petition the court to compel the production of documents at various stages of a trial.*"[28] Based on their analysis, the authors conclude that a court-issued order under Section 91 would arguably satisfy the CLOUD Act's requirement that an order be independently authorised. As discussed in more detail below, this is only one of the avenues for exercise of powers under Section 91.

Studies also point to several attempted uses of Section 91 which do not seem to flow from the text of the provision. Shora et al. note that Section 91 is often cited in takedown notices which seek *removal of content* alleged to be illegal.[29] Similar efforts to use the provision to censor online content have been noted by SFLC.in.[30]

Overall, it may be noted that several commentators have generally discussed the role played by Section 91 of the Cr.PC in relation to LEA access to data. Some have also touched upon extended uses of Section 91 and the relationship between Section 91 and 92 of the Cr.PC, while fewer have gone as far as to allude to the fact that Section 92 of the Cr.PC may be a more appropriate provision under which access to certain forms of data – such as the contents of communications – may be sought. From the above survey, it may be understood that Section 91 is widely used not only for production orders but also to order other positive acts such as takedown of content. Significantly, several authors cited above have also expressed serious doubts as to the adequacy of the safeguards contained in Section 91.

Despite the above, there has, till date, not been a detailed legal survey surrounding this provision. Much of the above writing (with exceptions) has been from a policy perspective and, therefore, is understandably issue-specific or high-level in nature. The following sections attempt to supplement this existing literature by examining the scope of Section 91 as interpreted by Indian courts. It is hoped that this analysis will be useful to those seeking to understand whether calls for broader reform of the provision are justified.

(*Cross-Border Data Forum*, 16 November 2018) <https://www.crossborderdataforum.org/how-stricter-procedures-in-existing-law-may-provide-a-useful-path-for-cloud-act-executive-agreements/> accessed 19 October 2019.

28 ibid.

29 Shehla Shora and Anja Kovacs, 'Criminalising Dissent? An Analysis of the Application of Criminal Law to Speech on the Internet through Case Studies' (*Internet Democracy Project*, 2013) <https://internetdemocracy.in/reports/criminalising-dissent/> accessed 19 October 2019.

30 'S. 91 of CrPC – the Omnipotent Provision?' (*Software Freedom Law Centre*, 19 March 2013) <https://sflc.in/s91-crpc-omnipotent-provision> accessed 19 October 2019.

IV. Section 91: Key Trends in Jurisprudence

Section 91 has been the subject of extensive judicial analysis. However, as noted by Hemmings and Sreenivasan, much of this has been in the context of applications made to a Court (under this provision) by an accused individual, complainant, or prosecutor seeking orders for certain documents or things to be produced.[31] As this piece is intended to focus on the unilateral powers of LEA to compel production under Section 91 (the likely field for future debate surrounding the provision), it would – at first glance – seem that these decisions are less germane to the present study.

However, this is not necessarily true. For one, several of these decisions enunciate broad principles regarding the exercise of powers under Section 91 generally. As such, they provide valuable guidance on the factors and principles that must also guide the exercise of compelled production powers by LEA under this provision. Further, decisions which discuss the powers of *courts* (to compel production) under Section 91 are also relevant as there is nothing to suggest that the legal standards or burdens in these cases are, in any way, distinct from those applicable to *police* exercising powers under this provision. Where the same power is exercisable in the same circumstances by two different authorities, it is likely that the similar overarching legal principles must govern. Even if this is not found to be the case, the principles applicable to court-ordered production, read in the most favourable light, will likely be required to be satisfied, as a minimum, by police in exercise of powers under this provision.

Lastly, it may also be noted that the focus of this section is on pronouncements which enunciate principles of law which are directly relevant to the application of Section 91 to data or technology. It is not intended to be a comprehensive survey of *all* decisions under Section 91 (or its predecessor provisions). For instance, issues such as the use of Section 91 against accused persons may also raise important questions relating to the right against self-incrimination guaranteed under the Indian Constitution. While potentially relevant in a context where Section 91 powers are sought to be asserted in relation to data in the possession of an accused,[32] broader issues such as these have not been covered here.

---

[31] Hemmings and others (n 27).

[32] These questions may also become relevant in relation to circumstances such as where accused persons are required to unlock or decrypt devices in which relevant data may be stored. However, in such circumstances, LEA may also be able to resort to the more stringent powers available under s 69 of the IT Act (subject to the limitations discussed above in n 15).

A. General Principles

i. Section 91 powers are very wide

It has come to be well-established that the powers and discretion available under Section 91 are extremely wide and only subject to the restriction found in the text of the provision. In *Om Parkash Sharma* v. *CBI*,[33] the Supreme Court noted that the language of the provision would:

> no doubt, indicate the *width of the powers to be unlimited* but the in-built limitation inherent therein takes its colour and shape from the stage or point of time of its exercise, commensurately with the nature of proceedings as also the compulsions of necessity and desirability, to fulfil the task or achieve the object.[34] (emphasis supplied)

In general, in relation to Section 91, a court:

> must be allowed a large latitude in the matter of exercise of discretion and unless in a given case the *Court was found to have conducted itself in so demonstrably an unreasonable manner unbecoming of a judicial authority*, the Court superior to that Court cannot intervene very lightly or in a routine fashion to interpose or impose itself even at that stage.[35]

This decision also demonstrates the legal standard that must be satisfied for an appellate court to properly interfere in a Section 91 order. These observations have been positively cited by a three-judge bench of the Supreme Court in *State of Orissa* v. *Debendra Nath Padhi*.[36] Here, the Supreme Court held that it would be proper to exercise powers under Section 91 only where it has been shown that the persons to whom the summons is addressed hold the records in question and that the same are necessary for purposes of the matter at hand. In other words, the powers under this provision cannot be used for what the Court terms a 'roving enquiry' (discussed below). Regardless, it may be generally inferred that courts and police officers have wide discretion and powers to order production under Section 91. This may particularly have relevance where an LEA order under Section 91 is questioned on grounds of being based on insufficient legal or factual grounds.

While not directly addressed, such discretion is likely to also be available to police officers exercising powers under this provision – which is intended

---

[33] *Om Parkash Sharma v CBI* (2000) 5 SCC 679 (*Sharma*).
[34] *Sharma* (n 33) 684.
[35] *Sharma* (n 33) 684.
[36] (2005) 1 SCC 568: 2004 AIR SCW 6183.

to obviate the need for police to obtain court orders on every occasion where production of any document or thing is required.[37] At the same time, while there is no requirement for judicial pre-authorisation where a police officer issues an order under Section 91, it may be erroneous to suggest that no remedies exist for a target once such an order has been issued. Apart from revision, High Courts may – under their inherent powers – interfere with Section 91 orders where good reasons exist.[38]

ii. Precondition to exercise of powers under Section 91

While the scope of Section 91 is broad, the powers under it are not absolute.[39] A precondition is the formation of a *prima facie* opinion that the document or thing sought to be produced is *necessary or desirable* for the purposes of an investigation or other proceeding under the Cr.PC. In this regard, courts have found that the document or thing called for:

> …must have some relation to or connection with the subject matter of the investigation, inquiry or trial and throw some light on the proceeding or some link in the chain of evidence…In plain words, the documents called for must have some sort of relevancy with the matter under investigation, inquiry or trial.[40]

Therefore, the key requirement to be satisfied is the relatively low standard of 'relevance'. In addition, where Section 91 powers are sought to be exercised by a lower court (Magistrate), this must be on the basis of a *judicial application of mind* to the facts of the case at hand.[41] Similarly, *prima facie* satisfaction must be arrived at by an empowered police officer prior to the issuance of an order under this provision.[42]

Practically, this means that a police officer must have had reasonable preliminary grounds to believe that the document or thing would be useful or relevant for the purposes of a proceeding under the Cr.PC. In other words – based on factors such as the nature and stage of proceedings[43] – it must have been reasonably possible for the officer to preliminarily conclude that

---

37 *CBI v V Vijay Sai Reddy* (2013) 7 SCC 452.

38 *Arun Kumar Kaushik v State of UP* 2013 SCC OnLine All 13023: (2013) 127 AIC 340.

39 Ratanlal and Dhirajlal, *The Code of Criminal Procedure* (21st edn, Lexis Nexis 2018) ch VII; *See also*, *Durga Das v R* 1942 SCC OnLine Lah 69: AIR 1943 Lah 28 *(Das)*.

40 *Subhasini Jena v Commandant of 6th Batallion, OSAP* 1988 SCC OnLine Ori 272: 1988 Cri LJ 1570.

41 Justice ML Singhal (ed), *Sohoni's Code of Criminal Procedure* (22nd edn, Lexis Nexis 2017) 497.

42 *Hussenbhoy Abdoolabhoy Lalji v Rashid B Vershi* 1941 SCC OnLine Bom 10: (1941) 43 Bom LR 523.

43 SC Sarkar, *The Code of Criminal Procedure* (11th edn, Lexis Nexis 2015) ch VII.

production of the concerned document or thing may have a bearing upon the proceeding at hand.[44]

The fact that the produced document or thing does not ultimately turn out to be relevant is of no significance.[45] *At the time of the issuance of the* order under Section 91, a court or empowered police officer must have been able to reasonably conclude that production may be necessary or desirable for investigative purposes.[46] As highlighted in the next section, this low standard may implicate the fundamental right to privacy, as recognised by the Supreme Court in the *Puttaswamy* decision.[47] Correspondingly, without reform, exercise of powers by LEA under this provision may be subject to increasing levels of judicial scrutiny and be set aside on privacy grounds – potentially imperilling evidence collection and investigative functions.

iii. Section 91 requires a written order to be issued by a police officer.

A procedural safeguard that has been built into Section 91 is the need for a written order where a police officer exercises powers under this provision. Within this context, courts have found that a verbal order or instruction issued to any person to produce a document or thing would not suffice.[48] In *Durga Das* v. *Emperor*, the Lahore High Court, in setting aside an order issued under Section 94 of the Code of Criminal Procedure, 1898 ('**1898 Code**')(analogous to Section 91 of the 1973 Code), observed (speaking through Din Mohammad J.):

> …Further I cannot subscribe to the proposition advanced on behalf of the Crown that under Section 94 discretion is vested in a police officer' to issue a written order or not and that if he so chooses, he can demand the production of books in any manner that he likes. If this were so, the provisions of law as contained in Section 94 would be rendered nugatory. The word used is no doubt 'may' but this word has not been used in the sense in which counsel for the Crown takes it to be. It merely means that if a police officer makes up his mind to issue an order to the person concerned, he must do it in writing. Any other interpretation would defeat the object of the Legislature in enacting this provision...[49]

---

[44] *Nizam of Hyderabad v AM Jacob* (1892) ILR 19 Cal 52, 64 (*Jacob*).
[45] *Jacob* (n 44) 64.
[46] Durga Das Basu, *Criminal Procedure Code, 1973* (5th edn, Lexis Nexis 2014).
[47] *KS Puttaswamy v Union of India* (2017) 10 SCC 1.
[48] Basu (n 46); *See also*, *Das* (n 39).
[49] *Das* (n 39) para 6.

Further, it is well-accepted as a general principle of law that, where a statutory provision prescribes a particular procedure in which a power is to be exercised, no deviation from the same is possible. For instance, the Supreme Court in *State of U.P.* v. *Singhara Singh*,[50] explained this rule in the following terms:

> The rule adopted in *Taylor* v. *Taylor*[51] is well recognised and is founded on sound principle. Its result is that if a statute has conferred a power to do an act and has laid down the method in which that power has to be exercised, it necessarily prohibits the doing of the act in any other manner than that which has been prescribed. The principle behind the rule is that if this were not so, the statutory provision might as well not have been enacted.[52] (internal citations omitted)

Therefore, an order issued under Section 91 which is not in writing is likely to be liable to be set aside solely on this ground. In the context of digital evidence sought to be produced, where concerns regarding grounds of proportionality arise, the written order ensures, at the very least, that there is a decision which may be challenged before higher courts.

iv. Non-compliance with order under Section 91

There is no doubt that an order issued under Section 91 is mandatory. The failure to produce a document in pursuance of a Section 91 order would at least amount to the offence of "*failure to produce a document before a public servant by a person legally bound to produce*". Under Section 175 of the Indian Penal Code, 1860, this is punishable with simple imprisonment (for one month), or fine of INR 500, or both.

These negligible penalties for conduct which may have the potential to obstruct or derail an entire criminal investigation only serves to buttress the case for review and reform of Section 91.

---

[50] *State of UP v Singhara Singh* 1964 AIR SC 358 *(Singhara Singh)*.
[51] (1875) LR 1 Ch D 426.
[52] *Singhara Singh* (n 50) para 8.

B. Principles Specifically Relevant to the Production of Data

i. Section 91 orders may be issued to individuals/entities or those holding items on their behalf

An interesting manner in which powers under Section 91 have been interpreted is that orders under the provision need not only be directed to individuals ('**target individuals**') who have in their personal possession, documents or things. Courts have interpreted the powers under this provision to extend to the production of documents and things which are in the control of an individual who is holding the same on behalf of the target individual. As per the author Sohoni:

> The instrument need not be in the actual possession of the party; it is enough if it is his power, which it would be if it were in the hands of a person in whom it would be wrongful not to give up possession to him. But he must have such right to it, as would entitle him not merely to inspect, but to retain it.[53]

For instance, even if an online service provider or intermediary was holding data or information on behalf of an individual, the same would be required to be produced. Such an approach may have crucial implications in the digital era where vast troves of information are stored by third party intermediaries on behalf of individuals.

At the same time, the Supreme Court has found that – where a non-party (to a proceeding) is called upon to produce any document or thing – such a summons or order would not amount to an 'interlocutory' order as a non-party would not have an opportunity to challenge such an order upon completion of proceedings (for example through appeal). Therefore, it was found that such non-parties could maintain revision petitions against such orders[54] – a remedy that is not ordinarily available against interlocutory orders. This line of reasoning has implications for proceedings where intermediaries are themselves not accused or subject of investigation in any matter. In such cases, intermediary entities would retain standing to challenge Section 91 orders where sufficient grounds exist.

---

[53] Singhal (ed) (n 41) 499.

[54] *Parmeshwari Devi v State* (1977) 1 SCC 169: AIR 1977 SC 403.

ii. Inconvenience not a ground for non-compliance with Section 91 order

Where a court or police officer issues an order under Section 91, inconvenience that may be occasioned by compliance with such an order is not a valid excuse for non-compliance. In *Surendra Mohan* v. *K.P.M. Tripathi*,[55] the Allahabad High Court refused to interfere with a Section 91 order issued by a police officer, holding:

> Merely because an order made by the Investigating Officer to produce books of accounts and other things would cause inconvenience to the person from whom it is summoned, it could not be said that the order is beyond the purview of Section 91. Under Section 91 of the Cr.P.C. it is for the Investigating Officer to decide as to whether a particular document or any other thing is necessary or desirable for the purposes of investigation or not. Since there is no material before us to show that the summons was issued by Respondent No. 1 with mala fide intentions, we cannot hold it to be beyond Section 91.

In light of this principle, it may be difficult for individuals or intermediaries who are recipients of a Section 91 order to argue that compliance is overly burdensome or onerous. Where the threshold for production has been met, recipients are bound to produce the documents or things sought. However, it remains an open question of how a court would consider arguments relating to impossibility (rather than inconvenience) to produce data, for example in relation to requests for contents of end-to-end encrypted communications.[56]

iii. Section 91 cannot be used to compel acts other than production

While the text of Section 91 is clear in that it is a means to compel production of *documents* or *things* that may be relevant to an investigation, reports by various organisations (supra) suggest that LEA have attempted to use Section 91 to issue orders requiring positive or negative actions such as the takedown of online content.

---

[55] *Surendra Mohan v KPM Tripathi* 1985 SCC OnLine All 1040: 1986 Cri LJ 1324.

[56] This issue is the subject-matter of ongoing litigation involving various social media platforms before the Madras High Court - WP Nos. 20774 and 20214 of 2018 SCC OnLine Mad 11785 (Madras High Court); *See*, Sameer Sachdeva, 'Impossible to Track Sender of Message due to Encryption: WhatsApp Tells Madras High Court' (*Firstpost*, 11 June 2019) <https://www.firstpost.com/tech/news-analysis/impossible-to-track-sender-of-message-due-to-encryption-whatsapp-tells-madras-high-court-6793561.html> accessed 19 October 2019.

Courts, interpreting previous versions of Section 91 have clearly concluded that this provision would not authorise such actions.[57] In *Prafulla Kumar Deb* v. *Suresh Chandra De*,[58] the Gauhati High Court set aside an order of the Magistrate restraining certain payments through an order under Section 91. The High Court, in relation to Section 94 of the 1898 Code, observed as follows:

> …All that the section authorises is that a document or thing necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under the Cr. P.C. may be ordered to be produced. Stopping of payment of certain bills presumably with a view to passing some order with regard to the amount due, to the accused at the termination of the proceedings is evidently not covered by this section….

Similarly, courts have also found that an order directing a bank to prevent an accused from operating his account was not something that could be authorised under *any* provision of the 1898 Code.[59] By implication, it follows that no such order could have been issued under Section 94 – the equivalent to Section 91 of the 1973 Code.

In *Jagdish Prasad Sharma* v. *State of Bihar*,[60] the Patna High Court considered the question of whether an order under Section 91 could compel conversion of the form of things or compel production of a document or thing in a form different to which it ordinarily exists in. In this case, a Magistrate issued an order under Section 91 requiring two bank managers to convert deposited monies into A/C payee drafts in the names of certain individuals. The High Court, setting aside this order, observed:

> …Evidently this section does not authorise the court to direct any person to convert the cash into a Bank draft and that also in the name of a person different from that in whose name the accounts stand. The words used in the section are 'document or thing' which are said to be in possession of the person who is being directed to produce the same. Apparently, this section does not authorise the Magistrate to direct that person to convert the 'thing' in a form different from that in which it was in his possession, Evidently, Section 91 was intended to give an aid in the investigation and trial of the offence under consideration and not for facilitating the disposal of the property involved…So, by this order, the learned Magistrate has not given direction for mere

---

[57] Basu (n 46).
[58] *Prafulla Kumar Deb v Suresh Chandra De* 1950 SCC OnLine Gau 52: AIR 1952 Assam 24.
[59] *Makhan Lal Chatterjee v Emperor* 1935 SCC OnLine Cal 258: (1935) 164 Ind Cas 377.
[60] *Jagdish Prasad Sharma v State of Bihar* 1987 SCC OnLine Pat 258: 1988 Cri LJ 287 (*Sharma*).

> production of the thing or document, but has asked the Managers to produce the same in a different form altogether, which, I am afraid, he was not authorised to do in terms of Section 91 of the Code.
>
> 6. Thus, it is apparent that the learned Magistrate has exceeded his jurisdiction in passing the impugned order, as Section 91 did not authorise him to pass such an order. He could, if necessary, in the interest of trial, direct the Managers concerned to produce the document or thing which he considered necessary to be produced in court, but he could not direct them to change the form of the thing sought to be produced.

This makes clear that Section 91 cannot be used by a court or police officer to compel acts other than the mere production of documents or things. Within this context, guidance offered by key documents such as the (now dated) Data Security Council of India/Deloitte Cyber Crime Investigation Manual – that Section 91 may be used to issue preservation notices/orders– would appear to be *prima facie* incorrect.[61]

Further, an order mandating production cannot require the recipient to fundamentally alter the nature or character of the concerned document or thing prior to production. The powers of magistrates and police officers are circumscribed by the provisions of the Cr.PC and they must act within its four corners.[62] It would be difficult for LEA to justify the use of Section 91, in its current form, to order actions other than production – including takedowns and other positive acts such as blocking or, in an extreme case, key-word based filtering of communications.[63]

iv. 'Documents' and 'Things' refer to *physical* objects

While the 1973 Code itself does not define the term 'document' for the purposes of Section 91, its meaning may be drawn from other contemporary statutes which provide indications as to its general understanding. For instance, the Indian Penal Code, 1860 in Section 29, defines a 'document' in the following terms:

> The word 'document' denotes any matter expressed or described upon any substance by means of letters, figures or marks, or by more than

---

[61] Data Security Council of India and Deloitte, 'India's First Cyber Crime Investigation Manual' (2011) 32, 46 <https://jhpolice.gov.in/sites/default/files/documents-reports/jhpolice_cyber_crime_investigation_manual.pdf> accessed 19 October 2019.

[62] *Sharma* (n 60) paras 5 and 6.

[63] Joseph Menn, 'Yahoo Secretly Scanned Customer Emails for U.S. Intelligence – Sources' (*Reuters*, 4 October 2016) <https://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT> accessed 19 October 2019.

> one of those means, intended to be used, or which may be used, as evidence of that matter.

Section 3 of the Indian Evidence Act, 1872, also defines a document in similar terms:

> 'Documents' means any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter.

This approach to definition is also found in Section 3(18) of the General Clauses Act 1897. Based on these, it may be observed that there has been a fairly consistent approach to defining 'document' within Indian law. Given that the Cr.PC was enacted in 1973, it is unsurprising that the term 'document' was originally intended to be restricted to a physical document. However, more recently, Indian courts have been open to interpreting the term 'documents' broadly to even include the *electronic contents* stored on various physical media (such as CDs or memory cards) in certain contexts.[64] As discussed below, this trend likely upsets the balance of (LEA and private) interests deemed appropriate by the framers of the Cr.PC and provides further justification for a timely review of Section 91.

In contrast, courts have also suggested that the powers under Section 91 would only extend to the production of *physical* 'things'. In relation to Section 94 of the 1898 Code, the Madras High Court in *T. Subbiah* v. *S.K.D. Ramaswamy Nadar*[65] held, in obiter:

> Section 94, Criminal P.C., will apply only to cases where the Court requires the production of any document or other thing necessary or desirable for the purpose of any investigation, inquiry, trial or other proceeding under the Criminal P.C. In this case, the summons was not issued to the petitioner for the production of any document or any other thing. *The word "thing" referred to in Section 94, Criminal P.C. is a physical object or material and does not refer to an abstract thing.* It cannot be said that issuing of summons to a person for the purpose of taking his specimen signature or handwriting is for the production of any document or a thing contemplated under Section 94, Criminal P.C. (emphasis supplied)

---

[64] For example, in relation to s 207 of the CrPC, *see*, general discussion in *P Gopalakrishnan v State of Kerala* 2018 SCC OnLine Ker 3244.

[65] *T Subbiah v SKD Ramaswamy Nadar* 1969 SCC OnLine Mad 45: AIR 1970 Mad 85.

While the above is not dispositive on the application of Section 91 to data and electronic information, these observations provide insight into how compelled production powers have been understood over time. The provision, in its present form, was undoubtedly only intended to apply to physical documents and objects. Therefore, the procedural safeguards under Section 91 have to be understood to be limited to the context of production of such classes of physical documents and things which originally fit within the definitions above.

While it may be possible to interpret the terms 'document' and 'thing' progressively to include electronic material, such an approach may be ill-advised as it would seek to apply procedural safeguards formulated in the context of physical objects to the electronic domain – where production orders may lead to production of far more material and be significantly more invasive. Such an approach to interpretation would also distort the internal balance between LEA and private interests that were considered appropriate by the framers of the Cr.PC. Further, as discussed in the section below, several considerations extraneous to the text of the Cr.PC may also necessitate revaluating this balance.

v. Roving enquiries are not permitted under Section 91

Courts have consistently held that Section 91 powers cannot be used for 'roving' or 'fishing' expeditions. In practice, this means that the particular document or thing to be produced as well as the person in whose possession the same lies must be clearly specified in an order issued under Section 91.[66] In other words, a 'general direction' to produce all papers relating to any subject will not be enforceable. In *Prankhang* v. *King-Emperor*,[67] the following observations were made on this point:

> …We desire again to point out that the law does not empower a police officer to search an accused's house for anything but the specific article which has been or can be made the subject of summons or warrant to produce. A general search for stolen property is not authorised, and the law cannot be got over by using such an expression as 'stolen property relevant to the case.' Such expressions are vague and misleading and the terms of the law are extremely specific…

As followed in subsequent cases, the document or thing called for must be specified.[68] As discussed below, this reading could raise several issues when

---

[66] *Lotan Bhoji Patil v State of Maharashtra* 1974 SCC OnLine Bom 133: 1975 CriLJ 1577.
[67] *Prankhang v King-Emperor* 1912 SCC OnLine Cal 7: (1911-12) 16 CWN 1078.
[68] Sarkar (n 43).

applied in relation to evidence stored electronically. For instance, it is unclear if a general order to produce all data relating to a specific incident or stored in a specific device would be enforceable. Further, where data is concerned, there is a higher likelihood that a non-particularised or vague order would result in the collection of exponentially more information than a similar order applied in the physical domain.

vi. Privacy as a consideration while issuing orders under Section 91

The level of procedural safeguards included suggest that privacy was not a core consideration of the drafters of Section 91. While there is no doubt that individuals carry far more information on devices like smartphones today, it was still possible for significant amounts of information to be held in physical form in the pre-digital era. A useful analogy concerns a personal diary – which, under most circumstances, could be said to contain significant amounts of personal or intimate information. This analogy was used by the United States Supreme Court in the seminal *Riley* v. *California*[69] case:

> A decade ago police officers searching an arrestee might have occasionally stumbled across a highly personal item such as a diary.…But those discoveries were likely to be few and far between. Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives— from the mundane to the intimate.…Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.[70] (internal citation omitted)

The fact that Section 91 contained no carveouts for any specific types of sensitive documents or things (such as a diary) would suggest that privacy was not a key consideration at the time of drafting this provision. Or alternatively, that LEA interests in investigation and security were intended to, as a matter of policy, prevail over individual interests such as privacy.

Despite this, with developments in technology and data collection, there seems to have been a handful of cases where courts have *read in* privacy requirements in relation to the exercise of Section 91 powers. In *K. Sureshkumar* v. *C. Sandhumani*,[71] the Madras High Court upheld the order of a lower court declining to order Vodafone to produce "*all call lists and*

[69] *Riley v California* 2014 SCC OnLine US SC 71: 189 L Ed 2d 430: 134 S Ct 2473: 573 US (2014).

[70] Riley (n 69) 2490.

[71] *K Sureshkumar v C Sandhumani* Crl OP No. 20741 of 2015 and MP No. 1 of 2015, decided on 18 August 2015 (Mad).

SMS messages" emanating from the mobile number of an individual. The Court held:

> 5. It is seen that for invoking Section 91 Cr.P.C., the petitioner should first satisfy the Court that such a record is available with the person and that the said record is necessary or desirable for the purpose of the case. In *State of Orissa v Debendra Nath Padi*[72], 2004 AIR SCW 6183, the Hon'ble Supreme Court has held that provision of Section 91 Cr.P.C., cannot be used for a roving enquiry.
>
> 6. In this case, the petition filed by the petitioner itself, does not disclose how the SMS details and call details of the complainant is necessary for the just decision of the case. That apart, such call details and SMS details will invade into the privacy of an individual, guaranteed by Article 21 of the Constitution of India and that cannot be infringed via Section 91 CrP.C.

In an analogous fact situation, where the call details and SMS records of an individual were sought to be summoned, the same judge held in *P. Karpagam* v. *N. Mahendran*:[73]

> 4. In the considered opinion of this Court, call details of a person cannot be summoned, just like that at the mere asking, as that would invade the privacy of a person. In the facts and circumstances of this case, especially in a prosecution under Section 138 of Negotiable Instruments Act, call details of the complainant will in no way advance the case of the accused. Hence, this petition is devoid of merits and accordingly dismissed.

The Delhi High Court has also arrived at similar conclusions concerning cell phone records. Interestingly, in *Attar Singh* v. *State (NCT of Delhi)*,[74] the Court affirmed the privacy of a police officer whose call and locational details were sought by an accused for exculpatory purposes. The High Court affirmed and refused to interfere with the decision of the lower court which dismissed the application of the accused:

> …on the ground of non-maintainability as the documents sought to be produced were not part of the charge-sheet and the details of personal telephone of IO/Witness of the case would amount to intrusion in the privacy of the investigating officer.

---

[72] (2005) 1 SCC 568: 2004 AIR SCW 683.

[73] *P Karpagam v N Mahendran* Crl OP No. 12961 of 2016 and Crl MP No. 6702 of 2016, decided on 29 June 2016 (Mad).

[74] *Attar Singh v State (NCT of Delhi)* 2016 SCC OnLine Del 3907.

On revision, the concerned Sessions Court partly dismissed the application by:

> …allowing the preservation of the call data record and location chart of Mobile No. 9818851024 of the petitioner. However, the learned Judge declined to preserve the call data record and location chart of Investigating Officer on the ground of fishing inquiry and intrusion in the privacy of I.O.

Despite the petitioner-accused limiting the request to information concerning two days and affirming that the data summoned could be kept in a sealed cover, the application was refused. The High Court in dismissing the petition, found that the lower court had issued a reasoned order and that there was no cause for interference with the same.

Therefore, it would be wrong to state that there have been no occasions where privacy has been considered in relation to the exercise of powers under Section 91. These decisions, while being the exception rather than the norm, are notable for the fact that they were issued prior to the decision of the Supreme Court in *Puttaswamy* which, with finality, affirmed (or arguably, *reaffirmed*) the constitutional status of the right to privacy under Article 21 of the Constitution of India.

V. The Future of Section 91: What May Lie Ahead

The section above likely constitutes one of the first surveys of the legal principles laid down historically by courts in relation to Section 91 (and its antecedent analogues) insofar as it may be relevant to the compelled production of data in the modern context.

While these principles provide the basis for the discussion to follow, namely what the future may hold for Section 91 of the Cr.PC, questions of judicial interpretation and analysis are unlikely to operate in a vacuum. Equally relevant are legal and policy developments taking place on connected issues such as privacy, data protection, and criminal procedure. Some of these most prominent developments are discussed below. Regardless of how these factors ultimately come to manifest, it is clear that pressing questions remain in relation to the need to reform and review the mechanism under Section 91. As it currently stands, the provision is not efficient to properly serve either individual nor LEA interests.

A. Developments Surrounding the Right to Privacy

A key development which will likely affect the exercise of powers under Section 91 going forward and which calls for its reform is the decision of the nine-judge bench of the Supreme Court in the landmark *Puttaswamy* case where the right to privacy was affirmed to be a fundamental right under the Constitution of India.[75] As per the majority judgment:

> A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the three-fold requirement of *(i)* legality, which postulates the existence of law; *(ii)* need, defined in terms of a legitimate state aim; and *(iii)* proportionality which ensures a rational nexus between the objects and the means adopted to achieve them;[76]

Within this context, it remains to be seen if the powers under Section 91 – especially where employed unilaterally by police – would satisfy the test of being fair, just, and reasonable. The broad discretion provided to police to issue orders under Section 91, with no guarantee that privacy will be considered as a ground,is likely to be of specific concern.

In *Puttaswamy* decision, the Supreme Court also seemed to reject the third-party doctrine. Here, the Court appeared to approve the ruling in *District Registrar and Collector* v. *Canara Bank*[77] which it read to hold that:

> the right to privacy is construed as a right which attaches to the person….[it] is not lost as a result of confidential documents or information being parted with by the customer to the custody of the bank" and that "…parting with information (to the bank) does not deprive the individual of the privacy interest.[78]

These observations suggest that orders under provisions such as Section 91 – when addressed to intermediaries – must satisfy the same standards as in cases where they are issued directly to the target individual. In other words, as far as personal privacy is concerned, a lower standard will not

---

[75] *Puttaswamy* (n 47).
[76] *Puttaswamy* (n 47) para 325 (Section T) of Majority judgement.
[77] *District Registrar and Collector v Canara Bank* (2005) 1 SCC 496.
[78] *Puttaswamy* (n 47) para 77 (Section H) of Majority judgement.

likely apply in relation to information entrusted by individuals to third parties such as banks, intermediaries or other organisations.

While there have been instances where Indian courts considered privacy as a ground for interference with Section 91 orders, these have been far and few between. In a post-*Puttaswamy* era, it is likely that this approach will change – with parties more regularly raising privacy-based challenges to orders issued under Section 91. The trickle-down effect of this will also mean that lower courts while issuing orders under Section 91 – will be more likely to consider the impact of summons to produce documents or things, on privacy.

However, likely most contentious will be the application of *Puttaswamy* to the exercise of Section 91 powers by a police officer unilaterally through written order, i.e. without court intervention. It remains to be seen whether a written order issued by a police officer – without any form of judicial authorisation would withstand the test of being "*fair, just and reasonable*" in cases where personal privacy is at issue. The risk of an adverse ruling on this point from an appellate court may result in LEA moving from the issuance of orders unilaterally to approaching courts more often to issue summons where the production of particularly sensitive information is sought. While several possible outcomes exist, none will result in clarity over the provision (and its limits) for either individuals or LEA. For clear and efficient process in the long-term, which ensures respect for privacy and provides a workable mechanism for LEA, legislative review and reform of Section 91 is likely to be required.

Such reform must consider whether safeguards deemed acceptable in 1973 would continue to be appropriate today in light of technological and policy developments. More so as the Court in *Puttaswamy,* at several points, expressed concern over the large-scale data collection by private entities in the digital age. It would be interesting to see if arguments drawing upon these concerns, to argue that Section 91 provides too low a standard of safeguards in production orders, would succeed. Lastly, with the Government in the process of enacting the Personal Data Protection Bill, the interplay between Section 91 powers and this framework is likely to raise several novel issues.

B. Reform to Facilitate Evidence Collection Efforts

Several policy considerations from LEA perspectives may also influence the desirability of reforms to Section 91 of the Cr.P.C.

i. Reform to facilitate cross-border data requests

Of these, a key driver is likely to be the difficulties experienced by Indian LEA in relation to ordering production of data stored in foreign jurisdictions. Presently, Indian LEA must follow the procedure set out in Mutual Legal Assistance Treaties ('**MLATs**') between India and the state from which production is sought. In practice, the complex forwarding mechanism involved and the inadequate resourcing of federal agencies have led to an average delay of 10 months (with exceptions) for obtaining evidence under MLATs.[79] Despite international consensus on the urgent need for reforms to this framework,[80] concrete alternatives for the way forward have yet to emerge.

One proposal that has been gaining traction is the Clarifying Lawful Overseas Use of Data Act ('**CLOUD Act**') which came into force in the United States in March 2018. The CLOUD Act provides an alternative to MLATs for countries seeking production of data stored by US-based companies for predefined investigative purposes. Specifically, the CLOUD Act authorises the U.S. Government to enter into bilateral agreements for cross-border production orders with foreign governments whose legal frameworks satisfy certain criteria. In essence, a foreign government which qualifies under CLOUD Act criteria (and with which a bilateral agreement has been entered) will be permitted to directly serve production requests (through designated LEA) on US-based entities – circumventing the MLAT mechanism.

Of the various criteria required to be satisfied by foreign governments, several pertain to the substantive and procedural legal safeguards which will govern data production requests under the law of the foreign jurisdiction. The following criteria are particularly relevant to issues arising under the 1973 Code and in relation to Section 91:

- Under the CLOUD Act, it is required to be agreed by a foreign government that any order issued by such foreign government *inter alia* "*shall be subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order;*"[81]

---

[79] The President's Review Group on Intelligence and Communications Technologies, *Final Report: Liberty and Security in a Changing World* (2013) 227 <https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf> accessed 19 October 2019.

[80] David P Fidler, 'Cyberspace, Terrorism and International Law' (2016) 21(3) Journal of Conflict and Security Law 475 <https://academic.oup.com/jcsl/article/21/3/475/2525373> accessed 19 October 2019; Andrew K Woods (Global Network Initiative), 'Data Beyond Borders – Mutual Legal Assistance in the Internet Age' (2015) 1 <https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf> accessed 19 October 2019.

[81] 18 USC, s 2523(*b*)(4) (2018).

- Under the CLOUD Act, for a foreign government to be eligible to enter into an executive agreement with the United States, it must be able to demonstrate that its legal system "*affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement;*"[82]
- Further, a factor to be considered in evaluating whether a foreign government's legal system meets the requirements of the CLOUD Act is whether the concerned government "*has adequate substantive and procedural laws on cybercrime and electronic evidence, as demonstrated by being a party to the Convention on Cybercrime, done at Budapest November 23, 2001… through domestic laws that are consistent with definitions and the requirements set forth in chapters I and II of that Convention.*"[83] India not being a party to the Convention on Cybercrime, must show equivalency of its extant framework to the standards under the Convention. One such standard is that various law enforcement powers including preservation, data production, and interception be subject to safeguards such as "*judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.*"[84]

Despite the immediate relevance of these requirements to the Section 91 debate, it must be noted that there are several other requirements of the CLOUD Act which are not presently satisfied by Indian law.[85] That said, there may be ways to satisfy the CLOUD Act requirements without substantive reforms to Section 91. For example, as Hemmings and Sreenivasan have suggested, it may be possible for the Indian government to mandate that all requests to be made under a CLOUD Act agreement be routed through courts (as opposed to being unilaterally issued by LEA). Therefore, much of this discussion may be presently academic. However, if India is seeking a more expeditious mechanism for enforcing cross-border data requests, review (and potentially reform) of Section 91 would likely be a necessary precondition.

---

82 18 USC, s 2523(*b*)(1) (2018).
83 18 USC, s 2523(*b*)(1)(B)(*i*) (2018).
84 Convention on Cybercrime 2004, art 15(2).
85 For an analysis of some of these requirements, *see,* Hickok and Kharbanda (n 17).

ii. Reform to clarify LEA powers

In addition to the above, from a LEA perspective, there may be several compelling practical reasons to push for reform to the mechanism under Section 91. For instance, as mentioned above, the current mechanism of orders under Section 91 does not empower police or courts to issue data preservation requests given the inability to issue positive commands under Section 91. The lack of such powers may lead to loss of critical evidence from an investigative or prosecutorial viewpoint.

Another issue on which no clarity has emerged is territorial jurisdiction. It is presently unclear if a police officer – acting under Section 91 – may order production where data is stored outside his district, city, or state. This issue assumes relevance particularly in the context of the rise of cloud computing and remote services which typically result in data being stored within certain metropolitan areas in the country.

Lastly, a key limitation of Section 91 is the negligible framework for penalties for non-compliance with an order or summons issued under the provision. Presently, non-compliance by a non-party to a proceeding is likely to be prosecuted under Section 175 of the IPC in addition to potential proceedings under contempt powers where a court-issued order has been violated. Penalties under this provision may be up to simple imprisonment (for one month), or fine of INR 500, or both. Today, when investigations can turn entirely on electronic evidence, courts may need broader discretion to levy stricter penalties for non-compliance with validly issued production orders.

Therefore, the next iteration of Section 91 may require stricter inbuilt penalties in the form of fines and imprisonment. However, such amendments will only be appropriate where broader reform results in more balanced powers under Section 91.

C. Other Interpretational Issues

A key driver of reform is likely to be the increase in the number of interpretational roadblocks surrounding Section 91. As the analysis above shows, several existing trends in interpretation are not necessarily internally consistent. Further, increased demands for compelled production of data will result in new challenges for LEA.

i. Conflicts of existing interpretations

Under the first category of issues: Section 91 does not lend itself to easy application to data stored electronically. Under one branch of cases (with exceptions), it seems likely that the provision – based on its text – applies only to *physical* objects – and not intangibles. On the other hand, caselaw suggests that orders under Section 91 must be specific and particular in scope. Reading these two principles together may produce anomalous results.

Where *certain* data is sought to be produced, it may be open for the target individual to argue that the production of data– as an intangible – is not recognised within the ambit of Section 91 at all. In order to get around this objection, LEA may use Section 91 to compel production of the relevant physical device or hardware (such as hard disk) housing the data in question. Further, as certain courts have accepted, it may be possible to show that 'documents' includes the electronic contents on such hardware. This may, however, result in a significant amount of unrelated data (housed on the same disk) also being produced – running contrary to the prohibition against roving enquiries and the particularity/specificity requirements that have also developed through caselaw.

Further, under existing case law, it is unclear if LEA can order individuals to copy or convert electronic data into another form for the purposes of production – positive acts which, under existing interpretations, may not be compelled under this provision. Lastly, under similar principles discussed above, even where an entire hard disk is sought to be produced, parties may not be able to take the ground that inconvenience or loss to productivity prevents production.

ii. Emerging interpretations

Under the second category: Significant questions are likely to arise regarding the appropriate substantive legal standards for compelled production of data. In addition to the general concerns discussed above, it may be possible for parties to plausibly argue that – in light of scientific and technological developments since the enactment of the 1973 Code – the mechanism and standard under Section 92 are more appropriate to compel production of data *held by intermediary entities* since they are, in many ways, conceptually similar to postal and telegraph authorities in that they facilitate third-party communication.[86]

[86] Iyengar (n 20).

From an interpretational lens, the question is whether private intermediaries can fall within the ambit of being telegraph or postal authorities – as recognised under Sections 91(3) and 92. While a detailed analysis of this question is beyond the scope of this piece, it must be acknowledged that technological developments have been found to play an important role in the interpretational exercise. In such cases, courts have also been willing to make 'creative' interpretations. For instance, in *State of Punjab* v. *Amritsar Beverages Ltd*., the Supreme Court observed as follows in relation to the seizure of a hard disk under the Punjab General Sales Tax Act, 1948:

> …Information Technology at that time far from being developed was unknown. Constitution of India is a living organ. It had been interpreted differently having regard to different societal situations…. Same principle is applicable in respect of some statutes.
>
> *Creative interpretation had been resorted to by the Court so as to achieve a balance between the age old and rigid laws on the one hand and the advanced technology, on the other.* The Judiciary always responds to the need of the changing scenario in regard to development of technologies. It uses its own interpretative principles to achieve a balance when Parliament has not responded to the need to amend the statute having regard to the developments in the field of science.
>
> Internet and other information technologies brought with them the issues which were not foreseen by law as for example, problems in determining statutory liabilities. It also did not foresee the difficulties which may be faced by the officers who may not have any scientific expertise or did not have the sufficient insight to tackle with the new situation. Various new developments leading to various different kinds of crimes unforeseen by our legislature come to immediate focus. Information Technology Act, 2000 although was amended to include various kinds of cyber-crimes and the punishments there for, does not deal with all problems which are faced by the officers enforcing the said Act…

The recognition of such an approach may provide some basis to widely interpret Sections 91(3) and 92 to apply to internet intermediaries.

Further, there is a general acceptance of the principle that courts must take into consideration developments in science and technology while interpreting statutes.[87] A court may interpret "*a statute according to its current*

---

[87] *Kashmir Singh v Union of India* (2008) 7 SCC 259, citing *Satyawati Sharma v Union of India* (2008) 5 SCC 287; *See also*, *State v SJ Choudhary* (1996) 2 SCC 428, citing Francis Bennion, *Statutory Interpretation* (2nd edn, Butterworths 1986) 288 ("*In construing an*

meaning and applying the language to cover developments in science and technology not known at the time of passing of the statute."[88] With reference to specific developments in technology, the Supreme Court has – in previous cases – "*recognised the progress of science and technology by bringing in line, the scope and meaning of the words and expressions used in existing statutes, with current norms and usage*."[89]

For instance, in *Senior Electric Inspector* v. *Laxminarayan Chopra*,[90] 'telegraph line' (as defined by the Indian Telegraph Act, 1885) was interpreted to include a wireless telegraph having regard to changes in technology. Similarly, in *Laxmi Video Theatre* v. *State of Haryana*,[91] 'cinematograph' (as contained in Section 2(c) of the Cinematograph Act, 1952) was held to cover video cassette recorders and players for representation of motion pictures on television screen.[92]

Interestingly, in relation to Section 92, there may be partial support for such an interpretative approach from an unlikely source – the Andhra Pradesh Police Manual which, in discussing Section 92, notes that "*[t]he reference to Posts and Telegraphs authorities in this section may be interpreted to include Bharat Sanchar Nigam Limited (BSNL) and any other basic telephone (including WiLL) service provider or cellular operator whether Private or Government*."[93] In a way, this accepts Iyengar's argument for private entities to be included with the ambit of 'postal and telegraph authorities' under Section 92.

Therefore, a semblance of a path ahead exists for a court seeking to adopt an interpretation which reads 'postal and telegraph' authorities in a manner

---

ongoing Act, the interpreter is to presume that Parliament intended the Act to be applied at any future time in such a way as to give effect to the true original intention. Accordingly, the interpreter is to make allowances for any relevant changes that have occurred, since the Act's passing, in law, social conditions, technology, the meaning of words, and other matters. Just as the US Constitution is regarded as 'a living Constitution', so an ongoing British Act is regarded as 'a living Act'. That today's construction involves the supposition that Parliament was catering long ago for a state of affairs that did not then exist is no argument against that construction. Parliament, in the wording of an enactment, is expected to anticipate temporal developments. The drafter will try to foresee the future, and allow for it in the wording"). This paragraph of Bennion's work was specifically cited in relation to the CrPC in *State of Maharashtra v Praful B Desai* (2003) 4 SCC 601.

88 *Balram Kumawat v Union of India* (2003) 7 SCC 628.

89 *Hanumant v State of MP* AIR 1952 SC 343: 1952 SCR 1091.

90 *Senior Electric Inspector v Laxminarayan Chopra* AIR 1962 SC 159: (1962) 3 SCR 146.

91 *Laxmi Video Theatres v State of Haryana* (1993) 3 SCC 715.

92 *See generally*, *Rama Pandey v Union of India* 2015 SCC OnLine Del 10484.

93 *Andhra Pradesh Police Manual* (2017) vol IIA 844 <http://www.policetrainingap.org/wp-content/uploads/2017/10/Final-Vol-002A.pdf> accessed 19 October 2019.

more appropriate to the modern context. At the very least, courts are likely to be called on to adjudicate upon these questions in the near future.

Moving away from an interpretational lens, it is also interesting to note that, in relation to Section 95 of the 1898 Code (which is analogous to Section 92 of the 1973 Code), the Law Commission in its 37th Report rejected a recommendation that these powers also be granted to senior police officers:

> 244. With reference to section 96, it has been suggested that powers be given to the Superintendent or Commissioner of Police to require delivery of postal articles, and that power be given to the Deputy Superintendent of Police to order detention, of such articles. We are not able to accept this suggestion. The District Magistrate, being the head of the administration, should have this power, but it is not desirable to give the power to police officers.[94]

This decision speaks to the fact that in a pre-internet (and pre-internet intermediary) era, postal and telegraph communications deserved a higher level of procedural safeguards prior to their detention or production. Further, this statement also arguably speaks to the acceptance of the notion that judicial officers – and not police – would be the more appropriate authority for the exercise of powers where there is a greater chance of sensitive or private information being at issue.

VI. Concluding Thoughts

The above sections constitute what is likely one of the first detailed discussions of the jurisprudence around Section 91 of the Cr.PC in so far as it may relate to questions raised by modern technology and the Internet. Based on the discussions of caselaw above, the following principles may be extracted as being particularly relevant in illuminating the way forward:

(*i*) Powers and discretion available under Section 91 have been interpreted very broadly;

(*ii*) Section 91 orders may be issued to individuals or entities holding *documents* or *things* on behalf of the target individual;

(*iii*) Inconvenience that may be occasioned in production is not a valid ground for non-compliance with an order under Section 91;

---

[94] Law Commission of India, *Thirty Seventh Report on the Code of Criminal Procedure* (December 1967) para 244.

(*iv*) Section 91 cannot be used to order positive actions other than the production of *documents* or *things;*

(*v*) *Documents* and *things,* as contemplated under Section 91, are those which are physical in nature. However, courts are stretching the meaning of 'documents' to also include electronic records stored on physical media;

(*vi*) Orders under Section 91 must be specific and particular. The provision does not permit roving or vague enquiries;

(*vii*) Even prior to the decision of the Supreme Court in *Puttaswamy*, courts have considered privacy concerns while considering orders under Section 91.

In addition to providing guidelines for the usage of Section 91, these principles concurrently outline the case for its reform. As discussed above, several of these principles are no longer relevant in the digital age, others have the potential to excessively invade privacy, while several others internally conflict.[95] Legislative reform is the only path to ensuring a balance between individual rights and LEA powers in a manner that upholds both individual and state interests. In its current form, the provision neither protects privacy nor provides clear and certain procedures for LEA to access evidence stored in electronic form.

A half measure may involve removing the ability of LEA to unilaterally issue orders for production. However, more sustainable reform will entail a comprehensive rebalancing of the various interests at stake. While considerations to ensure respect for privacy are required to be enshrined in the procedural safeguards governing Section 91, a more robust and certain framework for LEA access to data may also be desirable.

Specifically, ensuring that new safeguards (such as the need for judicial authorisation) do not make LEA procedures inefficient or unduly cumbersome will determine the extent of their adoption. In addition, reform must look to equip LEA with additional powers required to tackle the modern demands of criminal investigation. This may include specific provisions enabling preservation requests and clearer guidelines governing the various issues that arise in relation to summons, search and seizure of electronic devices and data. These will be required to account for the increased risk that a court – going forward – will find that insufficient privacy safeguards,

[95] For a general discussion of issues raised by applying 'traditional' frameworks to the electronic/digital domain, *see*, Orin Kerr, 'Digital Evidence and the New Criminal Procedure' (2005) 105 Columbia Law Review 279.

overbroad powers, or vague procedures make evidence acquired inadmissible at trial. A judiciary seeking to extend *Puttaswamy* to its logical conclusion may potentially be called upon to review the wholesale rejection of the exclusionary doctrine by Indian courts thus far. To minimise shocks to the system that may arise from the exclusion of evidence, legislative reform of Section 91 which seeks to comprehensively rebalance the rights of individuals as well as LEA is very much required.

While it is possible that courts will arrive at interpretations or readings of Section 91 which satisfy some of the concerns discussed in this paper, legislative intervention is required to signal a strong commitment to clearer law enforcement powers and their balanced application to scenarios where rights such as privacy and other civil liberties are at issue. Based on the above, a Section 91 of the future (or a Section 91A, if you will) may seek to include the following features:

Recommendations to enshrine privacy interests

(*i*) Requirement for judicial pre-authorisation prior to the issue of a production order – especially where electronic devices and data are at issue; and

(*ii*) Requirement that courts consider personal privacy, proportionality, convenience, and public interest prior to ordering production – especially where electronic devices and data are at issue;

(*iii*) Requirement that production orders are in writing/electronic form, signed, and are as narrowly framed as possible, specific, and particular;

(*iv*) Provision of avenues and grounds of challenge for target individuals (whether through appeal or revision) – regardless of whether they are party to the investigation at issue;

(*v*) Exceptions to the production of data which is subject to legal or other privilege.

Recommendations to clarify LEA powers and improve evidence gathering[96]

(*i*) Express powers for LEA to compel production of physical as well as electronic documents and information;

(*ii*) Stricter penalties for non-compliance with production orders;

[96] This categorisation is purely for organisational purposes. It is not, in any way, meant to suggest that privacy and LEA interests are distinct, separate, or mutually exclusive.

(*iii*) LEA powers to order data preservation of data at rest and detention of data in transit – pending judicial authorisation to compel their production;

(*iv*) Authorisation for LEA to issue orders for positive acts *which are required solely to give effect to compelled production orders* (such as to copy/image hard disks which contain relevant material);

(*v*) Where onerous, dragnet, or non-specific orders are required, the court must provide special reasons for their issuance. Further, lower courts must provide an opportunity to appeal their rulings to the High Court prior to their implementation. Alternatively, High Courts may be given jurisdiction so that they may be directly approached by LEA in cases where production orders involve a large number of individuals, are particularly urgent, or are complex to implement.

These suggestions, taken together, may provide the starting point for discussions of a new Section 91 which is oriented towards the digital age and adequately rebalances considerations of privacy, civil liberties, and LEA interests.

Accountability and Enforcement Aspects of the EU General Data Protection Regulation - Methodology for the Creation of an Effective Compliance Framework and a Review of Recent Case Law

Paolo Balboni[*], *Martim Taborda Barata*[**], *Anastasia Botsi*[†] & *Kate Francis*[‡]

Abstract *The General Data Protection Regulation (GDPR), which has been applicable within the EU/EEA since 18 May 2018, has brought about reinforced rules on personal data protection which have dramatically shifted the paradigm for all organisations bound by them. This includes not just those which actively handle personal data as a core part of their business model, but also those which are required to handle personal data (on employees, customers or suppliers, for example) as part of their day-to-day activities – in other words, all organisations falling under the GDPR's scope. By holding organisations responsibile for their own compliance, and requiring those organisations to carefully assess the risks to the rights, freedoms,*

[*] Prof. Dr Paolo Balboni is a top-tier European ICT, Data Protection & Cybersecurity lawyer and serves as Data Protection Officer (DPO) for multinational companies. Founding Partner of the international law firm ICT Legal Consulting. Professor of Privacy, Cybersecurity, and IT Contract Law at the European Centre on Privacy and Cybersecurity (ECPC) within the Maastricht University Faculty of Law. Lead Auditor BS ISO/IEC 27001:2013 (IRCA Certified), he also obtained the EU General Data Protection Regulation DPO Professional University Certificate (ECPC-B DPO). (paolo.balboni@ictlegalconsulting.com and paolo.balboni@maastrichtuniversity.nl) accessed 23 January 2020.

[**] Martim Taborda Barata, LL.M., is a Partner at ICT Legal Consulting International, and an Intellectual Property, Privacy & Data Protection lawyer registered at the Portuguese Bar Association. He also obtained the EU General Data Protection Regulation DPO Professional University Certificate (ECPC-B DPO). (martim.tabordabarata@ictlegalconsulting.com) accessed 23 January 2020.

[†] Anastasia Botsi, LL.B. is an Associate at ICT Legal Consulting International. She also obtained the EU General Data Protection Regulation DPO Professional University Certificate (ECPC-B DPO). (anastasia.botsi@ictlegalconsulting.com) accessed 23 January 2020.

[‡] Kate Francis, M.Sc., is a Privacy and Ethics Researcher, Development and Communication Specialist at ICT Legal Consulting. Ph.D. candidate at the European Centre on Privacy and Cybersecurity (ECPC) within the Maastricht University Faculty of Law. She also obtained the EU General Data Protection Regulation DPO Professional University Certificate (ECPC-B DPO). (kate.francis@ictlegalconsulting.com) accessed 23 January 2020.

and legitimate interests of individuals when implementing measures to address these rules, the GDPR demands a higher level of accountability from all organisations concerned – the ability to not only comply with the rules, but to also demonstrate that compliance has been achieved. To help organisations understand how they can address the practical implications brought about by the GDPR, this article seeks to break down a proposed Data Protection Compliance Framework – six overarching steps which, if correctly and comprehensively implemented by those organisations, will allow them to make the necessary adjustments to their internal practices to align with the GDPR's requirements. To highlight the importance of implementing such a Framework, the article also explores the different types of powers granted to supervisory authorities in order to enforce the Regulation, and includes a selection of relevant supervisory authority decisions to allow insight into common types of GDPR breaches, and common enforcement responses (including fines) taken by those authorities.

I. Introduction

The direct applicability to all Member States of the European Union of Regulation (EU) 2016/679 of the EU Parliament and of the Council of 27 April 2016 (the General Data Protection Regulation, or '**GDPR**') on 25

May 2018, brought about a new era for data protection in Europe. This era had commenced more than two years prior, when the GDPR was first published in the Official Journal of the European Union, back in May 2016.[1] At the time, entities falling under the GDPR's scope were given a transitional period of two years to shift from the older requirements set out in multiple national laws transposing Directive 95/46/EC of the EU Parliament and of the Council of 24 October 1995 (the '**Data Protection Directive**')[2] to the new data protection regulatory framework. However, this proved not to be a simple compliance exercise of making adjustments to certain requirements or specifications. Organisations would soon realise that the GDPR introduces fundamental game-changers, which require both controllers and processors to amend their perspective on the handling of personal data.

First and foremost is the express enshrinement of the principle of accountability.[3] As before, controllers are held primarily responsible for ensuring compliance with data protection rules; however, and additionally, controllers must now maintain evidence to allow them to demonstrate this compliance to supervisory authorities.[4] Supervisory authorities would take on a role more focused on monitoring and enforcement (with previous legal obligations of prior notification or authorisation in order to carry out processing activities done away with, for the most part). On the one hand, this brought about much-desired flexibility for controllers wishing to make use of personal data; on the other, those same controllers would now be required to assess all of their processes concerning personal data from the ground up, to ensure that they align with the GDPR's requirements. Controllers would need to make sure that they are able to document assessments, keep records and implement internal policies and procedures to demonstrate their compliance.

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119/1 (GDPR).

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281/31.

3 GDPR, art 5(2): "*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').*"

4 The Information Commissioner's Office, which is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies, and data privacy for individuals, explains that the accountability principle requires organisations to "*take responsibility for what [they] do with personal data*", and that organisations "*must have appropriate measures and records in place to be able to demonstrate your compliance*". UK Information Commissioner's Office, 'Accountability principle' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accountability-principle/> accessed 23 January 2020.

Secondly, the GDPR brings about a risk-based approach to compliance.[5] Rather than providing a checklist of clear actions to complete, the GDPR relies on overarching data protection principles and open-ended goal-oriented obligations. Controllers would be primarily responsible for assessing the circumstances under which they process personal data, with an emphasis on understanding the potential risks which could arise to the rights and freedoms of data subjects from the use of their personal data. They would also be responsible for implementing technical and organisational measures which they deem appropriate to bring those processing activities under compliance with the GDPR and its principles.[6] Once more, the added flexibility was offset by the uncertainty created. Controllers were reminded that, under the principle of accountability, they would be held responsible for all compliance decisions made, and would need to be able to demonstrate how those decisions were in alignment with the GDPR's key data protection principles.

Thirdly, the concepts of data protection by design and by default were expressly given legal recognition in the GDPR.[7] Controllers were now specifically required to ensure that all of their data processing systems, processes, services and products incorporated data protection requirements from their design phase. They would also need to periodically review these assessments, so as to ensure continued compliance throughout the lifecycle of those systems, processes, services and products. Furthermore, by default, any activities developed by controllers requiring the use of personal data should stick

---

[5] The Data Protection Commission, which is the national independent authority in Ireland responsible for upholding the fundamental right of individuals in the European Union (EU) to have their personal data protected, clearly explains the risk-based approach as follows: "*[w]hen your organisation collects, stores or uses (i.e. processes) personal data, the individuals whose data you are processing may be exposed to risks. It is important that organisations which process personal data take steps to ensure that the data is handled legally, securely, efficiently and effectively in order to deliver the best possible care. The risk-profile of the personal data your organisation processes should be determined according to the personal data processing operations carried out, the complexity and scale of data processing, the sensitivity of the data processed and the protection required for the data being processed. For example, where a data processing activity is particularly complex, or where a large volume or sensitive data is involved (i.e. an internet, health, financial or insurance company), this would attract a higher risk rating than routine personal data that relates solely to employee or customer account details. When looking at the risk profile of the personal data your organisation processes, it is useful to look at the tangible harms to individuals that your organisation needs to safeguard against. These are detailed in Recital 75 of the GDPR and include processing that could give rise to: discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation; or any other significant economic or social disadvantage*". The Data Protection Commission, 'Risk Based Approach' <https://www.dataprotection.ie/en/organisations/know-your-obligations/risk-based-approach> accessed 23 January 2020.

[6] GDPR, art 24.

[7] GDPR, art 25.

to the absolute minimum required, considering also the extent to which those data were processed and the time during which they should be stored.[8]

Last but not least, controllers and processors were given a healthy incentive to bring their activities into compliance with the GDPR: the exponential increase in the investigative and corrective powers of supervisory authorities, particularly concerning the maximum limits for administrative fines which might be imposed in the event of a relevant infringement.[9]

Perhaps unsurprisingly, come 25 May 2018, many entities were still struggling to develop means to meet the different GDPR requirements (and many continue to struggle to this day). There is still wide-spread uncertainty as to how compliance can be achieved in the practical sense, despite a wealth of available guidance from local supervisory authorities and the European Data Protection Board (formerly the Article 29 Working Party).[10] As such, this article seeks to propose a structured, six-step framework – a Data Protection Compliance Framework – through which entities under the GDPR's scope may systematically review their data processing practices. This framework will also help organisations to understand the adjustments that need to be made at the fundamental level, in order to understand and practically

---

[8] *See*, European Data Protection Supervisor, 'Opinion 5/2018 – Preliminary Opinion on Privacy by Design', (31 May 2018) <https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf> accessed 23 January 2020 (EDPS Opinion 5/2018). While the European Data Protection Supervisor is the supervisory authority responsible for the supervision of the personal data processing activities of EU institutions and bodies, the similarities between the rules on personal data processing applicable to those EU institutions and bodies (currently, as laid out in Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018) and the GDPR allow the drawing of relevant insights for private and public entities from the European Data Protection Supervisor's guidance.

[9] GDPR, ch VI, 'Independent Supervisory Authorities', s 2 'Competence, Tasks and Powers', and ch VIII 'Remedies, Liability and Penalties'.

[10] Article 29 Working Party was formed by representatives of all supervisory authorities within the EU under the Data Protection Directive and, among its various tasks and powers, was responsible for developing guidance to assist in compliance with data protection rules. With the entering into force of the GDPR, it was replaced by the European Data Protection Board, which retains similar advisory responsibilities. The guidelines, opinions, and other documents published by these bodies serve as interpretative guidelines for the GDPR's provisions, clarifying how supervisory authorities within the EU are likely to apply those provisions within their own jurisdictions. In this sense, these documents are invaluable tools for controllers and processors to adopt best practices from the privacy and data protection perspective. Their recommendations can also be used to support decisions made by controllers and processors on the configuration of their own processing activities, particularly when dealing with inquiries or inspections carried out by a supervisory authority. However, it must be stressed that these documents are not legally binding – they merely provide insight as to how supervisory authorities (and not necessarily local or EU-level courts) interpret the GDPR. (Available at: <https://edpb.europa.eu/> accessed 23 January 2020).

implement the GDPR's key data protection principles set forth in Art. 5. Moreover, in order to provide a more practical context, we will analyse a collection of decisions rendered by supervisory authorities within the EU under the GDPR, to offer insights into lines of interpretation followed across jurisdictions regarding different data protection principles and requirements.[11]

II. Topic, Approach and Methodology

This article seeks to break down a proposed Data Protection Compliance Framework. Such Framework includes six steps which, if correctly and comprehensively implemented by entities, will allow relevant adjustments to be made to organisations' internal practices, in order to align them with the GDPR's requirements. The Framework is covered in an abstract manner, to allow different entities to draw conclusions as to how it may best apply to their own processing activities, following the risk-based approach now made fundamental by the GDPR.

---

[11] While there are several other publications available which touch upon practical aspects of GDPR compliance measure implementation, this article distances itself from the rest by focusing primarily and at length on the practicalities of GDPR compliance, by means of a structured, step-based approach to the implementation of a data protection compliance framework. The closest examples to the aim of this article include Peter Carey, *Data Protection: A Practical Guide to UK and EU Law* (5th edn, OUP 2018); Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017); IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide* (2nd edn, IT Governance Publishing 2016-2017); Stephen Massey, *The Ultimate GDPR Practitioner Guide: Demystifying Privacy & Data Protection* (Fox Red Risk Publishing 2017); and Sanjay Sharma and Pranav Menon, *Data Privacy and GDPR Handbook* (Wiley 2019), which provide varied and substantial practical guidance on compliance with data protection requirements (from the legal and security perspectives), but dedicate only relatively brief chapters to the practicalities inherent to the creation of a data protection compliance programme or framework. Other less related examples include Richard Morgan and Ruth Boardman, *Data Protection Strategy: Implementing Data Protection Compliance* (3rd edn, Sweet & Maxwell 2019); Paul Lambert, *Understanding the New European Data Protection Rules* (CRC Press 2018); and Maciej Gawronski, *Guide to the GDPR* (Wolters Kluwer 2019), which address several, if not all, GDPR compliance requirements from a practical perspective, but do not specifically cover the development of a comprehensive internal compliance framework for dealing with all those requirements in a structured manner; European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law* (2018 edn); Daniel Rücker and Tobias Kugler, *New European General Data Protection Regulation, A Practitioner's Guide: Ensuring Compliant Corporate Practice* (1st edn, C.H. Beck, Hart and Nomos 2018); and Denis Kelleher and Karen Murray, *EU Data Protection Law* (1st edn, Bloomsbury Professional 2018); which focus more on a theoretical and expositional approach to data protection than a practical angle; Noriswadi Ismail and Edwin Lee Yong Cieh, *Beyond Data Protection: Strategic Case Studies and Practical Guidance* (Springer 2013), which covers targeted data protection issues in selected jurisdictions from a theoretical and practical perspective, without addressing the steps needed to create an internal framework for organisations to comply with GDPR requirements.

Each step has been carefully laid out in order to describe its requirements from the theoretical perspective. Examples and considerations are provided, drawn from practical experience in the development and implementation of various instances of such frameworks with numerous different entities, including multinational companies, local service providers and EU institutions and bodies (though the focus of this article is not on the similar data protection requirements of Regulation (EU) 2018/1725 of the EU Parliament and of the Council of 23 October 2018)[12]. The steps are described in a pre-determined order, so as to show how each successive step complements the one before it, given the interconnected nature of all six steps.

To further evidence the practical impact which a failure to properly and thoroughly address GDPR requirements may have, as well as to lay out actual interpretations of those requirements given by supervisory authorities, the most recent and relevant decisions rendered by those authorities, at the date of writing, were collected, summarised and filtered. This is reflected in the selection of decisions included at the end of the article, which is aimed to allow readers to succinctly understand the lines of reasoning which have been developed by those authorities over time (particularly where authorities have decided to impose administrative fines as a result of detected infringements).

Given that the GDPR applies to controllers[13] and processors[14] of personal data,[15] they represent the key players that should be concerned with the discussions presented in this article. However, this knowledge may also prove useful to data protection officers[16] and, in general, consultants and practitioners operating in the fields of privacy and data protection. As such,

---

[12] It is noteworthy to underline that there are in fact significant similarities between the discipline set forth in the GDPR and the one in Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018.

[13] GDPR, art 4(7): "'*controller' meansthe natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*".

[14] GDPR, art 4(8): "'*processor' meansa natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*".

[15] GDPR, art 4(1): "'*personal data' means any information relating to an identified or identifiable natural person*". Please mind that 'personal data' may, for the purpose of this article, be used interchangeably with 'data' or 'information', depending on the context.

[16] As noted in GDPR, Recital 97, a data protection officer is "*a person with expert knowledge of data protection law and practices*", which should be engaged to assist a controller or processor in monitoring internal compliance with the GDPR, whenever mandatory [GDPR, article 37(1)] or whenever this is deemed prudent by the organisation in question. For more information, refer to GDPR, arts 37-39 and Article 29 Working Party, Guidelines on Data Protection Officers ('DPOs') WP243 Rev. 01 (10 October 2017) <https://ec.europa.eu/

the article presumes that the more fundamental privacy and data protection concepts (such as definitions and principles) are grasped by the reader. Nevertheless, the article also touches upon them, as a means to reinforce their apprehension and emphasise their importance.

III. Structure and arguments

This article can be divided into two parts: the first covering the proposed Data Protection Compliance Framework, and the second covering the powers granted to supervisory authorities under the GDPR, as well as a review of selected decisions laid down by supervisory authorities across the EU.

The first part breaks down the Data Protection Compliance Framework into its six main steps:

1. Accountability;
2. Data protection by design and by default;
3. Risk assessments, data protection impact assessments and security;
4. Information to the data subject;[17]
5. Legitimate basis; and
6. Data subject rights.

Each step is addressed by providing a theoretical explanation of its objectives, an exposition of the relevant GDPR articles and practical considerations as to how the step may be implemented into the processing[18] practices of the reader. Connections between steps and with the GDPR's data protection principles are highlighted whenever relevant.

The second part begins by looking at the GDPR's enforcement from a theoretical perspective. It describes, in abstract, the investigative, corrective, advisory, and authorisation powers granted to supervisory authorities under

---

newsroom/article29/item-detail.cfm?item_id=612048> accessed 23 January 2020 (Art. 29 Working Party DPO Guidelines).

[17] Under GDPR, art 4(1), a data subject is an identified or identifiable natural person, where "*an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

[18] GDPR, art 4(2): "'*processing*' *means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

the GDPR. Specific focus is given to administrative fines, including the factors which must be assessed by supervisory authorities in their decision to impose an administrative fine, and in the determination of the amounts to be fined. This theoretical perspective is then complemented with an analysis of GDPR enforcement from a practical perspective. A selection of decisions rendered by supervisory authorities across the EU under the GDPR is reviewed, providing Each case presented includes the date of the decision (or the press release covering the decision, where the actual date of decision is not available), the identity and country of the supervisory authority in question (along with a link to the decision or a corresponding press release where the decision is not available), a summary of the facts of the case and the decision given, and an analysis of the conclusions which readers may draw from each case.

IV. The Six Steps of a Data Protection Compliance Framework

The territorial scope of the GDPR extends beyond the limits of the EU. The GDPR seeks to impose its obligations upon controllers and processors established in third countries, insofar as they offer goods or services to individuals within the EU, or monitor those individuals' behaviour within the EU.[19] As such, non-EU controllers and processors may also be required to implement appropriate measures to address the GDPR's requirements in a structured and comprehensive manner. Considering further that the GDPR's fundamental data protection principles (explored further below) are generally aligned with internationally recognised principles of personal data protection,[20] even companies which escape the wide territorial scope of the GDPR may benefit from aligning their internal processes with its rules. This applies also to multinational companies seeking to implement group standards for data protection compliance, which may consider using the GDPR as an international baseline. In this article, we will describe six main steps which should

[19] *See*, GDPR, art 3.

[20] Internationally recognised principles of personal data protection can be conventionally summarised as follows:
- Openness: Entities must me open about personal data practices;
- Collection limitation: Collection of personal data must be limited, lawful and fair;
- Purpose specification: Purposes of the collection and disclosure must be specified;
- Use limitation: Use of data must be limited to specific purposes;
- Security: Personal data must be subject to appropriate safeguards;
- Data quality: Personal data must be relevant, accurate and up-to-date;
- Access and correction: People must be able to access and correct their personal data; and
- Accountability: Entities must comply with the data protection principles and be able to demonstrate such compliance.

be addressed by companies seeking to bring their data processing practices into alignment with the GDPR. This may be achieved through the development and practical implementation of a set of internal policies, procedures, records and notices to regulate those practices – a structured internal framework for compliance with GDPR rules, which we will refer to as a '**Data Protection Compliance Framework**'.

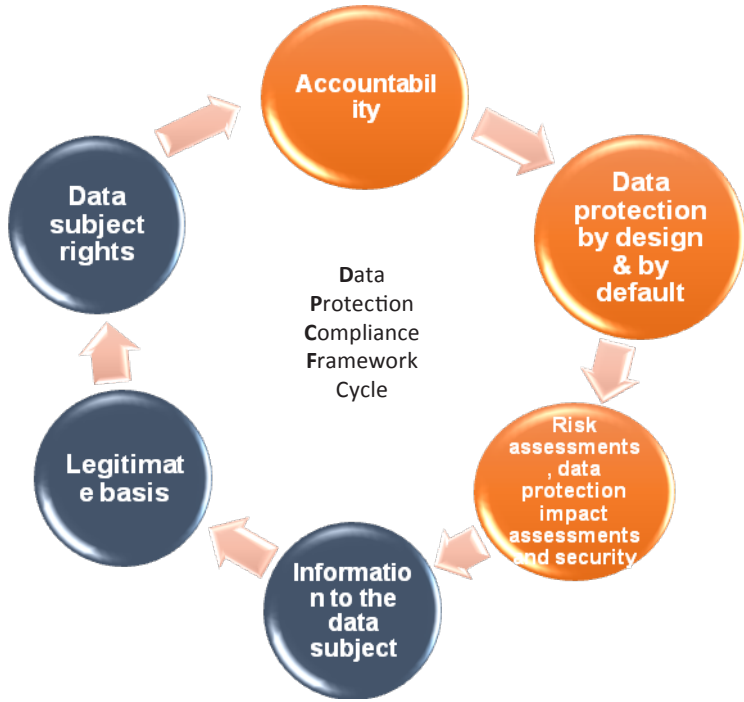

Fig. 1: The Data Protection Compliance Framework Cycle exemplifies a methodology which consists of six main steps which can be followed by entities seeking to bring their data processing practices into alignment with the GDPR through the development and practical implementation of a set of internal policies, procedures, records and notices to regulate those practices, a structured internal framework for compliance with GDPR rules.

By developing and implementing such a framework, both controllers and processors of personal data will seek to comprehensively and systematically implement the GDPR's requirements into their processes. This will, of course, be done in a manner which is deemed appropriate by the controller or processor to ensure compliance and to handle potential risks to the rights and freedoms of the individuals whose data are processed. The Data Protection Compliance Framework essentially aims to increase the means

by which a controller or processor can comply with the GDPR's principle of accountability, and generate demonstrable evidence of such compliance. This will cover an internal component, including the assessments carried out by the controller/processor as to the most appropriate manner for it to ensure its compliance and the internal policies and procedures developed as a result. In addition, an outward-facing component will be set up, through which the controller/processor's data processing practices, tempered by the internal assessments and compliance activities undertaken, are effectively communicated to data subjects, business partners and supervisory authorities, as a demonstration of the controller/processor's compliance.

As noted in Fig. 1, the steps to be taken in order to develop and implement a Data Protection Compliance Framework can be visually represented as a circle, rather than as a checklist with items to be ticked off. This is representative of the fact that the manner in which a controller/processor addresses each of the steps will influence the others. The development and implementation process is one of continuous and ongoing improvement, rather than a time-restricted project with a clear deadline in sight. This process operates on similar premises to those of the so-called 'Deming Cycle' (also used to implement the information security standard ISO/IEC 27001),[21] only adapted to the data protection domain: establish a plan for compliance on the basis of foreseeable results ('Plan"), execute the plan by taking steps under controlled circumstances ('Do'), check and analyse the results collected ('Check'), and take action to standardise or improve the plan on the basis of those results ('Act').[22]

Controllers and processors must take note that the measures they establish to align with data protection requirements will not be static, but will rather need to be progressively reviewed. This is to ensure that these measures remain relevant to their processing activities (which, themselves, may develop over time), adapt to the evolution of available technology and

---

[21] It is noteworthy to underline that compliance with the information security standard ISO/IEC 27001 can greatly support alignment with the GDPR, so organisations can surely leverage their alignment with ISO/IEC 27001 to build a solid Data Protection Compliance Framework. See on ISO/IEC 27001: <https://www.iso.org/isoiec-27001-information-security.html> accessed 23 January 2020.

[22] The Deming Cycle, or PDSA/PDCA Cycle, is a quality improvement model that uses the logical sequence of the four repetitive steps (plan, do, study, act) in order to ensure that the improvement of projects is a continuous effort, and to demonstrate that even in the duration of projects, it is valuable to go back, study the results that have been collected in the lifetime of the project and decide the changes necessary to improve the relevant processes and activities of the company. For more information, *See*, Ronald Moen, 'Foundation and History of the PDSA Cycle'<https://deming.org/uploads/paper/PDSA_History_Ron_Moen.pdf> accessed 23 January 2020.

means by which personal data may be processed, address relevant legislative changes, and are aligned with interpretations laid down by supervisory authorities or in relevant jurisprudential decisions. It is in this sense that the correct development and implementation of a Data Protection Compliance Framework will follow similar implementation and review processes to those defined in the international ISO/IEC 27001 standard. It will reflect a reiterative process of continued assessment of risks to the rights and freedoms of data subjects and the measures implemented to address them. It is worth noting, on this point, that adherence to ISO/IEC 27001 can be a valid tool to address GDPR compliance from the data security standpoint, but must necessarily be further complemented with other relevant technical and organisational measures to deal with the GDPR requirements which are not strictly related to data security (including, for example, the assessment of the possible risks that the data processing activities may pose on data subjects, like: discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage, the identification of correct legal bases for processing, and the proper management of data subject requests).

In the following sections, we will explore the different steps involved in the development and implementation of a Data Protection Compliance Framework from a more practical perspective. This will serve to illustrate the main points which must be borne in mind from a GDPR compliance perspective.

A. Step 1: Accountability

The principle of accountability was first adopted in 1980 within the Organisation for Economic Co-operation and Development ('**OECD**') Guidelines.[23] Now established in Art. 5(2) GDPR, it is an overarching principle which represents a fundamental paradigm shift from the Data Protection Directive (now repealed by the GDPR). Under the Data Protection Directive, supervisory authorities were considered to have a predominant role in ensuring that controllers remained compliant with data protection law. This was carried out, in particular, by analysing and advising on the various notifications and requests for authorisation which those entities were required to submit to the supervisory authority, as a pre-requisite for most of their processing activities. The GDPR turns this concept on its head.

[23] Peter Cullen, 'A Pivot (Back) to Accountability' (*The Information Accountability Foundation*, 28 March 2019) <http://informationaccountability.org/a-pivot-back-to-accountability> accessed 23 January 2020.

Under the GDPR, supervisory authorities are left with an investigative, monitoring and enforcement role (with the previous notification and authorisation requirements having been almost entirely removed). Controllers are now fully responsible for ensuring that they comply with the terms of the GDPR. They are also fully responsible for being able to demonstrate their compliance upon request, in a manner which can be understood by relevant stakeholders. In order to give more weight to this principle, the Information Accountability Foundation has previously set out a list of essential elements which make up the notion of 'accountability' in this domain:[24]

- A commitment on the part of an organisation to accountability, and the adoption of internal policies that are consistent with external criteria;
- The implementation of mechanisms to put privacy policies into effect, including tools, training, and education;
- The implementation of systems to ensure internal ongoing oversight, assurance reviews, and external verification;
- Transparency, and the implementation of mechanisms to allow for individual participation of data subjects; and
- The provision of means for remediation and external enforcement of data protection compliance.

These elements are all reflected, in some form, within the different steps making up the cycle of development and implementation of a Data Protection Compliance Framework. The dual purposes of a Data Protection Compliance Framework are (1) to establish means by which an entity may comply with evolving applicable data protection requirements, and (2) to create elements which that entity can use to demonstrate its compliance when necessary. As such, it can be said that this principle permeates the entirety of the Data Protection Compliance Framework cycle, with each step laying an additional brick in the road to accountability.

Under Art. 24 GDPR, controllers are given relative freedom to determine the technical and organisational measures which they will implement to comply with the rules of the GDPR. This should be determined based on an assessment of their processing activities and the risks inherent to them which may arise to the rights and freedoms of the data subjects concerned. Art.

[24] Martin Abrams, 'The Essential Elements of Accountability Form the Bedrock for Tomorrow's Data Governance' (*The Information Accountability Foundation*, 13 January 2015) <http://informationaccountability.org/essential-elements-form-the-bedrock/> accessed 23 January 2020.

24 GDPR thus reflects the risk-based approach, an integral part of accountability, which controllers and processors are required to adopt under the GDPR. The GDPR does not, for the most part, indicate specific measures which must be followed to achieve compliance (particularly where security of processing is concerned); instead, controllers and processors are required to consider the individuals whose data are processed (and, in particular, their fundamental rights and freedoms) as assets to be protected, and define suitable measures to safeguard those assets.[25] Controllers must therefore continuously consider the specific circumstances under which they carry out their processing activities in order to conduct an assessment of the likelihood and impact of relevant risks,[26] and review or update the measures which they have put in place to address those risks as appropriate.

Within the GDPR, accountability can be regarded as an 'umbrella principle'. This is because it is given substance by reference to the other six data protection principles set forth in Art. 5 GDPR. All of these principles are tackled in the different steps for development and implementation of a Data Protection Compliance Framework:

- The principles of *lawfulness*, *fairness*, and *transparency* are listed in tandem under Art. 5(1)(a) GDPR. Controllers are required to handle personal data exclusively in a manner which is lawful, namely by relying on an appropriate legal basis for each of the purposes for which they process personal data, as laid out in Art. 6 GDPR and, where applicable, by relying on appropriate derogations under Arts. 9, 10 or 22 GDPR.[27] They should further handle personal data only in manners which align with the reasonable expectations of data subjects, and not in a way which may cause unjustified adverse effects upon them (in particular, by refraining from any deceptive, misleading or unfairly biased processing practices).[28] Furthermore, controllers must be open and transparent about their data processing practices with

[25] EDPS Opinion 5/2018 (n 8) 6-7. While the European Data Protection Supervisor is the supervisory authority responsible for the supervision of the personal data processing activities of EU institutions and bodies, the similarities between the rules on personal data processing applicable to those EU institutions and bodies (currently, as laid out in Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018) and the GDPR allow the drawing of relevant insights for private and public entities from the European Data Protection Supervisor's guidance.

[26] EDPS Opinion 5/2018 (n 8) 6.

[27] *See*, UK Information Commissioner's Office, 'Principle (*a*): Lawfulness, Fairness and Transparency' 'What is lawfulness?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/> accessed 23 January 2020.

[28] ibid 'What is fairness?'.

data subjects and society at large. This requires them to provide clear, understandable, and comprehensive information about the terms under which they will handle personal data, notify data subjects of the occurrence of more serious personal data breaches, and generally facilitate the exercise of the rights conferred to data subjects by the GDPR.[29]

- The principle of *purpose limitation* follows under Art. 5(1)(b) GDPR. Controllers are required to clearly identify specific purposes for which they wish to process personal data upfront. They are also required to document the specific purposes identified and inform data subjects as to those purposes. As a rule, personal data may only be processed for those specific and identified purposes which motivated the collection of personal data by a controller; however, if this is clearly notified to data subjects, controllers are also able to further process collected data for additional purposes (so long as they are compatible with the initial purposes).[30]
- The principle of *data minimisation*, under Art. 5(1)(c) GDPR, demands that controllers only process personal data which are adequate, relevant and not excessive in relation to the specific purposes which they have identified. Controllers must always seek to handle the strict minimum amount of personal data necessary to meet those purposes, and proactively erase or anonymise any personal data which exceed that minimum amount.[31]
- The principle of *accuracy*, under Art. 5(1)(d) GDPR, asks that controllers take every reasonable step to ensure that all the personal data which they handle are accurate and kept up-to-date. This requires controllers to correct or dispose of personal data which are found to be inaccurate. The principle of accuracy includes a reactive component, in that controllers must allow data subjects to exercise their right to rectification concerning any of their personal data which may be inaccurate or incomplete, and a proactive component, requiring

---

[29] ibid 'What is transparency?'.

[30] *See*, UK Information Commissioner's Office, 'Principle (*b*): Purpose Limitation' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/> accessed 23 January 2020.

[31] *See*, UK Information Commissioner's Office, 'Principle (*c*): Data Minimisation' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/> accessed 23 January 2020.

controllers to make an effort to ensure that no incorrect or misleading data are actually used.[32]

- The principle of *storage limitation*, under Art. 5(1)(e) GDPR, opposes the indefinite retention of personal data. Controllers are required to define retention periods for the personal data they handle, in relation to the purposes for which those data are processed. These periods should be defined so as to allow the retention of personal data for the strict minimum amount of time necessary to allow the purposes to be met. Once those periods are up, those data should be erased or anonymised without delay.[33]
- Finally, the principles of *integrity* and *confidentiality* (also referred to jointly as the principle of *security*) require controllers to implement an appropriate level of security regarding the personal data they process. The goal for this is to prevent those data from becoming accidentally or deliberately compromised. This concerns the broader concept of information security, which is an important (though not sole) component of data protection compliance.[34]

A controller will comply with the principle of accountability insofar as it complies with all of the above principles and is able to produce relevant evidence to demonstrate this upon request - hence the definition of accountability as an 'umbrella principle'. Relevant elements which may be used for these purposes (and will, in fact, most likely be inspected by inquiring supervisory authorities) include:

- The controller's record of processing activities under Art. 30 GDPR;
- The internal policies and procedures implemented by the controller;
- The data processing agreements which the controller has signed with its processors;
- The information notices and privacy policies put in use by the controller;

---

[32] *See*, UK Information Commissioner's Office, 'Principle (*d*): Accuracy' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/> accessed 23 January 2020.

[33] *See*, UK Information Commissioner's Office, 'Principle (*e*): Storage Limitation' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/> accessed 23 January 2020.

[34] *See*, UK Information Commissioner's Office, 'Security'<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/> accessed 23 January 2020.

- The documented risk assessments which the controller has carried out to support its choice of implemented security measures;
- The registers kept by the controller to demonstrate appropriate management of personal data breaches and data subject requests; and
- The data protection training activities provided to employees, in order to demonstrate that each person authorised to process personal data in the organisation is effectively aware of the applicable data protection rules that need to be applied.

There are, thus, multiple means by which the controller can demonstrate its compliance, facilitating which is one major goal of the creation and implementation of a Data Protection Compliance Framework.

B. Step 2: Data protection by design and by default

While 'data protection by design' is referred to as a 'principle' at multiple points within the GDPR,[35] it is more useful to think of it as a 'means' by which to achieve true compliance with the different data protection principles listed in Art. 5 GDPR. This is evidenced in Art. 25 GDPR, which creates an obligation for controllers to assess all relevant circumstances pertaining to their processing activities (including their inherent risks to the rights and freedoms of data subjects) in order to select and implement appropriate technical and organisational measures "*which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the [GDPR] and protect the rights of data subjects*".

The concept of 'data protection by design' is derived from the similar concept of 'privacy by design'.[36] This latter concept was first popularised by the work of Dr. Ann Cavoukian, former Information & Privacy Commissioner of Ontario, Canada. Dr. Cavoukian published a list of seven foundational principles making up this concept, which can be used to further illustrate how implementing data protection by design is fundamental in ensuring effective compliance with the GDPR:[37]

---

[35] *See*, for example, GDPR, Recital 78, Recital 108, and art 47(2)(*d*).

[36] The term 'privacy by design' is often used in other contexts than the GDPR to refer to the same concept of 'data protection by design'.

[37] Ann Cavoukian, 'Privacy by Design – The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices' (2009) <https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf> accessed 23 January 2020.

- **Proactive not Reactive; Preventative not Remedial.** Controllers should seek to implement proactive measures to anticipate and prevent privacy risks, rather than merely reacting to materialised incidents. This requires a commitment on the part of controllers (and shared by all relevant stakeholders) to set and enforce a high level of privacy, while also establishing methods to detect and correct any poor privacy designs and practices.
- **Privacy as the Default.** Systems and activities involving the processing of personal data must be configured so that, by default, an appropriate level of privacy and security is guaranteed, such that data subjects do not need to take any action to ensure this. Currently referenced as the principle of 'data protection by default' under Art. 25(2) GDPR, its implementation is a means to ensure practical compliance with several of the fundamental GDPR data protection principles, including purpose limitation,[38] data minimisation,[39] and storage limitation.[40]
- **Privacy Embedded into Design.** Measures to ensure the privacy of individuals must be embedded into technologies, operations and information architectures in a holistic, integrative and creative manner. This requires a systematic, principled and structured approach, including the carrying out and documenting of prior detailed risk and data protection impact assessments (see Section 4.3), so as to avoid (or substantially minimise potential) negative consequences to the rights and freedoms of individuals.
- **Full Functionality – Positive-Sum, not Zero-Sum.** When embedding privacy into technology, processes or systems, the goal is to ensure that risks to privacy are appropriately managed without impairing the full functionality of the technology, process, or system in question.

---

[38] ibid: "*Purpose Specification – the purposes for which personal information is collected, used, retained and disclosed shall be communicated to the individual (data subject) at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances*".

[39] Cavoukian (n 37): "*Collection Limitation – the collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes. Data Minimisation – the collection of personally identifiable information should be kept to a strict minimum. The design of programs, information and communications technologies, and systems should begin with non-identifiable interactions and transactions, as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimised*."

[40] Cavoukian (n 37): "*Use, Retention, and Disclosure Limitation – the use, retention, and disclosure of personal information shall be limited to the relevant purposes identified to the individual, for which he or she has consented, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfil the stated purposes, and then securely destroyed*."

By clearly documenting all interests, objectives, desired functions and agreed metrics pertaining to a system which is being designed, it should be possible to develop solutions which avoid unnecessary trade-offs (eg, sacrificing security and/or knowledge in the interest of personal data protection) and instead allow the relevant aims to be met.

- **End-to-End Security – Lifecycle Protection.** Guaranteeing the security of personal data processed is fundamental, and this must be done from the start of the data lifecycle (when personal data are first collected or generated) to the end of it (when personal data are ultimately erased or anonymised). In coherence with Art. 32 GDPR, entities should apply effective security measure to assure the confidentiality, integrity and availability of the personal data they process, including strong identity management and access control to enforce the principle of least privilege, means of secure data destruction, and, where appropriate, pseudonymisation, encryption, and event logging and monitoring techniques.
- **Visibility and Transparency.** In order to develop accountability and foster trust with data subjects and other stakeholders, entities must be open and transparent in relation to their policies and practices concerning the management of personal data. Technologies used to process personal data should also be clearly explained to data subjects, set to operate according to data protection principles, and be independently verifiable. Easily understandable and effective complaint and redress mechanisms, as well as mechanisms to ensure the exercise of data subject rights, must be made available to data subjects.
- **Respect for User Privacy.** The process for incorporating privacy protection as a structural element of an entity's functioning must keep the interests and needs of data subjects at the forefront of its goals. Business operations, physical architectures, and any human-machine interfaces should be developed according to this data subject-centric perspective, rather than focusing primarily on business or other needs and interests.

'Data protection by design' is ultimately an approach which requires controllers to consider privacy and data protection issues at the design phase of any system, service, product, or process, as well as throughout their entire lifecycle. Data protection should be made an essential component of the core functionality of the controller's processing systems and services. There are several practical considerations which controllers should bear in mind to

achieve this, which can be traced back to each of the fundamental data protection principles of Art. 5 GDPR.[41] Further, when engaging processors, or relying on third-party systems, services, or products to handle personal data, controllers should be sure to carry out careful assessments and only rely on those who offer sufficient guarantees of the correct implementation of data protection principles.

Data protection by default can be seen as a specification of 'data protection by design', as seen above in Dr. Cavoukian's foundational principles ("Privacy as the Default"). The core idea behind data protection by default, as reflected in Art. 25(2) GDPR, is that controllers must ensure that, by default, they only process personal data which is strictly necessary to the specific purposes which they wish to achieve. Any further data which a controller might have an interest in processing should be conditioned upon the data subject taking a conscious action to allow this (namely, by providing consent). This applies also to further purposes for which those data might be processed[42] and further retention of those personal data, both of which should be kept to the strict minimum necessary unless otherwise decided by the individual. Practical considerations to develop this concept include:

- The adoption of a 'privacy-first' approach in the definition of the default settings in systems and applications which use personal data (ensuring that those settings only collect the minimal amount of data needed for the systems and applications to work as intended by the data subject);
- Providing actual choices to data subjects concerning how much of their data will be processed (and not processing more data than needed unless this is decided by the data subject);
- Ensuring that data are not automatically disclosed to the public without approval from the data subject; and
- In general, affording data subjects controls and options which allow them to exercise their rights under the GDPR, including to gain access to their data, to amend their data, to block any further processing of their data and to delete their data.[43]

---

[41] UK Information Commissioner's Office, 'Data protection by design and by default' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/> accessed 23 January 2020.

[42] See also in this respect the so called 'compatibility test', GDPR, art 6(4).

[43] ibid 'What is data protection by default?'.

The GDPR requires controllers to consider the combination of data protection by design and data protection by default. The practical enactment of these concepts is therefore identified as the second step within the development and implementation of a Data Protection Compliance Framework, complementing the first (accountability). This second step asks controllers to effectively apply data protection principles in the design of their processes and systems. In order to be able to do so, entities need to perform a systematic risk assessment on the data processing activities. After having carefully analysed the data processing and assessed the potential risks for the rights and freedoms of the individuals (see Section 4.3), controllers can start designing data processing operations which comply with the fundamental principles set forth in Art. 5 GDPR. Achieving this creates the material compliance foundation from which elements to demonstrate compliance (such as documented risk and data protection impact assessments, drafted information notices, and analyses of third-party providers and tools) can be drawn, in furtherance of the principle of accountability.

C. Step 3: Risk Assessments, Data Protection Impact Assessments and Security

i. Risk Assessments and Data Protection Impact Assessments

As anticipated in the previous section, it is not possible to effectively implement data protection principles into an entity's processes, systems, products, or services without performing prior and complete assessments of the potential risks to the rights and freedoms of data subjects which may be involved. It is through identifying and addressing those risks that the implementation of data protection by design and by default can be achieved. In the Introduction, we highlighted that one of the game-changers of the GDPR is that it establishes the need for a risk-based approach. In fact, according to Art. 24 GDPR, it is mandatory for controllers to evaluate the data protection risk per each data processing activity that they carry out. In this respect, the Irish Data Protection Authority specifies that "*[m]aintaining a data protection risk register can allow you to identify and mitigate against data protection risks, as well as demonstrate compliance in the event of a regulatory investigation or audit*."[44] Furthermore, when the data protection risk is high, Art. 35 GDPR prescribes an obligation to carry out a 'data protection impact assessment' ('**DPIA**').

[44] DPC, 'Risk based approach' (n 5).

Let's start from the latter. A DPIA can be seen as a more thorough form of privacy risk assessment.[45] Through a DPIA, a controller can assess a single processing operation (or multiple operations which are similar in terms of nature, scope, context, purpose and risks),[46] as well as technology products, tools, and systems, in order to identify inherent risks in a structured manner. A DPIA can also be used to identify measures which can be taken to bring those risks down to acceptable levels. DPIAs should contain, at least, a systematic description of the envisaged processing operation(s), the purposes for which personal data will be processed, an assessment of the legitimate interests pursued by the controller (where applicable – more on this below),[47] an assessment of the necessity and proportionality of the operation(s) in relation to those purposes, an assessment of the risks to the rights and freedoms of data subjects, and a description of the measures envisaged to address those risks, as noted in Art. 35(7) GDPR.

In practical terms, controllers should:

- Identify the purposes for which personal data will be processed, in connection with the operation under assessment.
- Identify the categories of data subjects concerned, as well as the categories of personal data which will be processed (in particular, whether any special categories of personal data,[48] under Art. 9 GDPR, or personal data relating to criminal convictions and offences, under Art. 10 GDPR, will be processed), should be identified, along with the sources used to collect the personal data to be processed.
- Identify any categories of individuals or entities who foreseeably may receive these personal data in connection with the assessed operation should be identified, including persons authorised by the controller to process personal data (such as the controller's employees),and also engaged processors or other controllers.
- Confirm that they have duly assessed all processors involved, to ensure that they offer sufficient guarantees of security and overall compliance with the GDPR. The controllers should also confirm that

[45] Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' WP248 Rev.01 (4 October 2017) 4 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236> accessed 23 January 2020 (Art. 29 Working Party DPIA Guidelines).

[46] ibid 7.

[47] *See*, s. IV.E.i.f.: Legitimate interests pursued by the controller or a third party.

[48] *See*, s. IV.E.ii.: Special categories of personal data and personal data relating to criminal convictions and offences.

an appropriate data processing agreement has been entered into with each processor (meeting the requirements of Art. 28 GDPR)[49] and that each processor has been logged in the controller's records of processing activities.[50]

- Identify other controllers which may receive the data should be identified as either joint[51] or autonomous controllers. A specific legal basis[52] justifying the communication of personal data to each other controller must be identified. It should be confirmed that each other controller has also been logged in the controller's records of processing activities.
- Identify specific retention periods for the personal data processed, along with a justification for those periods. A description of the procedure which will be used to ensure that those data will be erased, anonymised or, at least, restricted from further processing once the applicable retention period has expired should be given.
- Identify the specific assets through which personal data may be processed (including hardware, software, any operations carried out by non-automated means and an identification of the specific teams and departments within the controller which will process those data).
- Further analyse the specific processing purposes identified in order to demonstrate that they are specific (clear and unambiguous), explicit (able to be communicated in a clear and understandable manner to data subjects), legitimate (not unlawful) and coherent (accurately reflecting the actual purposes for which data are sought to be used).

---

[49] GDPR, art 28 requires controllers and processors to regulate their data processing relationship by means of a written agreement, which must contain a set of minimum obligations listed under the various sub-paragraphs of GDPR, art 28(3).

[50] Maintaining a record of processing activities, meeting the requirements of GDPR, art 30, is a fundamental accountability tool for controllers and processors, in that it allows the mapping out of all activities carried out using personal data in a manner identifying specific terms which demonstrate compliance with the various requirements of the GDPR (for example, the purposes of processing which were defined, the categories of personal data processed, the retention periods applied, the transfers of those personal data which may be carried out, and more) per processing activity.

[51] Two controllers will be considered joint controllers if they jointly determine the purposes and means for which personal data are processed, under GDPR, art 26. In this case, they must enter into an arrangement between them through which they transparently determine their respective responsibilities for compliance with the GDPR obligations upon controllers regarding the processing activities which they jointly carry out, and make the essence of this arrangement available to data subjects.

[52] *See*, s. IV.E.: Step 5: Legitimate basis.

A suitable legal basis should be identified for each of the purposes,[53] along with applicable derogations under Art. 9, 10 or 22 GDPR, as appropriate.

- Document its assessment as to whether the intended processing of personal data is adequate, relevant and limited to what is necessary in relation to the identified purposes should be documented. In particular, the controller should describe the tools, procedures or technology in place to ensure this in practice.
- Confirm that a suitable information notice, containing all of the minimum information requirements listed under Arts. 13 or 14 GDPR (as appropriate),[54] has been drafted and can be shared with the data subjects concerned.
- Confirm that a procedure exists to allow data subjects to effectively exercise their data subject rights[55] in connection with the processing activity under assessment, including a description of how those rights can be exercised in practice.
- To the extent that the processing operation will involve the transfer of personal data to countries outside of the European Economic Area ('**EEA**'), the controller should identify the manner in which it ensures that those transfers remain lawful under the GDPR.[56]

At the end of this descriptive process, the controller must perform a comprehensive analysis of the risks to the rights and freedoms of data subjects represented by the processing activity under assessment. Such risks are indicated in Recital 75 GDPR[57] and include processing activities that may

---

[53] In particular, where the controller relies on its legitimate interests as a legal basis for a processing purpose, it must ensure that it has carried out an appropriate 'balancing test' or 'legitimate interests assessment' beforehand. *See*, s. IV.E.i.f.: Legitimate interests pursued by the controller or a third party.

[54] *See*, s. IV.D.: Step 4: Information to the data subject.

[55] *See*, s. V.F.: Step 6: Data subject rights.

[56] GDPR, art 44 establishes that any transfers of personal data to countries outside the EEA, or to international organisations, can only take place, as a rule, where the recipient has received an adequacy decision issued by the European Commission (GDPR, art 45), where appropriate safeguards are put in place (GDPR, art 46, including standard contractual clauses approved by the European Commission) or where a derogation can be applied to the specific transfer (GDPR, art 49).

[57] The 173 Recitals of the GDPR are very useful to better understand the intentions behind each of the GDPR's provisions, at the time of enactment. While these Recitals are not 'hard law' (in the sense that only the actual provisions of the GDPR create legal obligations or rights), they serve an important interpretative and integrative purpose in this sense, and are often relied on by supervisory authorities and courts to develop and support legal arguments on the GDPR's rules. In this sense, it is important to also consider relevant Recitals when seeking to understand what is required from a provision within the GDPR.

give rise to: discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage. The GDPR does not prescribe a specific, objective methodology which must be used by controllers in the DPIA exercise.[58] However, controllers may wish to leverage and adapt existing and acknowledged methodologies for risk assessment in the sphere of data protection, such as those developed by the European Union Agency for Cybersecurity ('**ENISA**') for the assessment of severity of personal data breaches.[59] Controllers shall highlight the different categories of potential risks which may arise from the processing activity under assessment[60] and use ENISA's criteria on the definition of severity levels for personal data breaches[61] to calculate a level of impact for each identified risk (or leverage other criteria deemed appropriate for the purpose, insofar as these are based on reasonably objective and relevant factors) and assign an estimated level of

---

[58] It is worth underlining that the Commission Nationale de l'Informatique et des Libertés (CNIL – the French Data Protection Authority) has provided a tool to carry out the DPIA: The PIA software <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment>. Moreover, there is an international standard which also provides guidelines for privacy impact assessment: ISO/IEC 29134:2017 <https://www.iso.org/standard/62289.html> accessed 23 January 2020.

[59] European Union Agency for Network and Information Security, 'Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches' (20 December 2013) <https://www.enisa.europa.eu/publications/dbn-severity> accessed 23 January 2020.

[60] GDPR, Recital 75 gives some guidance in this respect: "*The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.*"

[61] ENISA, 'Recommendations for a methodology of the assessment of severity of personal data breaches'(n 59) 3-6. This assessment leverages three different criteria to reach a final severity level: the Data Processing Context (addressing the type of data concerned, as well as the overall circumstances of the processing activity), Ease of Identification (how easily the identity of individuals can be deduced from the data concerned) and Circumstances of Breach (which, when applied to the risk analysis in the context of a DPIA, should address the specific circumstances under which each risk may materialize, including as a result of a personal data breach).

likelihood that each identified risk will actually occur. Any relevant aggravating factors affecting the potential impact of the risks identified should also be included in this assessment.[62] The culmination of this analysis will be the identification of specific risk levels for each of the identified risks. Depending on the criteria used, these levels may range anywhere from low risks (which may be considered acceptable) to high risks (which will be found unacceptable and require immediate mitigation). Following this process of risk analysis, the controller will then need to identify measures to mitigate each specific risk which has been assigned a relevant risk level, and then recalculate that risk level considering the effect of the mitigation measures proposed.[63]

The controller should ensure that it documents all DPIAs it performs. However, a concluded DPIA will not become a static proof of assessment. An inevitable component of this exercise is the possibility of a change in the risks represented in the initial DPIA, as a result of changes in the context in which the processing activity is performed (eg, changes to the personal data collected, new vulnerabilities discovered in the technology implemented to process those data, changes to the manner in which personal data will be handled). As such, Art. 35(11) GDPR requires controllers to review completed DPIAs whenever necessary to address changes to the level of risk represented by the assessed processing activities.[64]

---

[62] For example, where special categories of personal data, personal data related to criminal convictions or offences, electronic communications data, location data, financial data or other sensitive data are involved, where the processing activity under assessment involves the use of personal data to profile individuals (such as by assessing personal data in order to analyse or predict aspects concerning those individuals' performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements), where the data subjects concerned are particularly vulnerable (eg, employees, patients, minors), where a significant amount of personal data are processed or where a large amount of data subjects are affected.

[63] Under GDPR, Recital 94 and art 36, where a DPIA indicates that the processing would result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the controller will be required to suspend the processing activity under assessment and reach out to the competent supervisory authority for prior consultation. Through this process, the supervisory authority will provide written advice to the controller, as well as exercise any of its investigative, corrective, or advisory powers, to ensure that the processing activity in question is configured in a manner which is aligned with the GDPR.

[64] Art. 29 Working Party DPIA Guidelines, 14: "*Data processing operations can evolve quickly and new vulnerabilities can arise. Therefore, it should be noted that the revision of a DPIA is not only useful for continuous improvement, but also critical to maintain the level of data protection in a changing environment over time. A DPIA may also become necessary because the organisational or societal context for the processing activity has changed, for example because the effects of certain automated decisions have become more significant, or new categories of data subjects become vulnerable to discrimination.*

It should be noted that the obligation to perform a DPIA is of a relatively limited scope. Art. 35 GDPR requires controllers to carry out DPIAs whenever they are faced with a processing activity which is likely to result in a high risk to the rights and freedoms of individuals, and provide three cases where a DPIA is considered mandatory:1. systematic and extensive evaluations of personal aspects relating to natural persons which are based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning natural persons or similarly significantly affect natural persons; 2. processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences; or 3. systematic monitoring of publicly accessible areas on a large scale.[65]

The Article 29 Working Party has developed the concept of 'likely to result in a high risk' in this context, by producing a list of nine criteria which should be considered by controllers in their assessment as to whether or not a DPIA should be carried out for a particular operation:

1. Evaluation or scoring;
2. Automated-decision making with legal or similar significant effect;
3. Systematic monitoring;
4. Sensitive data or data of a highly personal nature;
5. Data processed on a large scale;
6. Matching or combining datasets;
7. Data concerning vulnerable data subjects;
8. Innovative use or applying new technological or organisational solutions; and
9. When the processing in itself "*prevents data subjects from exercising a right or using a service or a contract*"; specifying that "*[i]n most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out*".[66]

Each of these examples could be an element that leads to a change of the risk resulting from processing activity concerned. Conversely, certain changes could lower the risk as well. For example, a processing operation could evolve so that decisions are no longer automated or if a monitoring activity is no longer systematic. In that case, the review of the risk analysis made can show that the performance of a DPIA is no longer required. As a matter of good practice, a DPIA should be continuously reviewed and regularly re-assessed".

[65] *See*, GDPR, art 35(3).

[66] Art. 29 Working Party DPIA Guidelines 9-11 (*see*, 11-12 for examples of the application of these criteria in practice).

Furthermore, as established in Art. 35(4) GDPR, supervisory authorities are allowed to develop 'DPIA blacklists' (lists of processing activities for which a DPIA will always be required)[67] and 'DPIA whitelists' (lists of processing activities exempt from the performance of a DPIA), which should also be taken into account by controllers, depending on the territorial scope of the intended processing activity.

However, the risk-based approach to compliance which is required of controllers does not allow them to limit the assessment of the risks to the processing activities which are considered as triggering the obligation for the performance of a DPIA. In fact, it will be difficult for a controller to accurately judge whether or not a DPIA is required for each of the different processing activities it carries out without comprehensively carrying out an assessment of the risks to the rights and freedoms of individuals inherent to every single one of its processing activities. Art. 24 GDPR emphasises the broad span of this risk-based approach, which must permeate each of the processing activities performed by the controller – it does so by requiring controllers to assess the circumstances of their processing activities and the resulting risks of varying likelihood and severity for the rights and freedoms of individuals and, consequently, implement appropriate technical and organisational measures to ensure compliance with the GDPR (and be able to demonstrate that compliance).

Therefore, controllers are required to specifically assess the relevant risks involved in each of their processing activities. They are also required to document this assessment in order to demonstrate that appropriate measures have been put in place, to ensure that those activities are carried out in alignment with the GDPR's data protection principles. Finally, controllers are required to trigger a more complete DPIA exercise in the event that this assessment unveils the existence of likely high risks, under Art. 35 GDPR. For this purpose, controllers may leverage the methodology used to analyse risks in the context of the performance of a DPIA; if an assessed processing activity reveals that these risks are high (according to the scale used by the controller, and considering any relevant aggravating factors), then that analysis can be leveraged and complemented with the aforementioned descriptive elements in order to convert the risk assessment into a full-fledged DPIA, along with proposed mitigation measures.

---

[67] *See*, European Data Protection Board's Opinions 1 to 28/2018, 1 and 2/2019, 6 and 7/2019 <https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en> accessed 23 January 2020.

Both DPIAs and risk assessments are means for the controller to analyse risks inherent to its processing activities for data subjects and, where necessary, identify and implement appropriate mitigation measures to reduce those risks to acceptable levels. By documenting and reviewing these assessments periodically, and whenever deemed necessary due to relevant changes in the underlying activities, controllers generate tools by which they can not only ensure that those activities remain in compliance with the GDPR, but also demonstrate how the controller has addressed any relevant risks in order to guarantee this compliance, in furtherance of the principle of accountability. Additionally, by performing these assessments prior to the start of an intended processing activity, the controller is able to preventively identify relevant risks and address them. This will also allow the controller to make sure that the activity is configured so as to meet the requirements of all data protection principles from the outset. As such, DPIAs and privacy risk assessments are undoubtedly effective tools in the implementation of data protection by design and by default.

ii. Technical and organisational security measures

Art. 32 GDPR is another reflection of the GDPR's risk-based approach. In fact, Art. 32 GDPR can be seen as a specification of the obligations laid down under Art. 24 GDPR. In order to define and implement appropriate technical and organisational security measures, controllers and processors are required to take into account the available technology (including the state of the art and the costs of implementation), the circumstances under which the controller/processor processes personal data and the risks which may result to the rights and freedoms of individuals (particularly, those which may result from the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data), with the end-goal of ensuring a level of security appropriate to those risks. The GDPR does not prescribe specific security measures that each and every controller or processor must implement in order to comply with the principle of security. Instead, it lists examples which may be considered, if and insofar as they are judged to be appropriate by the controller or processor:

- The pseudonymisation[68] and encryption of personal data;

---

[68] See the definition of 'pseudonymisation' in GDPR, art 4(5): "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*". It should be noted that, under GDPR, Recital 26, "*[p]ersonal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional*

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner, in the event of a physical or technical incident; and
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The definition of appropriate security measures is logically subsequent to the carrying out of an assessment of "*the risk of varying likelihood and severity for the rights and freedoms of natural persons*"[69] potentially involved in the processing activities undertaken by the controller or processor. This further highlights the importance of risk assessments and DPIAs (see Section 4.3.1) as means to demonstrate that the security measures chosen by a controller or processor to protect personal data have been deliberately and cautiously selected, in order to address specific and identified risks for data subjects (in compliance with the principle of accountability, see Section 4.1).

The risk-based approach offers a great amount of freedom to controllers and processors in deciding the most appropriate means to secure the personal data processed. However, it also creates uncertainty as to whether or not the implementation of particular measures may lead to a "*level of security appropriate to the risk*",[70] as established in Art. 32(1) GDPR. In practice, even where comprehensive risk assessments are carried out, controllers and processors may not be fully sure of the recommended or best means to address any data protection risks identified. While adhering to internationally recognised information security standards, such as those of the ISO/IEC 27000 family, may provide a good data security baseline for controllers and processors in this respect, it is by no means a sure-fire way to ensure compliance with Art. 32 GDPR (as the specific processing activities carried out by those entities may generate particular data protection risks for individuals, which those standards may not be equipped to fully handle). In this respect, it is worthwhile for entities processing personal data to pay

information should be considered to be information on an identifiable natural person"; given the definition of personal data contained in GDPR, art 4(1), it can be concluded that pseudonymised personal data are still 'personal data', for the purposes of the GDPR, as opposed to anonymous data.

69 GDPR, art 32(1).

70 GDPR, art 32(1).

attention to relevant decisions handed down by supervisory authorities,[71] as well as existing guidance on security measures, to assist in the decision-making process.

As an example, ENISA has developed guidelines aimed at digital service providers,[72] which identify 27 different security objectives and list technical and organisational security measures which can be implemented to achieve each one. These measures are ranked, per security objective, in three different levels of sophistication:

- Level 1 reflects basic security measures, which may be implemented to reach the objective in question;
- Level 2 reflects industry standard security measures, which not only allow the objective to be reached, but also the review of the implementation of that objective (in the event of relevant changes or incidents);
- Level 3 reflects the state of the art, which are advanced security measures allowing for continuous implementation monitoring and structural implementation review, considering relevant changes, incidents, tests, and exercises, to proactively improve the implementation of those measures.[73]

Controllers and processors can select a sophistication level which is appropriate to address the risks they have identified, as well as the specific characteristics of their organisation (such as size, resources and services).

Another example is provided by the French supervisory authority, the Commission Nationale de l'Informatique et des Libertés ('**CNIL**'), which has produced a guide to list the basic precautions which controllers and processors should systematically implement when managing the risks to data subjects presented by their processing activities. This guide is also aimed at helping to select measures to ensure a level of security appropriate to those risks.[74] Topics addressed by this guide include:

---

[71] *See*, s. VI: Decisions rendered by supervisory authorities on the monitoring and enforcement of the GDPR.

[72] European Union Agency for Network and Information Security, 'Technical Guidelines for the implementation of minimum security measures for Digital Service Providers' (16 February 2017) <https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers> accessed 23 January 2020.

[73] ibid 11. Naturally, given that these guidelines were drafted in 2017, it should be noted that the 'state of the art' is likely to have evolved since.

[74] Commission Nationale de l'Informatique et des Libertés, 'Security of Personal Data' (*The CNIL's Guides–2018 Edition*) <https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf> accessed 23 January 2020.

- The raising of user awareness on each organisation's privacy and security challenges;
- The management of data and system access rights assigned to users (including the definition of those rights in a manner which ensures effective compliance with the principle of data minimisation, and the logging of access to personal data);
- The management of security incidents and personal data breaches;
- Measures which can be implemented to secure workstations, mobile equipment, internal networks, servers and websites;
- Backup policies and secure data archiving;
- The performance of maintenance on data processing systems and the secure destruction of data;
- The management of processors and transmissions of data to other organisations;
- The physical security of premises;
- Data protection by design and by default; and
- Measures to ensure the integrity, confidentiality and authenticity of personal data.

While the above guidance may be useful in assisting controllers and processors in correctly moulding their security posture, blind adherence to any sort of guidance on security measures is not a valid means of ensuring compliance with Art. 32 GDPR or, more generally, with the principle of accountability (see Section 4.1). Controllers (and processors) should rely on a systematic methodology when choosing their security measures. This implies carrying out a complete assessment of the risks for the rights and freedoms of data subjects presented by their processing activities and selecting the security measures which are deemed to be most appropriate, in terms of their effectiveness and costs of implementation, to sufficiently mitigate those risks. Controllers and processors will be held accountable for their decisions in the event of an inspection by a supervisory authority. Therefore, they must ensure that they are able to show that their security measures were chosen as a result of a ponderation of the risks (by documenting risk assessments carried out), and justify why those measures are deemed adequate in addressing the specific risks identified. Data security should be intended as an integral dimension to do business, both for the protection of the individuals concerned and for the protection of the integrity and reputation of the

business itself (see in this respect the next Section 4.3.3. on Personal data breach management).[75]

iii. Personal data breach management

'Personal data breach' is defined, under Art. 4(12) GDPR, as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*." In other words, personal data breaches are security incidents which have a relevant impact on personal data.[76] As noted above concerning Art. 32 GDPR, when defining appropriate technical and organisational security measures, risks arising from the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data must be specifically taken into account, under Art. 32(2) GDPR. It is further relevant to highlight, as done by Recital 85 GDPR, that "*[a] personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned*". A key element of any appropriate personal data security policy is, therefore, the ability to prevent and detect personal data breaches, as well as react to occurred breaches in a timely and compliant manner.[77]

The concept of 'personal data breach' is quite vast. Broadly speaking, personal data breaches can be classified as:

1. confidentiality breaches (where there is an unauthorised or accidental disclosure of, or access to, personal data);

---

[75] See also on security the very recent publication of the European Union Agency for Network and Information Security, 'Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity' (16 April 2019) <https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/> accessed 23 January 2020, which is a report concerning human aspects of cybersecurity including not only psychology and sociology, but also ethnography, anthropology, human biology, behavioural economics, and any other subject that takes humans as its main focal point.

[76] Article 29 Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679' WP250 Rev.01 (6 February 2018) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052> accessed 23 January 2020 (Art. 29 Working Party Data Breach Notification Guidelines) p. 7: "*(…) in essence, whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches*".

[77] ibid 6.

2. integrity breaches (where there is an unauthorised or accidental alteration of personal data); and
3. availability breaches (where there is an accidental or unauthorised loss of access to, or destruction of, personal data), or any combination of these.[78]

In practice, events ranging from mere and simple human error (such as where an e-mail containing personal data is accidentally sent to the wrong recipient, or where a USB drive containing personal data is lost) to malicious interference with an organisation's processing systems (such as a targeted cyberattack through which personal data are encrypted and held for ransom) may qualify as a personal data breach under the GDPR.

Controllers and processors alike are therefore strongly recommended to develop and implement internal policies and procedures to ensure effective management of personal data breaches, alongside the security measures which they have defined with an aim to prevent breaches from taking place (including technical means to prevent and detect breaches, but also efforts to raise employees' awareness on the risks inherent to personal data breaches and rules on the acceptable use of an organisation's systems and devices[79]). The key objectives to be met, from the data protection perspective, are:

- The detection of relevant security incidents;
- The assessment of relevant security incidents (in terms of whether or not they may qualify as a personal data breach, and in terms of the severity of their impact to the rights and freedoms of data subjects affected);
- The notification to the relevant supervisory authority and communication to data subjects (where relevant);
- The documentation of personal data breaches managed; and
- Review.

Rules and specific channels on the reporting of security incidents or abnormal events should be clearly defined. In particular, organisations should consider reliance on an electronic form or dedicated e-mail through which information on a detected incident or event can be reported internally. All employees and other persons working within the organisation of

[78] ibid 7-8.
[79] See also in this respect ENISA, 'Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity' (n 75).

a controller and processor should be made aware, in understandable terms, of the types of occurrences which may qualify as a reportable security incident (eg, by providing them with examples which the controller or processor deems most common and understandable, considering the processing activities developed by the organisation).Organisations may also, for example, detect irregularities by using certain technical measures, such as data flow and log analysers, which make it possible to define events or alerts by the use of log data that has been collected.[80] It is further possible that organisations receive reports of relevant incidents and events from outside their organisation, such as from data subjects or business partners (for example, where a customer reports that he/she has unduly received personal data belonging to another person from the organisation). Organisations should be prepared to handle such external reports.

A team of competent individuals (including, preferably, the data protection officer[81] and members of the organisation's information/physical security departments), which can be referred to as the 'Data Breach Assessment Unit', should be identified. All internal or external reports of relevant security incidents and events should be relayed to this team. The first task of the Data Breach Assessment Unit is to carry out and document a preliminary analysis of each and every reported incident or event, to establish whether or not a personal data breach has occurred. This will involve liaising with the reporter and other departments and functions within and outside the organisation, as appropriate, to gather all information which may be relevant in order to complete the analysis (eg, date of occurrence of the event, date and time on which the organisation became aware of the event, source of the report, identification of systems affected, description of categories of documents or records affected, description of categories of personal data which may have been affected). From the data protection perspective, one of two results may arise from this assessment:

- **False positive.** The reported incident or event did not actually take place, or did not actually impact any personal data stored, transmitted or processed by the organisation. This finding will close the incident management process. The organisation should use the case to refine its internal rules on the detection of false positives, so that future, similar incidents are more readily classified as such (and do not necessarily trigger the incident management process in full). In any case, false positives should be recorded in a 'personal data breach

[80] Art. 29 Working Party Data Breach Notification Guidelines, 10.
[81] On the data protection officer, *see* GDPR, arts 37-39 and Art 29 Working Party DPO Guidelines (n 16).

register" kept by the organisation, which will be used to log any reported events and document the actions taken by the organisation to address each one, so as to show that they have been properly handled under the GDPR's rules.

- **Personal data breach.** The reported incident or event is an actual security incident, and it had an impact on personal data processed, stored or transmitted by the organisation (eg, personal data has been disclosed to an unauthorised third party, access to personal data has been lost, or personal data has been altered without permission). This finding will trigger an escalation of the analysis performed on the personal data breach occurred.

The finding that a personal data breach has taken place will create a need for a second level of assessment for controllers. In this second level, the assessment (which must be documented) will focus on the actual and potential risks resulting from that breach to the rights and freedoms of the data subjects affected, in order to:

1. Determine to what extent it is required, under the GDPR, to notify the personal data breach to a competent supervisory authority, as well as communicated to the data subjects affected; and
2. Establish the most appropriate mitigation measures which may be implemented in order to reduce the risks and damages which have been identified.

While the controller's Data Breach Assessment Unit may also be tasked with this second-level analysis, it is recommended that the team involved be expanded to include representatives of other teams and departments within the controller, including the managers of the specific departments affected by the breach and members of the controller's highest level of management, given the significance of the decisions which may need to be taken in order for a breach to be definitively addressed. This expanded team may be referred to as the 'Data Breach Management Unit'.

The main task to be carried out by the Data Breach Management Unit is to perform a specific and targeted risk assessment on the occurred personal data breach, relying on the information gathered by the Data Breach Assessment Unit. Further input may be collected from relevant stakeholders, if needed. Breaches should be classified in accordance with pre-determined

categories,[82] after which they should be classified in terms of the level of risk posed to the data subjects concerned. This targeted risk assessment can be carried out in a similar fashion as described above,[83] only it will seek to focus on specific risks arising from a concrete breach occurred, rather than addressing any and all risks which may potentially arise from a given processing activity. The Data Breach Management Unit should, in particular, focus on the impact and likelihood of occurrence of the risks on data subjects described in Recital 85 GDPR,[84] as well as on relevant aggravating factors.[85]

To help this assessment along, the Data Breach Management Unit may rely on the aforementioned ENISA's *Recommendations for a methodology of the assessment of severity of personal data breaches* (20 December 2013),[86] which have been specifically developed to provide organisations with an objective process through which to assign a level of severity to a specific personal data breach. This is done by assigning concrete values to three different criteria, depending on the specific personal data breach occurred:[87]

- **Data Processing Context (DPC)**: Addresses the type of the breached data, along with other factors related to the overall processing context. This is the core criterion of this methodology, and is used to evaluate the criticality of the affected dataset.
- **Ease of Identification (EI):** Determines how easily data subjects can be identified from the affected dataset. This serves as a correcting factor to the Data Processing Context, given that the overall severity of a personal data breach is strongly linked to the degree to which the affected data allow the respective data subjects to be identified.

---

[82] Organisations may consider the simpler confidentiality/integrity/availability classification mentioned above, the classification provided by GDPR, art 4(12) (unlawful destruction of personal data, unlawful loss of personal data, unlawful modification of personal data, accidental destruction of personal data, accidental loss of personal data, accidental modification of personal data, unauthorised disclosure of personal data, unlawful access to personal data), or any other form of classification deemed appropriate.

[83] *See*, s. IV.C.iii.: Risk assessments and data protection impact assessments.

[84] Discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation measures, significant economic or social disadvantages, deprivation or limitation of rights or freedoms, loss of control over personal data, and other physical, material, or non-material damages which may be suffered by individuals.

[85] *See*, s. IV.C.iii.: Risk assessments and data protection impact assessments.

[86] ENISA, 'Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches' (n 59).

[87] ibid 3.

- **Circumstances of Breach (CB):** Addresses the specific terms under which the breach took place, concerning the type of breach occurred and whether any malicious intent was involved. This criterion will come into play where specific circumstances pertaining to the breach add to its severity.

The final severity score (SE) assigned to a breach will be the result of the values assigned to the three aforementioned factors: **SE = DPC x EI + CB**. Based on the final severity score, organisations will be able to assign an objective overall risk level to an occurred breach, ranging from low to very high, which will determine the further actions which may need to be taken (in terms of mitigation and compliance with notification requirements).[88] Having assigned an overall level of risk to a personal data breach, the Data Breach Management Unit must define and implement any further measures which are found to be appropriate to mitigate the impact of the breach on the data subjects affected.

A decision must also be taken as to the extent to which the organisation must comply with relevant notification and communication obligations. Under Art. 33(1) GDPR, controllers are required to report any personal data breaches they detect to the competent supervisory authority[89] within 72 hours of becoming aware of the breach,[90] unless the personal data breach in question is deemed unlikely to result in a risk to the rights and freedoms of individuals.[91] Art. 33(2) GDPR describes the minimum content which these notifications should include.[92] Controllers should note that, in the event

---

[88] ibid 6.

[89] Art. 29 Working Party Data Breach Notification Guidelines, 17: "*(…) whenever a breach takes place in the context of cross-border processing and notification is required, the controller will need to notify the lead supervisory authority. Therefore, when drafting its breach response plan, a controller must make an assessment as to which supervisory authority is the lead supervisory authority that it will need to notify*".

[90] ibid 10-11: "*WP29 considers that a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised*".

[91] The Article 29 Working Party has provided examples of situations where a notification to a supervisory authority may not be required, including a case where a USB key containing an encrypted backup of personal data is stolen (provided that the encryption is not compromised) and a brief power outage of several minutes at a call centre prevents customers from calling the controller and accessing their records – ibid 31. Another example may include a case where an e-mail containing non-sensitive personal data is sent to a wrong recipient, but that recipient is a trusted business partner and provides assurances that the received personal data have been deleted, without any further copies having been made.

[92] A description of the nature of the personal data breach (including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned), the name and contact details of the controller's data protection officer or other point of contact, a description of the likely consequences of the personal data breach (as assessed by the controller), and a description

that they are unable to provide all required information within the first 72 hours, they should still provide all relevant information at their disposal to the supervisory authority within that deadline and update the notification made with additional details as they become available, justifying the need for this to the supervisory authority ('notification in phases').[93] Under exceptional circumstances, controllers may be able to delay their first notification beyond this deadline (such as where a controller experiences multiple, similar confidentiality breaches over a short period of time, affecting large numbers of data subjects in the same way, and considers it less burdensome to submit a 'bundled' notification representing all of those breaches),[94] as long as they are able to provide a reasonable justification for this to the supervisory authority at the moment of notification. However, whenever feasible, controllers should give preference to notification in phases, as supervisory authorities may disagree with the justification given by the controller for the delay (potentially leading to the imposition of corrective measures, including administrative fines, for failure to notify in a timely manner).

Moreover, according to Art. 34 GDPR, if a controller's assessment of the severity of a personal data breach indicates a high level of risk to the rights and freedoms of individuals, the controller will also, as a rule, be required to directly inform the affected individuals of the occurred breach, without undue delay (though not subject to the 72-hour deadline mentioned above). In accordance with the principle of transparency, any information provided should contain clear and plain language, and describe:

- The nature of the personal data breach;
- The name and contact details of the controller's data protection officer (or other point of contact);

---

of the mitigation measures taken by the controller to address the breach (or those which the controller proposes to be taken).

93 Art. 29 Working Party Data Breach Notification Guidelines, 15: "*(…) the GDPR recognises that controllers will not always have all of the necessary information concerning a breach within 72 hours of becoming aware of it, as full and comprehensive details of the incident may not always be available during this initial period. (…) Consequently, in many cases the controller will have to do more investigation and follow-up with additional information at a later point. This is permissible, providing the controller gives reasons for the delay, in accordance with Article 33(1). WP29 recommends that when the controller first notifies the supervisory authority, the controller should also inform the supervisory authority if the controller does not yet have all the required information and will provide more details later on. The supervisory authority should agree how and when additional information should be provided. This does not prevent the controller from providing further information at any other stage, if it becomes aware of additional relevant details about the breach that need to be provided to the supervisory authority*".

94 ibid 16.

- The likely consequences of the breach and the mitigation measures taken or proposed to be taken by the controller; and
- Any other information which is deemed relevant.

This information should be provided in a dedicated message sent to data subjects, rather than included in newsletters or regular updates.[95] Controllers may further need to ensure that the information is made available in alternative formats and relevant languages, with the purpose of allowing the data subjects affected to fully understand the information provided.[96]

There are also exceptions to the need to communicate personal data breaches to data subjects. Controllers may be exempt from this obligation in the event that they had applied appropriate technical and organisational measures to protect the affected data, in particular where those measures render them unintelligible to any unauthorised recipient (such as where the data were protected with state-of-the-art encryption or by tokenisation).[97] Controllers may further be exempt if they take steps to ensure that the high risk identified to individual's rights and freedoms is no longer likely to materialise, immediately after the breach has taken place (such as where the controller is able to take action against an individual unduly accessing personal data before they were able to do anything with those data, though this would still require an assessment of the risks posed by the fact that the confidentiality of those data were still breached, in any case).[98] Finally, controllers may be exempt from directly notifying data subjects in the event that this would involve a disproportionate effort on the part of the controller, or be impossible (such as where the controller no longer has access to contact details on the data subjects concerned). However, in this case, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner (such as by publishing the required communication on the controller's website).[99] In any case, controllers should note that, under the principle of accountability, they will be held accountable for their decision not to communicate a relevant personal data breach to the data subjects concerned. This means that they must be able to provide a reasoned assessment for this decision. Supervisory authorities may, however, disagree and order the controller to complete the direct

[95] ibid 21.
[96] ibid 21.
[97] ibid 22.
[98] ibid 22.
[99] ibid 22.

communication (as well as impose any corrective measures deemed appropriate for failure to communicate).[100]

Processors, on the other hand, are only required to communicate detected personal data breaches to the controller on whose behalf the processor was handling the affected data, under Art. 33(2) GDPR. Processors are not under any requirement to make a specific risk assessment pertaining to a personal data breach. Instead, once it has been established that a personal data breach has occurred, the appropriate controller(s) must be informed without undue delay.[101] Processors must then further cooperate with controllers as established in the terms of the data processing agreement entered into with them (in particular, to further investigate and collect information on the personal data breach in question). It should be noted that the 72-hour notification deadline for controllers to report to a supervisory authority, under Art. 33(1) GDPR, commences from the moment that a controller is aware that a personal data breach has occurred. After being informed that this has happened by a processor, the controller may undertake a short period of investigation in order to establish whether or not a breach has, in fact, occurred, to a reasonable degree of certainty – only after this investigation will the controller be considered 'aware', as such.[102]

The penultimate step is for controllers and processors to ensure that all relevant information on a personal data breach and the manner in which it was handled is documented in a register of personal data breaches, as set out in Art. 33(5) GDPR. This register should include all facts pertaining to the personal data breach, its effects and remedial action taken (including notification to the supervisory authority, communication to data subjects, and all technical and organisational mitigation measures applied), and should further reference the documented assessments carried out by the organisation during the management process (including the classification of the incident as a personal data breach, as well as the classification of the personal data breach in terms of category and severity level). As noted above, organisations should also record any false positives assessed in this register in order to demonstrate their assessment as to all reported incidents, under the principle of accountability.[103]

The final stage in the management of a personal data breach is the completion of a final collection of evidence and additional information gathered

[100] ibid 22.
[101] ibid 22.
[102] ibid 11.
[103] ibid 26.

on the incident. This evidence and information can be used to perform a 'post-breach analysis'. The purposes of this analysis will be to:

- Confirm the effectiveness of the actions taken during the management of the breach in question and identify areas of improvement; and
- Identify, on the basis of the root cause of the incident, adequate technical and organisational measures which can be implemented to reduce or eliminate the likelihood of similar incidents taking place in the future.

Given that, in general, the occurrence of a personal data breach is likely to trigger one of the most serious risks which an organisation has identified during the risk assessments carried out, it is essential to incorporate a functional and complete data breach management process within a Data Protection Compliance Framework. Controllers and processors should take into account their organisational structure, their previous experience with security incidents and personal data breaches, and the results of the risk assessments and DPIAs performed on their processing activities, in order to define processes to swiftly detect, assess, contain, notify, record and prevent personal data breaches, in furtherance of the principle of security. This will help to mitigate both risks to the relevant data subjects and legal risks to controllers, in terms of possible exposure to sanctions, damage claims and reputational damages.

D. Step 4: Information to the data subject

The fourth step in the development and implementation of a Data Protection Compliance Framework is also the first outward-focused step. It concerns the provision of complete and understandable information to data subjects on a controller's data processing practices, under the principle of transparency (and related principles, such as the principle of fairness). Openness and transparency are fundamental means by which controllers can show accountability towards data subjects and the community at large, by publicly stating the terms under which they will process personal data. Controllers, in this way, subject themselves to being held accountable for those statements.

The GDPR includes specific information requirements upon controllers. Other than the need to communicate high-risk personal data breaches to data subjects (as seen above),[104] and the need to facilitate the exercise of data subject rights (covered below),[105] controllers are also required to inform data

[104] *See*, s. IV.C.iii.: Personal data breach management.
[105] *See*, s. IV.F.: Step 6: Data subject rights.

subjects as to the specific terms under which their personal data will be processed (with varying requirements, depending on whether data is collected directly from data subjects or not).

In all of these cases, information should be provided efficiently and succinctly in order to avoid information fatigue on the part of data subjects. It should be clearly differentiated from non-privacy related information. The language used should be considered in order to ensure that it can be understood by an average member of the intended audience, avoiding unnecessary ambiguities and describing the information in as simple a manner as possible. Information should be provided directly to data subjects, or otherwise data subjects should be able to easily access the information when necessary. By default, information should be provided in writing, although other means can also be considered by controllers (such as electronic means and, where specifically requested by a data subject, orally). Finally, controllers must generally offer this information free of charge, and may not make any information provided under transparency requirements conditional upon financial transactions (such as the payment for, or purchase of, services or goods).[106] Given the inherent tension between the GDPR requirements of providing comprehensive information, and ensuring that the information provided is concise, transparent, intelligible, and easily accessible, controllers are required to perform their own assessment as to which information should be prioritised, what the appropriate level of detail is and which are the best means by which to convey this information to data subjects.[107]

The information requirements under Arts. 13 and 14 GDPR require the controller to develop appropriate information notices or privacy policies to communicate to data subjects relevant information as to the circumstances under which their personal data will be handled. One means of information provision which is particularly recommended in the online context is the use of the so-called 'layered approach'. This allows the controller to refrain from providing all required information to data subjects at once, and instead structure the information into relevant categories which the data subject can select, to ensure immediate access to the information deemed most relevant by the data subject and prevent information fatigue.[108] When designing layered privacy policies, controllers are recommended to include the most

---

[106] Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' WP260 Rev.01 (11 April 2018) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227> accessed 23 January 2020 (Art. 29 Working Party Transparency Guidelines) 6-13.

[107] ibid 18.

[108] ibid 19.

immediately relevant information to data subjects – the purposes of processing, the controller's identity and contact details, a description of the data subject's rights, and any information deemed relevant for data subjects to understand the consequences which may arise for them from the processing activities in question – within the very first layer. This allows data subjects to immediately perceive this information without needing to click further within the layered policy.[109] The UK Information Commissioner's Office has prepared more visual guidelines on the 'layered approach', which may help controllers to better understand the concept.[110] Further, controllers may wish to consider a 'layered approach' even outside of the online context. This could include providing abbreviated information to data subjects during telephone communications, referring them to an online privacy policy for more information (or directly e-mailing them the privacy policy during or after the call), as well as providing abbreviated paper-based notices to customers at physical stores, including a link to the more complete privacy statement made available online.[111]

With the above guidelines in mind, controllers should understand the specific information requirements to which they are subjected in relation to the data subjects whose data they process, and which vary according to the manner of collection of those data, under Arts. 13 and 14 GDPR.

i. Directly collected personal data

Art. 13 GDPR applies where a controller collects personal data directly from a data subject. This includes cases where the data subject actively submits the personal data in question to the controller, or the controller collects those personal data as a result of observations performed on the data subject. Although Art. 13 GDPR appears to be structured in such a way that the information of Art. 13(1) GDPR must always be provided, and the information of Art. 13(2) GDPR need only be provided where this is necessary to ensure fair and transparent processing, the Article 29 Working Party has stated that "*there is no difference between the status of the information to be provided under sub-article 1 and 2 of Articles 13 and 14 respectively. All*

[109] ibid 19.

[110] UK Information Commissioner's Office, 'What methods can we use to provide privacy information?' 'What is a layered approach?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/> accessed 23 January 2020.

[111] Art. 29 Working Party Transparency Guidelines, 20.

of the information across these sub-articles is of equal importance and must be provided to the data subject".[112]

The information which must be provided includes:[113]

- **The identity and contact details of the controller and, where applicable, the controller's representative in the EU.** This should allow the controller to be easily identified, and should preferably include multiple forms of contact details (eg, e-mail address, postal address, phone number, etc.);
- **Contact details for the data protection officer (if one has been appointed).** Note that the name of the data protection officer does not strictly need to be provided, though this may be seen as a best practice;
- **The purposes and legal basis for the processing.** Each specific identified purpose for which the data subject's personal data may be handled should be identified, along with the corresponding legal basis which has been identified to justify it. It should be easy for data subjects to make the connection between each specific purpose and the corresponding legal basis (as opposed to listing various processing purposes and then, separately and without establishing any connection to each purpose, listing various legal bases deemed applicable). Where special categories of personal data, or personal data related to criminal convictions or offences are processed, the appropriate derogation under Art. 9 or 10 GDPR should also be identified in the same manner. This applies also to derogations under Art. 22 GDPR, to the extent that any automated individual decision-making[114] is carried out.
- **Legitimate interests.** If the controller identifies its own legitimate interests, or those of a third party, as a legal basis for any of the defined processing purposes, it must identify the specific interest which is pursued. Controllers should also inform data subjects that they can obtain information on the 'balancing test' or 'legitimate interests assessment' carried out to justify the use of this legal basis,[115] and controllers should consider providing such information upfront as a best practice.

---

[112] ibid 14.
[113] Ibid 35-40.
[114] *See*, s. IV.F.vii.: Rights concerning automated individual decision-making.
[115] *See*, s. IV.E.i.f.: Legitimate interests pursued by the controller or a third-party.

- **Recipients of the personal data.** These include any individuals, companies, public authorities, agencies or any other bodies to which the personal data may be transferred (including other controllers, as well as processors engaged by the controller). The principle of fairness requires controllers to provide meaningful information to data subjects as to recipients, which generally requires them to be individually named. However, where the controller does not deem this to be appropriate, recipients may also be listed by category, by providing information which is as specific as possible on the type of recipients (referring to the activities performed by the recipient), the industry, sector, sub-sector and location of the recipients.
- **Transfers to third countries.** Controllers should identify any transfers of the personal data to outside of the EEA, or to an international organisation. Under the principle of fairness, the rule is that the specific third countries receiving the data should be named, whenever feasible. For each of the transfers identified, the controller must be able to quote the relevant GDPR article permitting the transfer and the corresponding mechanism to ensure its lawfulness (eg, adequacy decisions under Art. 45 GDPR, standard contractual clauses under Art. 46 GDPR, binding corporate rules under Art. 47 GDPR, an applicable derogation under Art. 49 GDPR). If applicable, information as to how data subjects can access or obtain the binding corporate rules, standard contractual clauses or other mechanisms relied on should be provided.
- **Retention periods.** Controllers should clearly identify the applicable retention periods concerning the personal data, by linking a retention period to each processing purpose and/or each category of data. Where it is not possible to define a specific retention period (meaning, it is not possible to define a fixed number of hours, days, weeks, months or years during which those data will be retained), the criteria used to determine the retention period should be identified as specifically as possible – it will generally not be considered valid to generically state that personal data will be kept "for as long as necessary" to meet a given purpose.
- **Data subject rights.** Controllers should provide information on the rights afforded to data subjects under the GDPR which is specific to the processing activities undertaken, explains what each right involves and describes the process by which those rights can be exercised. The right to object, in particular, must be explicitly brought to the data subject's attention and presented clearly and separately from

any other information. Further, if consent is identified as a legal basis, the right to withdraw consent must be included. Lastly, the right to lodge a complaint with a supervisory authority, in particular that of the Member State of the data subject's habitual residence, place of work or place of alleged infringement of the GDPR, must also be brought to the data subject's attention.

- **Mandatory or optional data provision.** Controllers should inform data subjects as to whether they are required (by law or by contract) to provide certain categories of data or not, and what the consequences of failing to provide these data may be. This includes an obligation to clearly differentiate between mandatory and optional fields in any online forms through which personal data are collected.
- **Automated individual decision-making.** Where the controller relies on automated individual decision-making, under Art. 22 GDPR, to process personal data, it must provide meaningful information about the logic involved (by finding a simple manner in which to explain the rationale and criteria relied on to reach these automated decisions, avoiding any overly complex explanations and with no requirement to disclose the actual algorithms involved), as well as the significance and envisaged consequences of this processing activity for the data subject (requiring the controller to inform the data subject as to how these decisions may affect them, providing real and tangible examples of the possible effects which may occur).

Under the principle of purpose limitation, controllers are required to stick to the specific purposes identified at the time of collection of personal data. Where a controller determines that a subsequent purpose for which it wishes to process personal data is compatible with the initial purpose, it must provide the data subject with the above information prior to carrying that additional purpose out, under Art. 13(3) GDPR.[116]

One of the key components of the principle of accountability, as noted above, is transparency. This applies not only at the point of data collection, but also throughout the processing lifecycle. Controllers should therefore adhere to the same transparency principles when updating or amending privacy policies and information notices as when they are first communicated by data subjects. Any material or substantive changes should be communicated directly to data subjects in a manner which ensures that they will be

[116] GDPR, art 6(4) provides a list of factors which must be assessed by controllers in order to determine whether two purposes may be considered compatible.

noticed.[117] It will not be valid to merely inform data subjects that they should regularly check a privacy policy for changes or updates, given the inherent unfairness to data subjects which this represents.[118]

ii. Indirectly collected personal data

Art. 14 GDPR establishes the information which must be communicated to data subjects, where personal data is not collected directly from those individuals, but from other sources (such as other persons, publicly available sources, and data brokers). While there is no need to inform data subjects in this case as to whether there are applicable statutory or contractual requirements to provide their personal data (given that, at the moment of provision of information, these data have already been collected by the controller), controllers are additionally required to inform data subjects as to:

- The categories of personal data which have been collected; and
- The source(s) from which the personal data originate (specific sources should be identified whenever possible, or otherwise general information about sources used should be provided, including their nature, whether public or private, and the type of organisation/industry/sector of the source).[119]

There is a general requirement under Art. 14(3) GDPR that this information be provided to the data subject within a reasonable period after the collection of his/her personal data, and no later than one month from that moment. This general time-limit may, however, be further curtailed in two situations:

1. Where the personal data are to be used for communication with the data subject (in which case, the data subject should be informed, at the latest, at the time when that communication is first carried out, but never later than one month from the collection of their personal data); and
2. Where the personal data are to be disclosed to another recipient (in which case, similarly, the data subject should be informed, at the

[117] Art. 29 Working Party Transparency Guidelines, 16-17. Examples of substantive and material changes include changes in processing purposes, the identity of the controller, or the manner in which data subjects can exercise their rights, as opposed to mere corrections of misspellings or stylistic/grammatical flaws.
[118] ibid 17.
[119] ibid 35-40.

latest, at the time when that disclosure is first carried out, but never later than one month from collection of their personal data).[120]

However, there are circumstances under which a controller may be exempted from providing this information to data subjects. In particular:

- Controllers are not required to provide this information where this is impossible. Controllers seeking to rely on this exception must be able to demonstrate factors actually preventing it from providing information to data subjects (and may be required to provide the information anyway at a later date, if those factors no longer exist).[121]
- This may also be the case where the provision of this information would represent a disproportionate effort for the controller (particularly where personal data are processed for archiving purposes in the public interest, scientific/historical research purposes or statistical purposes), due to factors which are directly connected to the fact that personal data was not obtained directly from the data subject. Controllers seeking to rely on this exception will need to carry out and document a specific assessment to balance the effort involved for the controller against the potential impact and effects on data subjects if this information is not provided.[122]
- It is also possible for controllers to avoid this obligation where the provision of information would be likely to render impossible or seriously impair the achievement of the objectives sought by the processing activity. In this case, controllers will need to demonstrate that the provision of this information would nullify those objectives.[123]

In these three cases, controllers must take appropriate measures to ensure the protection of the rights and freedoms of individuals regardless of the fact that this information is not directly provided to them, such as by making the information publicly available (eg, on the controller's website), as stated in Art. 14(5)(b) GDPR.

Controllers may further be exempted from this requirement if the obtaining or disclosure of those personal data is expressly laid down in EU or Member State law applicable to the controller. This may also apply where providing this information would conflict with professional secrecy

[120] ibid 15-16.
[121] ibid 29.
[122] ibid 30-31.
[123] ibid 31-32.

obligations regulated under EU or Member State law (such as those imposed upon doctors or lawyers), as laid down in Arts. 14(5)(c) and (d) GDPR.

The rules on providing information to data subjects concerning further processing activities, as well as material and substantive changes to information provided previously, apply equally to this situation as they do for the situation where personal data are collected directly from the data subject.

E. Step5: Legitimate basis

i. Legal bases for the processing of personal data

A fundamental step in the implementation of a practical framework for compliance with the GDPR is the correct identification of legal bases for each of the specific purposes for which personal data are processed. This is a direct result of the principle of lawfulness, established in Art. 5(a) GDPR, which requires all personal data to be processed lawfully. This is densified in Art. 6 GDPR: "*Processing shall be lawful only if and to the extent that at least one of the following applies*". Therefore, "*[w]hen initiating activities that involve processing of personal data, a controller must always take time to consider what would be the appropriate lawful ground for the envisaged processing*".[124] This requires a clear understanding of the scope and additional requirements that may need to be met in order to be able to validly rely on each legal basis under the GDPR, so that a controller can make the most appropriate choice regarding the purpose for which personal data are processed.

There are six different legal bases which a controller may, in abstract, rely upon to justify the processing of personal data for a given purpose:

- Art. 6(1)(a) GDPR: The data subject has consented to the use of their personal data for the specific purpose;
- Art. 6(1)(b) GDPR: Processing personal data is necessary to perform a contract with the data subject, or otherwise to take steps prior to entering into a contract at the request of the data subject;
- Art. 6(1)(c) GDPR: Processing personal data is necessary to comply with a legal obligation upon the controller;

[124] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' WP259 Rev. 01 (10 April 2018) 3 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> accessed 23 January 2020 (Art. 29 Working Party Consent Guidelines).

- Art. 6(1)(d) GDPR: Processing personal data is necessary to protect the vital interests of the data subject, or of another individual;
- Art. 6(1)(e) GDPR: Processing personal data is necessary to perform a task in the public interest, or in the exercise of official authority vested in the controller; or
- Art. 6(1)(f) GDPR: Processing personal data is necessary for the purposes of legitimate interests pursued by the controller.

There is no legal distinction made between the six legal bases, nor is there any suggestion of a hierarchy among them.[125] As long as the controller is able to validly rely on any given legal basis, the processing purpose in question will be lawful under the GDPR. Controllers must therefore carefully select the legal basis which appears most adequate to the circumstances of the processing activities they carry out, and reflect this choice in the information notices which are provided to data subjects (see Art. 13(1)(c) and 14(1)(c) GDPR). It is also generally recommended to reflect this choice also in the controller's records of processing activities, along with a justification for the choice made (even though this is not strictly required by Art. 30 GDPR) – this allows those records to accurately reflect all relevant information pertaining to the controller's processing activities, in order to allow them to act as an effective tool for accountability purposes (i.e., allowing the controller to demonstrate that an appropriate legal basis has been selected for each processing activity).

a. Consent

'Consent' is defined in Art. 4(11) GDPR as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or clear affirmative action, signifies agreement to the processing of personal data relating to him or her*". This definition highlights the various different requirements which must be met for consent to be considered valid under the GDPR:

- 'Freely given': There must be real choice and control on the part of data subjects in providing their consent. Data subjects must not be

[125] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' WP217 (9 April 2014) 10 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 23 January 2020 (Art. 29 Working Party Opinion 06/2014). This was said in relation to Art. 7 of Directive 95/46/EC of the EU Parliament and of the Council, of 24 October 1995 (the '**Data Protection Directive**'), the wording of which is functionally equivalent to the wording of GDPR, art 6(1).

compelled to consent in any way, or be subjected to negative consequences if they refuse to or withdraw their consent.[126] Consent will be considered invalid if there is any element of pressure or influence upon the data subject which prevents him or her from freely choosing whether or not to consent to a given processing purpose.[127] This precludes controllers from bundling requests for consent with the acceptance of terms and conditions. It also forbids making the provision of a service conditional upon consent – if the processing activities for which consent is asked are necessary in order for the service to be provided, then the controller should instead rely on Art. 6(1)(b) GDPR as a legal basis.[128] Whenever there is a relevant imbalance of power between the controller and data subject, so that the data subject may feel pressured into providing their consent (for example, in the case of employees vis-à-vis their employer), there is a presumption of invalidity of that consent.[129]

- 'Specific': The controller must clearly specify the purpose(s) for which consent is requested. This is in line with the principle of purpose limitation, set out in Art. 5(1)(b) GDPR. This is a requirement of granularity, so that data subjects are able to consent to specific, limited, and clearly defined purposes. This prevents controllers from making overly generic descriptions of purposes for which consent is asked. Examples include 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research', all of which, without further detail or concretisation, would be considered insufficiently specific.[130]

- 'Informed': A minimum set of information must be provided to data subjects prior to their granting of consent. In particular, data subjects must be informed as to the identity of the controller, the purpose for which consent is sought, the types of data which will be collected and used for that purpose, and the possibility to withdraw consent. If consent is being relied on to use personal data in order to make decisions related to the data subject which are based solely on automated processing of those data, and which may produce legal or similarly significant effects upon the data subject (Art. 22 GDPR), then the data

[126] Art. 29 Working Party Consent Guidelines, 5.
[127] ibid 5-6.
[128] ibid 8.
[129] ibid 7.
[130] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' WP203 (2 April 2013) 16 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 23 January 2020.

subject must also be given meaningful information about the logic involved, the significance of this processing, and the potential consequences for the data subject. Finally, if this consent is used to justify a transfer of personal data outside of the EEA (to a country not covered by an adequacy decision issued by the European Commission, and in the absence of appropriate safeguards to cover that transfer under Art. 46 GDPR), the data subject must also be informed of the possible risks involved.[131]

- 'Unambiguous indication of wishes': Consent must be provided by means of a clear affirmative statement or act. It must be obvious that the data subject has consented, by taking a deliberate action to agree to the particular processing.[132] The use of pre-ticked opt-in boxes, or implied consent (through silence or inactivity or the data subject), is invalid under the GDPR.[133] Whatever the method chosen by the controller to request consent, it must avoid ambiguity and ensure that the action by which consent is given can be distinguished from any other actions. Consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service,[134] or by simply continuing to make use of services or a website without giving any clear indication of consent (this affects the validity of, eg, pop-up banners asking for consent for the use of cookies, which state that consent will be presumed if the user continues to browse the website).[135]

One crucial point about reliance on consent as a legal basis is that, under Art. 7(3) GDPR, data subjects must be free to withdraw the consent given at any time, as easily as they granted it in the first place. If consent is withdrawn, the processing actions covered by consent must stop. If there is no other legal basis to continue processing those personal data, the data must be deleted or anonymised.[136] Consent is therefore not recommended as a legal basis for processing activities which require stability, given that consent can potentially be withdrawn at any moment and for any reason.

Controllers must be able to demonstrate that consent has been validly obtained under Art. 7(1) and Recital 42 GDPR, and in line with the principle of accountability under Art. 5(2) GDPR. There is no legally prescribed

---

[131] Art. 29 Working Party Consent Guidelines, 13.
[132] ibid 15-16.
[133] ibid 16.
[134] ibid 16.
[135] ibid 17.
[136] ibid 22.

method to do so. Controllers are responsible for choosing appropriate means to collect and document the collection of consent. Examples include keeping records of consent statements or, in an online context, logs of user sessions in which consent was expressed (together with documentation of the methodology used to obtain consent and the information which was provided to the user at the time).[137]

Consent does not have a set validity period under the GDPR, and will theoretically remain valid so long as the underlying processing operations which it covers do not suffer any material changes. If changes to any of the essential information elements listed above occur, it may be necessary to renew the request for consent. As a best practice, it has been recommended that consent requests be regularly refreshed with data subjects, by providing those individuals with all relevant information once more and asking them to confirm that they continue to consent to the processing of their data.[138] However, if those data subjects do not renew their consent (either because they expressly withdraw it, or simply do not reply), then the controller must stop processing their data. While this may be an effective way to ensure that consent obtained from data subjects remains relevant over time, it also represents a business risk which many controllers may not be comfortable with.

Consent is also subject to specificities when requested from children in connection with information society services offered directly to them. Controllers must ensure that if consent is provided directly by a child, the child is of legal age to provide consent. Each Member State is able to define their local legal age, insofar as it is not set any lower than 13 – Art. 8(1) GDPR. If a child is not of legal age, then consent must be provided by the child's parents, or other holders of parental responsibility, under Art. 8(2) GDPR. Controllers are responsible for establishing appropriate verification measures to confirm this in accordance with the level of risk inherent to the processing activities in question.[139] Possible solutions include e-mail verification and requiring parents to make a minimal payment via bank transaction,[140] but also verification codes sent to mobile phone numbers via SMS, trusted third-party verification systems, toll-free phone or video calls to confirm the presence of an adult, and others.

[137] ibid 20-21.
[138] ibid 21.
[139] ibid 27.
[140] ibid 26 and n 66.

b. Performance of a contract with the data subject, or taking steps prior to entering into a contract at the request of the data subject

As stated by the European Data Protection Board, "*[i]f the specific processing is part and parcel of delivery of the requested service, it is in the interests of both parties to process that data, as otherwise the service could not be provided and the contract could not be performed*".[141] To rely on Art. 6(1)(b) GDPR as a legal basis, it is vital that the covered purpose is strictly necessary to provide a service or to perform a contract with an individual. If the contract can be performed without the specific processing taking place, then the controller should consider another legal basis.[142]

Art. 6(1)(b) GDPR will not cover processing which is useful, but not objectively necessary, for the performance of a contract or to take relevant pre-contractual steps at the data subject's request (even if it may be necessary for other business purposes of the controller).[143] The European Data Protection Board has produced a list of questions which may be posed by a controller wishing to assess whether or not a given processing activity falls under the requirements for applicability of this legal basis:[144]

- What is the nature of the service being provided to the data subject?
- What are its distinguishing characteristics?
- What is the exact rationale of the contract (i.e., its substance and fundamental object)?
- What are the essential elements of the contract?
- What are the mutual perspectives and expectations of the parties to the contract?
- How is the service promoted or advertised to the data subject?
- Would an ordinary user of the service reasonably expect that, considering the nature of the service, the envisaged processing will take place in order to perform the contract to which they are a party?

The key is for the controller to determine whether or not the service can be provided and the contract can be performed without the processing activity

---

[141] European Data Protection Board, 'Guidelines 2/2019 on the processing of personal data under Art. 6(1)(*b*) GDPR in the context of the provision of online services to data subjects' (9 April 2019) 3 <https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-22019-processing-personal-data-under-article-61b_it> accessed 23 January 2020.

[142] ibid 6.

[143] ibid 7.

[144] ibid 9.

taking place. For example, it is generally not necessary for an online retailer to send marketing communications to its customers in order to be able to provide its retailing services; in this case, an alternative legal basis must be used in order to do so (such as consent, or – where applicable –its own legitimate interests). Likewise, the performance of customer satisfaction surveys, or the use of data related to activities or preferences of service users in order to improve services, may be subject to the same conclusions. However, the European Data Protection Board has conceded that use of personal data for personalisation of content, in an online services context, may potentially be considered as "necessary" in this context, depending on (1) the nature of the service, (2) the expectations of the average user/data subject, and (3) whether the service can be provided without personalisation.[145] Naturally, data subjects may also expressly request that this personalisation be carried out, in which case it may reasonably be argued that Art. 6(1)(b) GDPR applies directly.

Controllers should bear in mind that this legal basis applies only to contracts entered into with data subjects, i.e., individuals. Art. 6(1)(b) is often wrongly invoked as a legal basis for the processing of details on contact persons in order to allow for the performance of a contract between two companies. In this case, because the data subjects in question are not a party to the contract, the controller must instead consider leveraging its own legitimate interests as a legal basis.

This legal basis applies also to situations where a contract has not yet been formed with a data subject, but it is necessary to process personal data concerning that individual in order to allow the controller to take relevant pre-contractual measures. For example, a controller would be able to process the postal code of a data subject under this legal basis if necessary to confirm whether the controller is able to provide services in the area of the data subject.[146] In general, the use of personal data to respond to queries submitted by potential customers may fall under the scope of Art. 6(1)(b) GDPR. However, if the controller is required to collect personal data on a data subject prior to entering into an agreement as a result of the applicable law (eg, due to know-your-client or related obligations), it is more reasonable to maintain that the appropriate legal basis is Art. 6(1)(c) GDPR,[147] the need for processing to comply with a legal obligation.

---

[145] ibid 13-14.
[146] ibid 12.
[147] ibid 12 (Example 5).

c. Compliance with a legal obligation

Controllers may also process personal data where this is strictly necessary to comply with the applicable law, under Art. 6(1)(c) GDPR. This is limited to compliance with legal obligations resulting from European or Member State law, as set out in Art. 6(3) GDPR. Use of personal data for compliance with extra-EU legal obligations must therefore be based on an alternative legal basis, such as, eg, the controller's own legitimate interests.[148]

In order for this legal basis to apply, the law must impose a mandatory obligation upon the controller which can only be carried out via the processing of personal data. It must also be sufficiently clear as to the processing which is required, referring specifically to its nature and object, so that the controller is not afforded an excessive degree of discretion on how to comply with the obligation.[149] In short, if it is possible to comply with a given obligation without processing personal data, or by processing fewer or different categories of personal data than those foreseen by the controller, then Art. 6(1)(c) GDPR cannot be relied upon. Examples include where employers are subjected to obligations to report information on their employees to competent public authorities (eg, tax and social security authorities), where financial institutions are obliged to report suspicious transactions, or where local authorities collect data for the purpose of applying fines or penalties in the case of infractions,[150] as well as retention obligations, under which controllers may be required to maintain copies of personal data (or, rather, of documents containing personal data) for certain pre-determined periods of time, as is the case with invoices and other financial documents in many jurisdictions.

d. Protection of vital interests of individuals

Art. 6(1)(d) GDPR is a very specific legal basis (eg, widely applied in the healthcare, human assistance and support sectors) as the conditions for its applicability are very strict: in essence, it will only apply in cases where the life of an individual is at stake or, at least, where there is a risk of injury or other damage to the health of an individual if the processing is not carried out.[151] The Article 29 Working Party, in the context of the Data Protection Directive, limited the applicability of this legal basis further, by stating that

[148] Art. 29 Working Party Opinion 06/2014, 19.
[149] ibid 19.
[150] ibid 19.
[151] ibid 20.

it should only be relied on, in practice, where it is not feasible to seek the individual's consent.[152]

Art. 6(1)(d) GDPR may be particularly relevant for the provision of emergency medical care (where the individual is incapable of providing consent), or where processing personal data related to a parent is needed to protect the vital interests of a child. It may also potentially be applied to larger-scale processing activities, such as those inherent to the monitoring of epidemics or the provision of humanitarian aid as a result of a natural or man-made disaster.[153]

While the GDPR does not distinguish between the legal bases of Art. 6 in terms of their validity, nor does it create any sort of hierarchy or subsidiary relationship between them, Recital 46 GDPR clearly states that "*[p]rocessing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis*". Therefore, when processing the personal data of a data subject in order to protect vital interests of another person, the controller should carefully consider whether any other legal basis may be applicable (in particular, the consent of the data subject) before deciding to rely on Art. 6(1)(d) GDPR.

e. Performance of a task in the public interest, or exercise of official authority vested in the controller

Controllers may only rely on Art. 6(1)(e) GDPR where the processing of personal data is necessary to perform a task in the public interest of the European Union or a Member State, or where the official authority vested in the controller has been granted by the European Union or a Member State. An alternative legal basis must be sought out if the public interest or the official authority granted in question is extra-European.[154]

This legal basis applies where the controller is legally charged with tasks established in a relevant public interest, or has been granted official authority, and the processing of personal data is strictly necessary in order to accomplish those tasks or to exercise that authority. Examples include the processing of individuals' tax returns by the competent tax authorities, professional associations carrying out disciplinary actions against their members and

---

[152] ibid 20.

[153] UK Information Commissioner's Office, 'Vital interests' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/> accessed 23 January 2020.

[154] Art. 29 Working Party Opinion 06/2014, 21.

local government bodies processing data in order to run local services, such as libraries or municipal swimming pools.[155]

Secondly, this legal basis may also cover situations where a controller discloses personal data to a competent public authority, such as law enforcement authorities, upon request (such as in the case where the controller is requested to cooperate in ongoing criminal investigations) or proactively (for example, where the controller reports information on a detected criminal offence on its own initiative, even where no legal obligation to do so exists).[156] It is important, however, for controllers to consider all relevant data protection principles when disclosing personal data to law enforcement authorities. This means, in particular, understanding to what extent authorities are legally allowed to request certain categories of personal data from controllers, under the applicable law, and whether or not the controller is required or prevented from informing affected data subjects of disclosures performed.

Other examples include processing activities carried out in the context of governmental tasks which are outsourced to the private sector, such as tasks related to transportation or public healthcare (including epidemiological studies and research).[157] The European Data Protection Board has stated, for example, that "*[t]he processing of personal data in the context of clinical trials can thus be considered as necessary for the performance of a task carried out in the public interest when the conduct of clinical trials directly falls within the mandate, missions and tasks vested in a public or private body by national law*".[158]

f. Legitimate interests pursued by the controller or a third party

Art. 6(1)(f) GDPR can be regarded as a 'double-edged sword'. While it is the most flexible out of the six legal bases available to controllers, it is mandatory for controllers to perform a specific assessment, referred to as a 'balancing test' or a 'legitimate interests assessment', in order to determine whether the interests they wish to pursue with a given processing activity are not overridden by the interests or fundamental rights and freedoms of the data

---

[155] ibid 21.
[156] ibid 21.
[157] ibid 22.
[158] European Data Protection Board, 'Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR) (art. 70.1.b))' (23 January 2019) <https://edpb.europa.eu/our-work-tools/our-documents/stellungnahme-artikel-70/opinion-32019-concerning-questions-and-answers_en> accessed 23 January 2020 (EDPB, Opinion 3/2019) 7.

subjects concerned.[159] To put this in more practical terms, controllers seeking to leverage their own legitimate interests are responsible for making sure that they are pursuing interests which are lawful, in a manner which does not excessively intrude upon the privacy and other rights of individuals. To accomplish this, controllers must carry out and document an assessment in which they balance their interests against those individuals' rights. The Article 29 Working Party, in the context of the Data Protection Directive, provided extensive guidance on the performance of this assessment, listing several factors which must be considered by controllers in this process.[160]

As a first step, controllers should describe the intended activity, identifying relevant persons in charge of the activity and the systems used in connection with the activity. It should be clarified whether the intended activity will require the processing of personal data and, if so, the specific categories of personal data should be identified.

Controllers should then establish whether Art. 6(1)(f) is the most appropriate legal basis for the activity in question. This will not be the case, for example, where the activity is required in order to comply with an EU legal obligation or perform a contract with a data subject. Moreover, controllers should then describe the interest being pursued. As noted by the Article 29 Working Party, "*[t]he concept of 'interest' is closely related to, but distinct from, the concept of 'purpose'*";[161] whereas a 'purpose' is the specific reason for which personal data are processed, an 'interest' is the broader stake that the controller may have in the processing activity, or the benefit which may be derived from this activity (eg, in order to pursue the *interest* of ensuring the health and safety of its staff, an employer may have as a *purpose* the implementation of specific access control procedures which require the processing of personal data on employees).[162] It should be established whether this interest is lawful, in that it does not amount to the pursuit of illegal values or goals, and whether it is a real and present interest of the controller (as opposed to overly vague or speculative interests).[163]

It is then necessary to assess the specific purposes for which personal data will be processed. This purpose must be described, and it must be determined

---

[159] To a certain extent, the factors analysed in the carrying out of this assessment overlap with those listed in GDPR, art 6(4), regarding the assessment of compatibility between an initial purpose for which collected personal data are processed and an additional, subsequent purpose for which the controller may intend to process those data.

[160] Art. 29 Working Party Opinion 06/2014, 30-44.

[161] ibid 24.

[162] ibid 24.

[163] ibid 24.

whether the intended processing activity is strictly necessary in order to meet the purpose. In essence, this requires controllers to make an impartial and comprehensive assessment as to whether there is any less-intrusive manner in which the controller would be able to reach its goals. A specific example which can be given is the use of biometric scanners in order to control employees' access to restricted areas in the workplace. The controller must be able to justify that the use of these scanners is the only truly effective means of achieving the intended security purposes, as opposed to other less invasive means, such as allowing employees to use access cards or PIN codes/passwords in order to access those areas.[164]

The controller's pursued interest must then be assessed more in-depth: it is important to explain whether it corresponds to the exercise of a fundamental right of the controller or a third party, under EU law (such as the right to conduct a business), whether it lines up with the public interest or wider interests of the community in which the controller is inserted, and whether it is legally, socially and/or culturally recognised as legitimate. The impact upon the controller or the third party if the activity is not carried out is also relevant for this purpose.

Next, the impact on the data subjects affected by the processing must be considered. Accordingly, it has to be understood whether any sensitive data[165] are handled in connection with the activity, whether the data subjects concerned are in a position of vulnerability towards the controller and whether the controller is in a dominant position regarding those data subjects. Certain characteristics of the foreseen processing activity may be found relevant, including where the activity involves the disclosure of personal data to the public, the collection of a large amount of personal data (eg, data mining), the matching or combination of datasets or the profiling of data subjects. Key questions to be asked during this stage include whether data subjects, as a result of their relationship with the controller or any other applicable circumstances, will reasonably expect the processing to take place, and what will be the rights, freedoms, and interests of those data

---

[164] Commission Nationale de l'Informatique et des Libertés, '*Délibération n° 2019-001 du 10 janvier 2019 portantrèglement type relatif à la mise en oeuvre de dispositifsayant pour finalité le contrôled'accès par authentificationbiométrique aux locaux, aux appareils et aux applications informatiquessur les lieux de travail*' art 3 <https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-daces-biometrique.pdf> accessed 23 January 2020 (in French).

[165] The concept of 'sensitive data' used here is broader than 'special categories of personal data', as established in GDPR, art 9. It includes those data, as well as personal data on criminal convictions and offences (GDPR, art 10), communications data (such as traffic and billing data), location data, financial data, and, in general, any information on individuals that may require special protection, such as children.

subjects potentially affected by the processing (which requires controllers to analyse the various ways, both positive and negative, in which data subjects may be affected by the processing of their data[166]).

At the end of this exercise, the controller should arrive at a provisional conclusion. There may be clear-cut cases, where the interests of the controller manifestly outweigh the impact upon data subjects, or where data subjects are clearly impacted in a manner which is excessive and disproportionate towards the aims sought by the controller (particularly where there may exist less intrusive alternatives to meet the same goal). However, it is more likely that the controller will arrive at a point where it is possible to interpret the balance as tendentially, but not clearly or manifestly, favouring the interests of either the controller or the data subjects. In this case, it is important for the controller to lay down additional safeguards for the intended processing activity, which aim to resolve the conflict in favour of the controller by further ensuring that the rights, freedoms of interests of data subjects are adequately protected. These may include measures to ensure that personal data cannot be used to take decisions or other actions with respect to individuals, anonymisation techniques, data aggregation, privacy-enhancing technologies, increasing transparency on the activity towards data subjects and providing a general and unconditional right to opt-out, among many others which controllers may consider.[167]

In any case, it is important that the controller considers that the safeguards put in place sufficiently address the risks which may have been detected to the rights of the data subjects concerned, so that the controller may convincingly state (and demonstrate) that the interests it wishes to pursue are not overridden by those rights. Only where this is possible will it be feasible for a controller to rely on its own legitimate interests (or those of a third party) as a valid legal basis under the GDPR.

ii. Special categories of personal data and personal data relating to criminal convictions and offences

When it comes to processing special categories of personal data,[168] or personal data which relates to criminal convictions and offences, it is not enough for a controller to identify an appropriate legal basis under Art. 6

[166] Art. 29 Working Party Opinion 06/2014, 37.
[167] ibid 42 onwards.
[168] GDPR, art 9(1): "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*".

GDPR, as described above. Art. 9(1) GDPR establishes a general prohibition on the processing of special categories of personal data. However, this prohibition may be lifted in the event that one of the derogations listed in Art. 9(2) applies. Some of these are broad in scope, while others are crafted in a very specific manner, such that they apply only where a restricted set of circumstances are met. Some derogations create additional restrictions for controllers, depending on the legal basis which they have chosen to rely on under Art. 6 GDPR:

- Explicit consent has been obtained from the data subject (Art. 9(2)(a) GDPR). Explicit consent must not only meet the requirements for consent explained above, but must also be given by way of an express statement of consent on the part of the data subject. This may be achieved by having the data subject expressly confirm consent in a written statement, but also by filling in an electronic form, sending an e-mail, uploading a signed scanned document or using an electronic signature, as well as via an oral statement (though this may raise issues for the controller in terms of proving that all conditions needed for consent to be valid were met at the moment when the statement was made).[169]

- The processing is necessary to carry out obligations and exercise specific rights, of the controller or the data subjects, in the field of employment, social security, and social protection law (Art. 9(2)(b) GDPR). This is, in part, a further specification of the legal basis of Art. 6(1)(c) GDPR, which restricts the relevant legal obligations to those related to employment, social security and social protection. Naturally, these obligations must also be based on EU or Member State law. However, the reference to "specific rights" of the controller may also justify the processing of personal data in cases where the controller may have relied on its legitimate interests as a legal basis, insofar as those interests correspond to a right afforded to the controller under employment, social security or social protection law. For example, this derogation may potentially be relied on to justify the use of biometric data for the purpose of identifying employees and controlling their access to restricted areas or for monitoring their attendance.[170]

- The processing is necessary to protect the vital interests of an individual, where the data subject is incapable of providing consent (Art.

[169] Art. 29 Working Party Consent Guidelines 18.
[170] CNIL (n 164) Art. 5.

9(2)(c) GDPR). All of the considerations made above regarding Art. 6(1)(d) GDPR are applicable here, with the added caveat that if it is feasible for the data subject to consent to the intended processing, this derogation becomes inapplicable (regardless of whether the vital interests to be protected are of the data subject or a third person).

- The processing is necessary for a substantial public interest, on the basis of EU or Member State law (Art. 9(2)(g)). This acts as a further requirement upon controllers which leverage Art. 6(1)(e) GDPR as a legal basis, given that the tasks which they may seek to accomplish must be carried out on the basis of a public interest which is substantial (although little guidance exists to clarify the scope of this qualification).
- The processing is necessary for reasons of public interest in the area of public health (Art. 9(2)(i) GDPR). This includes processing carried out to protect against serious cross-border threats to health, and also to ensure high standards of quality and safety for healthcare/medicinal products and devices. Clinical trials may also potentially be justified under this derogation, depending on their specific circumstances, as noted by the European Data Protection Board.[171]

Other derogations refer to the circumstances of the processing operation and the parties involved:

- The processing is carried out by a foundation, association or non-profit body with a political, philosophical, religious, or trade union aim, insofar as this processing is carried out in the course of its legitimate activities, with appropriate safeguards, relates solely to its members, former members or persons in close contact with the body and the personal data are not disclosed outside of the body without consent (Art. 9(2)(d) GDPR).
- The personal data which are to be processed have been manifestly made public by the data subject (Art. 9(2)(e) GDPR), such as where the data may have been uploaded by the data subject onto a public page on the Internet.
- The processing is necessary in order for the controller to establish, exercise, or defend against legal claims (Art. 9(2)(f) GDPR). Courts may rely on this derogation to process special categories of personal data whenever they act in their judicial capacity.

[171] EDPB, Opinion 3/2019 (n 158) 7.

- The processing is necessary for purposes related to preventive or occupational medicine, for the assessment of the working capacity of the employee (including workplace health and safety assessments of employees), for the performance of medical diagnoses or the provision or management of healthcare/social care services, including where necessary to manage systems through which those services are provided (Art. 9(2)(h) GDPR). Hospitals, clinics and healthcare practitioners will seek to leverage this derogation in order to justify their handling of health and data related to patients. In fact, under Art. 9(3) GDPR, this derogation can only be leveraged where the processing is carried out by, or under the responsibility of, a professional subject to a valid obligation of secrecy (such as a doctor, given the rules on confidentiality applicable to doctors in most jurisdictions).
- The processing is necessary for archiving purposes (in the public interest), research purposes (whether scientific or historical) or statistical purposes, insofar as appropriate safeguards are put in place (Art. 9(2)(j) GDPR).

In turn, personal data related to criminal convictions and offences may be processed by controllers only (1) under the control of official authority (which may be the case for, eg, competent entities in the public sector), or (2) when this processing is authorised under EU or Member State law. This may create limitations, for example, on the possibility to collect copies of criminal records from job applicants, which will only be admissible where there is a specific permission for this under the law applicable to the controller (meaning that there does not necessarily need to be a legal obligation to do so).

In our opinion, Art. 9 and Art. 10 GDPR do not create specific legal bases, outside of those listed in Art. 6 GDPR, for the processing of special categories of personal data, or personal data related to criminal convictions and offences, respectively. They create additional requirements upon controllers wishing to process these more sensitive types of personal data. Not only must the controller identify an appropriate legal basis under Art. 6 GDPR, but it must also identify an applicable derogation under Art. 9 GDPR, or an authorising law under Art. 10 GDPR. This means that, in particular, it is possible, under the GDPR, to process special categories of personal data on the basis of the controller's legitimate interests, provided that a derogation under Art. 9 GDPR applies.[172]

---

[172] *See*, for example, EDPB, Opinion 3/2019 (n 158) 5: "*Depending onthe whole circumstances of the trial and the concrete data processing activity, research related activities*

F. Step 6: Data Subject Rights

The GDPR offers data subjects a wide variety of rights which they can exercise towards controllers. Controllers are required to provide data subjects with relevant information as to the existence of those rights, and how they can be exercised (Arts. 13(2)(b) and 14(2)(c) GDPR, tied into the principle of transparency, addressed also in Step 4 above). Controllers must also develop a consistent and effective approach to receiving, tracking and addressing in full any requests received from data subjects to exercise any of the rights described below. The approach which a controller chooses to implement regarding the response to data subject rights must consider several factors in order to correctly manage those responses under the GDPR, regardless of the type of request which is made:

- The controller may identify specific channels through which data subjects may submit requests (eg, a dedicated e-mail address, an online form which may be filled out, paper-based forms), considering that these channels should be appropriate to the context and nature of the relationship and interactions between the controller and data subjects.[173] However, controllers must respond to all requests received from data subjects, even if made by other channels.[174] The rule is that a response must be given within one month of receipt of the request, although this period can be extended by an additional two months for more complex requests (provided that this is justified to the requester within the first month) – Art. 12(3) GDPR.

---

may either fall under the data subject's explicit consent [Article 6(1)(a) in conjunction with Art. 9(2)(a)], or a task carried out in the public interest [Article 6(1)(e)], or the legitimate interests of the controller [Article 6(1)(f)] in conjunction with Art. 9(2)(i) or (j) of the GDPR." This was suggested also by the Art. 29 Working Party Opinion 06/2014, referring to arts 7 and 8 of the Data Protection Directive (which substantially equate to GDPR, arts 6 and 9 respectively), p. 15: "*the Working Party considers that an analysis has to be made on a case-by-case basis whether Article 8 in itself provides for stricter and sufficient conditions, or whether a cumulative application of both Article 8 and 7 is required to ensure full protection of data subjects. In no case shall the result of the examination lead to a lower protection for special categories of data*".

[173] Art. 29 Working Party Transparency Guidelines, 27.

[174] UK Information Commissioner's Office, 'Right of access'<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/> accessed 23 January 2020: "*(…) you should note that a subject access request is valid if it is submitted by any means, so you will still need to comply with any requests you receive in a letter, a standard email or verbally*". Given that the GDPR does not prescribe specific means by which data subjects must submit any requests to controllers, it should be understood that this applies also to the other rights of data subjects under the GDPR.

- Upon receiving a request, the controller must first take steps to reasonably identify and authenticate the requester, depending on the scope of the request and the level of risk involved. For example, if a controller receives an e-mail request asking for removal from a mailing list, it may be sufficient to check the requester's name and e-mail address against the mailing list itself. However, if the request asks the controller to provide a copy of personal data processed on an individual, the controller should take additional steps to reasonably authenticate the individual making the request, so that personal data are not unduly disclosed to an unauthorised third party (for instance, by asking for a copy of a valid identification document from the requester, which will be used only to confirm the requester's identity) – Art. 12(6) GDPR.
- Having confirmed the identity of the requester, the controller should also confirm whether the requester is a data subject relative to the controller – meaning, the controller should confirm whether or not any personal data related to the requester is handled by the controller. If not, the controller will be unable to address the request made, and should notify the requester of this. On the other hand, if it is confirmed that personal data related to the requester is processed by the controller, then it will be important to identify the type of request made, in order to properly respond.
- Any responses given should be intelligible, concise, and written in clear and plain language, so that the requester is able to understand them. As a rule, responses should be provided in writing (even if in electronic format, such as by e-mail), though controllers may also respond orally if this is expressly requested by the data subject – Art. 12(1) GDPR.
- The controller must keep track of all requests received and responses given to those requests, so that it can demonstrate its compliance with the GDPR rules in this regard, as required by the principle of accountability. This can be done by keeping a register of data subject requests, listing the dates on which a request was received and resolved, the identity of the requester and scope of the request, and by storing evidence of the actual communications exchanged with requesters.
- All requests should, as a rule, be handled free of charge to the requester. Only in exceptional cases, such as where a request is considered manifestly unfounded or excessive (particularly where the requester has made a similar or same request multiple times, or where the scope of a request is excessively broad), may the controller refuse

to act on that request or charge a reasonable administrative fee in order to respond – Art. 12(5) GDPR. Given that the burden of proof as to the unfounded or excessive nature of the request lays upon the controller, it is strongly recommended that controllers ensure that a request can objectively be considered unreasonable before deciding on whether to charge a fee or refuse to comply (as, naturally, supervisory authorities may disagree with controllers' assessment on this).

It may also occur that a processor receives a request for the exercise of data subject rights. Processors are not under any obligation under the GDPR to address such requests directly, and should therefore handle them in the manner agreed with the controller, within the data processing agreement signed with that controller. A standard approach is for processors to relay requests received to the appropriate controller within a given period of time and remain cooperative as appropriate to enable the controller to effectively guarantee the exercise of data subjects' rights; or otherwise to simply advise requesters to submit their request to the appropriate controller.

i. Right of access

The right of access can be divided into three different components:

- The right to obtain confirmation from a controller as to whether or not personal data concerning a data subject are being processed;
- The right to access those personal data and receive a copy of those personal data; and
- The right to receive information about the processing of personal data undertaken.

Whether or not the controller must address all three of these components depends on the scope of the request received. If a data subject merely asks for confirmation that his/her personal data are being processed by controller, this does not necessarily require the controller to provide to the data subject a copy of the data which are being processed.

The first component is relatively simple. After having verified the identity of the requester, the controller must confirm whether or not the requester is a data subject related to the controller (i.e., whether the controller currently processes any personal data related to him/her), as noted above. The controller should inform the requester of the result of this confirmation. If the controller does not process any personal data related to the requester, it will not be possible to address any other aspect of the request.

The second component requires allowing the data subject to access the personal data relating to him/her which is processed by the controller, and to receive a copy of those data if requested. The GDPR does not create any limitation as to categories of personal data which may be covered by an access request. In principle, if a data subject submits a request to exercise the right of access, without specifying the categories of personal data he/she wishes to access, the controller must provide access to all personal data held on the data subject. However, it is also possible for the controller, faced with a broad request for access and an extensive and complex dataset pertaining to that data subject, to ask the data subject to clarify their request –for example, by presenting the data subject with a list of types of personal data, or documents containing personal data, which may be held on him/her, and asking the data subject to narrow down their access request to some of those types.[175]

The right of access, along with the remaining data subject rights, "*are designed to meaningfully position data subjects so that they can vindicate their rights and hold data controllers accountable for the processing of their personal data*".[176] The right of access is not an instrument to be used by data subjects to gain access to any and all documents, correspondence or data held by a controller. As such, Art. 15(4) GDPR establishes a restriction to the right of access: "*The right to obtain a copy (…) shall not adversely affect the rights and freedoms of others*". These 'rights and freedoms of others' include those of the controller and third parties, thereby allowing controllers to refrain from providing certain documents, or parts of certain documents, which contain information covered by trade secrets (including lists of customers, know-how, financial records, etc.) or intellectual property rights. The rights and freedoms of other individuals must also be protected by the controller. As a rule, the controller should redact any information related to other persons contained in documents or data provided to the requester. However, it is also possible for the controller to seek consent from those other persons in order to be able to disclose their information to the requester.[177]

The third component requires the controller to provide specific information to the data subject on the terms under which his/her data are processed. This includes, under Art. 15 GDPR:

- The purposes for which the data are processed;

---

[175] ibid.

[176] Art. 29 Working Party Transparency Guidelines, 26.

[177] ibid 'What should we do if the data includes information about other people?'. Note that this section refers to the UK Data Protection Act 2018 which regulates the matter of providing documents containing other persons' data more specifically than the GDPR.

- The categories of personal data processed;
- The intended or actual recipients of those personal data (or categories of recipients);
- The retention periods applied to those personal data;
- The existence of data subject rights under the GDPR;
- The right to lodge a complaint with supervisory authorities;
- The source of the personal data (where they were not collected directly from the data subject); and
- Information on the existence of automated decision-making, under Art. 22 GDPR, including meaningful information about the logic involved, the significance and the foreseen consequences of such processing for the data subject.

These are all information requirements which should have already been met by the controller within one or more information notices or privacy policies made accessible to the data subject (see Step 4 above). Therefore, it may be possible for controllers to address a request for such information, if only in part, by referring to the applicable privacy policy or information notice made previously available to the data subject. Controllers are not required to provide all of this information to data subjects upfront when faced with an access request, unless data subjects specifically require this from the controller.

It is quite common that requests to exercise the right of access are drafted broadly by data subjects. Without a structured system in place to allow a controller to effectively track down and provide access to all personal data held on a given data subject, responding can become a lengthy, arduous, and uncertain task for the controller. While the recommendation to ensure that the controller has mapped out all databases and files containing personal data goes without saying, it is also strongly recommended to tackle broad access requests as early as possible. This can be done, for example, by replying to the data subject to ask him/her to narrow down his/her request (providing a list of categories of data or documents which the data subject may wish to access). Doing so helps to ensure that the controller is able to respond within the general one-month deadline set by the GDPR, rather than having to resort to an extension of the deadline. It is important to note that, under the principle of accountability, it will be upon the controller to justify that the complexity and/or number of requests received from a data subject justifies a larger response time, and supervisory authorities are not

likely to favour delayed reactions or a lack of structure on the controller's part as a valid excuse.

Unlike the right to data portability, the GDPR does not create requirements as to the format in which a copy of personal data should be provided to the data subject under the right of access. Controllers may consider, for example, relying on file-sharing platforms which may allow data subjects to directly access all files gathered by the controller on them, sending physical print-outs of the relevant information to data subjects, or providing the documentation via e-mail. It is important that the personal data is provided to the data subject in a secure manner, allowing the data subject to read and understand it.

ii. Right to rectification

As a reflection of the principle of accuracy, which requires controllers to ensure that the personal data they process is accurate and kept up-to-date, the GDPR grants to data subjects the right to rectification – the right to demand that controllers correct or complete any personal data they hold on a data subject which may be inaccurate or incomplete, under Art. 16 GDPR.

When submitting a request for rectification, a data subject will typically indicate the information which he/she wishes to have corrected or completed, and may provide evidence or arguments which justify this. The controller does not have to take the data subject's claims at face value, and should carry out its own assessment as to whether the personal data in question is incorrect, misleading or incomplete. If the data subject requests this, the controller should restrict the processing of the personal data in question while this assessment is being carried out, under Art. 18(1)(a) GDPR (which will result in those data being segregated and not used for other purposes, as will be seen further below). As a matter of best practice, the controller should restrict the challenged data even in the absence of an express request from the data subject for this restriction.[178] If the controller disagrees with the data subject, the controller may refuse to comply with the request, by explaining its reasoning to the data subject and informing the data subject of their right to lodge a complaint with the competent supervisory authority (Art. 12(4) GDPR).[179]

---

[178] UK Information Commissioner's Office, 'Right to rectification' 'What should we do while we are considering the accuracy?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/> accessed 23 January 2020.

[179] ibid: "*It is also good practice to place a note on your system indicating that the individual challenges the accuracy of the data and their reasons for doing so.*"

Not all personal data are equal under the lens of the right to rectification. As noted by the European Data Protection Supervisor,[180] "*[t]he right to rectification only applies to objective and factual data, not to subjective statements (which, by definition, cannot be factually wrong). (…) However, data subjects are permitted to complement existing data with a second opinion or counter expertise in such situations, e.g. as regards decisions made during an appeal procedure in disciplinary cases, or comments on an annual performance appraisal*".[181] Therefore, while 'hard data', such as a name, e-mail address, or date of birth, may be considered incorrect and subject to a need for rectification, 'soft data', such as an individual opinion issued in a performance report for an employee, cannot. However, the right to rectification may entitle the employee to instead submit a statement with his/her own observations on the information contained in that report.

Under Art. 19 GDPR, if the controller considers that a request for rectification is valid, they are required to notify the correction and/or completion carried out to any other recipients of those personal data, so that they may likewise correct and/or complete the information in their possession. Controllers may, however, be exempt from this obligation to the extent that it is impossible, or requires disproportionate effort, to notify all potential recipients (eg, where the inaccurate or incomplete personal data may have been published online, allowing any number of entities to be qualified as a recipient).[182] If the data subject requests this, the controller must inform the data subject as to the identity of these recipients.

---

[180] As noted previously, the European Data Protection Supervisor is the supervisory authority responsible for the supervision of the personal data processing activities of EU institutions and bodies, rather than any other public or private entities within the EU. Given the similarities between the rules on personal data processing applicable to those EU institutions and bodies and the GDPR, however, it is still possible to draw relevant insights from the European Data Protection Supervisor's guidance.

[181] European Data Protection Supervisor, 'Guidelines on the Rights of Individuals with regard to the Processing of Personal Data' (25 February 2014) 18 <https://edps.europa.eu/sites/edp/files/publication/14-02-25_gl_ds_rights_en.pdf> accessed 23 January 2020.

[182] By analogy with GDPR, art 14(5)(*b*), which allows controllers to exempt themselves from the obligation to provide information to data subjects, where personal data was not collected directly from them, if this proves impossible, or would result in disproportionate effort on the part of controllers, we can densify the notion of 'impossibility' and 'disproportionate effort' used in GDPR, art 19. The Article 29 Working Party, in its Transparency Guidelines notes that "*[t]he situation where it 'proves impossible' under Article 14.5(b) to provide the information is an all or nothing situation because something either is impossible or it is not; there are no degrees of impossibility. Thus if a data controller seeks to rely on this exemption it must demonstrate the factors that actually prevent it from providing the information in question to data subjects. If, after a certain period of time, the factors that caused the "impossibility" no longer exist and it becomes possible to provide the information to data subjects then the data controller should immediately do so. In practice, there will be very few situations in which a data controller can demonstrate that it is actually impossible to provide the information to data subjects*" (p. 29), and "*Where a*

iii. Right to erasure

The right to erasure, or 'right to be forgotten', is set out in Art. 17 GDPR. It draws its roots from a famous decision handed down by the Court of Justice of the European Union in the 'Google Spain' case.[183] This decision, rendered under the framework of the Data Protection Directive, considered, among other controversies, whether the plaintiff, a Spanish national, could require Google to remove or alter search results. The plaintiff's objective was that, when his name would be searched using Google's search engine, certain pages containing personal data related to him would no longer appear. Those pages concerned attachment proceedings for the recovery of social security debts of the plaintiff which, at the time of the plaintiff's request, had been fully resolved for a number of years. Thus, as maintained by the plaintiff, those data had become irrelevant, and it should be within his rights as a data subject to request that they no longer be made easily accessible to the public at large via search engine results. The Court of Justice stated that "*if it is found (…) that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with Article 6(1)(c) to (e) of the directive because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased*".

While the right to erasure, or 'right to be forgotten', was not expressly laid out in the Data Protection Directive, it is expressly set forth in Art. 17 GDPR. However, contrary to common belief (considering the frequency with which inappropriate requests for erasure are submitted to controllers by data subjects), the right to erasure has a limited scope of application. There are several exceptions which may allow controllers to exempt themselves from fully complying with otherwise valid erasure requests. It is important to consider the scenarios under which a request for erasure is valid – data

---

data controller seeks to rely on the exception in Article 14.5(b) on the basis that provision of the information would involve a disproportionate effort, it should carry out a balancing exercise to assess the effort involved for the data controller to provide the information to the data subject against the impact and effects on the data subject if he or she was not provided with the information. This assessment should be documented by the data controller in accordance with its accountability obligations" (p. 31).

[183] Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos*, 2014 QB 1022, ECLI:EU:C:2014:317.

subjects are allowed to demand that a controller erase personal data relating to them if:

- Those data are no longer necessary in relation to the purposes for which they were collected or are processed by the controller (Art. 17(1)(a) GDPR);
- The personal data were processed on the basis of the data subject's consent, and the data subject withdrew the consent given. In this situation, the controller must delete or anonymise those personal data, unless another legal basis exists which may justify continued processing of the personal data in question (for example, the controller may have a legitimate interest in archiving some of the personal data for evidentiary purposes, in order to protect itself against legal claims which the data subject may bring against the controller related to the processing activity in question);
- The data subject files a valid objection to the processing of their personal data by the controller (more on the right to objection below);
- The personal data have been processed unlawfully;
- An applicable legal obligation upon the controller, rooted in EU or Member State law, requires the controller to erase those personal data; or
- The personal data were collected in the context of the provision of information society services to children, on the basis of consent provided by those children or adults with parental responsibilities over those children (Art. 8 GDPR).

In most of the above cases, under the principles of data minimisation and storage limitation, the controller should proactively delete personal data even in the absence of a specific request for erasure. This, in itself, highlights the limited scope of the right to erasure under the GDPR. Save for the last condition of applicability presented above, all other conditions refer to situations in which the controller is already required to erase or anonymise the personal data in question anyway, either due to application of the aforementioned principles or to comply with other legal obligations imposed upon it. The right to erasure, therefore, serves as a means for data subjects to enforce controllers' compliance with those principles and obligations, rather than creating additional circumstances under which personal data must be erased or anonymised by controllers (for the most part).Furthermore, even in the presence of one of the above conditions, the controller may be able to oppose

a request for erasure if one of the exceptions laid out in Art. 17(3) GDPR applies. In particular:

- Where the personal data must continue to be processed in order to allow the exercise of the rights of freedom of expression and information;
- Where the controller is required to continue processing the personal data in order to comply with its legal obligations, perform a task in the public interest, or exercise official authority vested in the controller (under EU or Member State law);
- Where the personal data are processed for reasons of public interest, in the area of public health;
- Where the personal data are processed for archiving purposes in public interest, scientific/historical research purposes, or statistical purposes, subject to appropriate safeguards; or
- Where the personal data must continue to be processed in order to allow the controller to establish, exercise, or defend against legal claims.

However, if a request for erasure is validly presented to a controller and none of the above exceptions apply, the controller must ensure that the personal data covered by the request are fully erased from its systems – including any backup systems. This may create practical difficulties for controllers, as it may not be possible to immediately erase data from backups, due to security protocols in place. While it is important to delete all relevant personal data as soon as practically feasible, controllers should ensure that, in the interim, any personal data covered by a valid request for erasure which are contained in backup systems are put 'beyond use' (restricted), so that they cannot be used for any purpose until they are overwritten or replaced, in accordance with the controller's backup schedule.[184]

Considering that 'personal data' is defined, under Art. 4(1) GDPR, as "*any information relating to an identified or identifiable natural person*", compliance with a valid request for erasure can be achieved not only by deleting the personal data in question, but also by anonymising them, so that they no longer relate to an identified or identifiable natural person. Controllers are advised, however, that the bar for anonymisation is set very high by the

[184] UK Information Commissioner's Office, 'Right to erasure' 'Do we have to erase personal data from backup systems?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/> accessed 23 January 2020.

Article 29 Working Party. It must be ensured that the possibility to identify the individuals to which the information pertains is fully and irreversibly excluded, in order for that information to be considered anonymised, rather than merely pseudonymised:[185] "*An effective anonymisation solution prevents all parties from singling out an individual in a dataset, from linking two records within a dataset (or between two separate datasets) and from inferring any information in such dataset. Generally speaking, therefore, removing directly identifying elements in itself is not enough to ensure that identification of the data subject is no longer possible. It will often be necessary to take additional measures to prevent identification, once again depending on the context and purposes of the processing for which the anonymised data are intended*".[186]

As noted above, under Art. 19 GDPR, regarding the right to rectification, controllers are required to communicate any erasure of personal data carried out in response to a valid erasure request to other recipients of those personal data, so that they may also comply with that request, if the conditions for its validity apply also to them (unless this proves impossible or would require a disproportionate effort).[187] In particular, if the data were made public by the controller, then the controller must take reasonable steps to inform other controllers processing those data that erasure of links to copies or replications of those data has been requested, considering the available technology and costs in its implementation, under Art. 17(2) GDPR. Likewise, if the data subject requests this, the controller must inform the data subject as to the identity of these recipients.

iv. Right to restriction of processing

The right to restriction of processing entitles data subjects to request that controllers place their personal data under restricted conditions of use. As set out in Art. 18(2) GDPR, personal data covered by a request for restriction of processing may continue to be stored by the controller. However, as a rule, restricted personal data cannot be used for any other purposes without the consent of the data subject. Exceptions exist, such as where it is necessary to process those data in order to (1) establish, exercise or defend against legal claims; (2) protect the rights of another natural or legal person; or (3) carry out tasks or activities of important public interest (of the EU or a Member

[185] *See*, s. IV.C.ii.: Technical and organisational security measures.

[186] Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' WP216 (10 April 2014), <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 23 January 2020 (Art. 29 Working Party Opinion 05/2014) 9.

[187] *See*, s. IV.C.ii.: Right to rectification.

State). In order for a data subject to validly request the restriction of processing of their personal data, one of the following circumstances must apply:

- The data subject has contested the accuracy of personal data processed by the controller, and the controller requires time to assess this (Art. 18(1)(a) GDPR) – in this situation, the data subject may request that the processing of those data be restricted until the controller has come to a conclusion;
- The processing of the personal data is unlawful (Art. 18(1)(b) GDPR) – if the data subject does not wish for those personal data to be erased, he/she may instead request that their processing be restricted;
- The controller no longer requires the personal data, in light of the purposes for their collection or processing (Art. 18(1)(c) GDPR) – the data subject may request that the controller continue to store those data under restricted conditions of use, provided that those data are required by the data subject for the establishment, exercise, or defence of legal claims;
- The data subject has objected to the processing of personal data, and the controller requires time to assess whether the objection must be considered valid (Art. 18(1)(d) GDPR) – the data subject may request that the processing of those personal data be restricted until a conclusion is arrived at by the controller.

Controllers should, as a matter of good practice, automatically restrict the processing of personal data which has had their accuracy contested by a data subject, for the period of time necessary to assess this. The same can be said of personal data which is covered by an objection presented by a data subject, with the necessary adjustments.[188] In terms of how to practically comply with a request for restriction, the UK Information Commissioner's Office has provided some guidance which may be of use: "*The GDPR suggests a number of different methods that could be used to restrict data, such as: [1] temporarily moving the data to another processing system; [2] making the data unavailable to users; or [3] temporarily removing published data from a website. (…) If you are using an automated filing system, you need to use technical measures to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. You*

[188] UK Information Commissioner's Office, 'Right to restrict processing' 'When does the right to restrict processing apply?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/> accessed 23 January 2020.

should also note on your system that the processing of this data has been restricted".[189]

By definition, a restriction on the processing of personal data is temporary. Where the controller intends to lift a restriction put in place (for example, because it has completed its assessment as to whether the personal data in question are inaccurate or not, following a challenge to their accuracy raised by the data subject), it must anticipate this to the data subject beforehand, under Art. 18(3) GDPR.

Just as noted above regarding the rights to rectification and erasure, controllers are required to communicate any restriction of the processing of personal data carried out to other recipients of those personal data, so that they may also comply with that request, if the conditions for its validity apply also to them (unless this proves impossible or would require a disproportionate effort).[190] Likewise, if the data subject requests this, the controller must inform the data subject as to the identity of these recipients.

v. Right to data portability

The right to data portability, under Art. 20 GDPR, is possibly the most novel of the data subject rights granted by the GDPR. In a nutshell, the right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine-readable format. It also includes the right to request that a controller transmit those data directly to another controller.[191] It is a complex right which raises many practical questions to be understood and addressed by controllers, in order to ensure appropriate responses to any portability requests made.

It is first important to understand exactly what types of personal data may be covered by a request for data portability. There are three criteria which must be applied by controllers to understand whether or not certain data will be covered by the request:

- First, the right to data portability applies only to personal data which have been processed on the basis of the data subject's consent, or on the need to perform a contract with the data subject. Personal data

[189] ibid 'How do we restrict processing?'.
[190] *See*, s. IV.F.ii.: Right to rectification.
[191] UK Information Commissioner's Office, 'Right to data portability' 'What is the right to data portability?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/> accessed 23 January 2020.

processed on other legal bases are therefore excluded from the scope of application of this right.[192]

- Second, the right to data portability applies only to personal data processed by automated means. Therefore, most paper files containing personal data are not covered by the scope of this right.[193]
- Third, the right to data portability applies only to personal data which the data subject has provided to the controller. This includes not only the personal data actively and knowingly provided by the data subject (such as personal data submitted by a data subject via a form), but also the personal data collected by the controller from the observation of the data subject's activities (eg, activity logs, history of website usage or search activities, location data, traffic data). This excludes personal data which are created by the controller, by inferring or deriving those data from the information received from the data subject (such as assessments or profiles created by the controller on the data subject).[194]

Having established this, controllers may be faced with situations in which documents or data covered by the scope of a data subject's right to data portability also contain personal data related to other persons. In this scenario, it is important for the controller to make an assessment as to whether transmitting those personal data to the requesting data subject, or to another controller, may create an adverse effect to the rights, freedoms, and interests of those other persons. It is generally understood that providing such personal data to an individual is typically acceptable, assuming that the individual provided those data to the controller in the first place.[195] This is as opposed to a situation where the new controller (to whom the data may be transmitted) might seek to use those personal data for other purposes, such as for its own marketing purposes. As such, it is understood that the processing of personal data related to other persons by a new controller, as a result of the exercise of the right to data portability, should be allowed only to the extent that those data are kept under the sole control of the individual who made the portability request, and are managed only for purely personal or household needs of the requester (eg, a directory within a webmail account

---

[192] Article 29 Working Party, 'Guidelines on the right to data portability' WP242 Rev.01 (5 April 2017) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233> accessed 23 January 2020 (Art. 29 Working Party Data Portability Guidelines) 8.

[193] ibid 9.

[194] ibid 9.

[195] UK ICO, 'Right to data portability' (n 191) 'What happens if the personal data includes information about others?'.

may contain personal data on other individuals with which the requester has exchanged communications – this, however, should not prevent the controller of the webmail service from transmitting the entire directory of incoming and outgoing e-mails to the data subject).[196]

Similar considerations as drawn regarding the right of access can be made here, concerning documents or data containing information which, if disclosed, could create an adverse effect to the rights, freedoms, and interests of the controller or third parties (where, eg, trade secrets, sensitive business information or information protected by intellectual property rights may be included in the data set). On this matter, the Article 29 Working Party has stated, on one hand, that "*[t]he right to data portability is not a right for an individual to misuse the information in a way that could be qualified as an unfair practice or that would constitute a violation of intellectual property rights*";[197] on the other, they have also stated that "*[a] potential business risk cannot, however, in and of itself serve as the basis for a refusal to answer the portability request and data controllers can transmit the personal data provided by data subjects in a form that does not release information covered by trade secrets or intellectual property rights*".[198] This suggests that controllers should consider whether it is feasible to redact or exclude certain sensitive parts of documents or data, before refusing to comply with a portability request outright.

It is also important to consider the right to data portability from a technical perspective. Art. 20(1) GDPR requires the personal data in question to be transmitted to the data subject in a structured, commonly used, and machine-readable format. Further, Recital 68 GDPR adds the requirement that such format be "*interoperable*". In essence:

- 'Structured' can be defined as a characteristic of the format which must allow for specific elements of the dataset to be extracted. Spreadsheets with data organised into rows and columns are an example of a structured dataset.[199]
- 'Commonly used' means that the format chosen must be widely-used and well-established.[200] While there is little concrete guidance on how to establish whether a specific format meets this criterion, it is certain

[196] Art. 29 Working Party Data Portability Guidelines, 11.
[197] ibid 12.
[198] ibid 12.
[199] UK ICO, 'Right to data portability' (n 191) 'What does 'structured' mean?'.
[200] UK ICO, 'Right to data portability' (n 191) 'What does 'commonly used' mean?'.

that this requires controllers to avoid any internal or proprietary formats which are not available to the public at large.[201]

- 'Machine-readable' is a requirement that the format be able to be automatically read and processed by a computer, so that specific elements of data can be readily identified, recognised, and extracted.[202] Recital 21 of Directive 2013/37/EU of the EU Parliament and of the Council, of 26 June 2013, provides further clarity: "*a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format*".
- 'Interoperable' means that the format should allow data to be exchanged between different systems and be understandable to both.[203] However, Recital 68 GDPR clearly states that the right to data portability "*should not create an obligation for the controllers to adopt or maintain processing operations which are technically compatible*". Therefore, while the aim of this right is to create an incentive for controllers to use interoperable systems, there is no requirement that controllers maintain systems which are technically compatible with each other.[204]

When deciding on a format, controllers should consider how the format chosen may impact or hinder the individual's right to re-use the data.[205] Note that Art. 20(1) GDPR grants data subjects the right to transmit these personal data to another controller, without hindrance from the controller to which the data were originally provided. Formats such as .XML, .JSON, .CSV,[206] and .RDF[207] have all been suggested by EU supervisory authorities

[201] Art. 29 Working Party Data Portability Guidelines, 17.
[202] UK ICO, 'Right to data portability' (n 191) 'What does 'machine-readable' mean?'.
[203] UK ICO, 'Right to data portability' (n 191) 'Should we use an 'interoperable' format?'.
[204] Art. 29 Working Party Data Portability Guidelines, 17.
[205] ibid 18.
[206] ibid 18. *See also*, UK ICO, 'Right to data portability' (n 191) 'What is CSV?'; 'What is XML?'; and 'What is JSON?'.
[207] UK ICO, 'Right to data portability' (n 191) 'Are these the only formats we can use?'

as possible choices. Controllers may also consider employing automated tools to allow data subjects to extract the relevant data themselves.[208]

One additional point of interest is Art. 20(2) GDPR: "*In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible*". Where this is requested, controllers will need to determine, on a case-by-case basis, whether it is possible to communicate the data directly to the intended new controller in a secure manner (if there are any relevant technical impediments to this, the controller must explain them to the data subject), under the same terms as if the controller had refused to act upon the request.[209]

Controllers who receive a dataset as a result of a portability request made to another controller will be fully responsible for ensuring their own compliance with the GDPR's requirements. This includes, in particular, responsibility for identifying an appropriate legal basis to process those data, and for assessing the data received to ensure they are not excessive or irrelevant in relation to the purposes for which they will be processed. Controllers should ensure that they do not use third-party personal data received from a data subject for purposes other than to allow that data subject to manage those data.[210]

vi. Right to object to processing

Art. 21 GDPR establishes the right to object. This right allows data subjects to seek to prevent a controller from continuing to process their personal data for a given purpose. Depending on the purpose to which it refers, the right to object may be an absolute or limited right.

Data subjects are afforded an absolute right to object to the processing of their personal data for direct marketing purposes, at any time and for any reason, under Art. 21(2) GDPR. This includes also any profiling activities which may be carried out regarding those data subjects, to the extent that they are related to direct marketing activities (eg, clustering of individuals with the aim to send them targeted advertisements). If an objection is received (such as, for example, when a data subject asks to be unsubscribed from a mailing list, either expressly or by clicking on the relevant unsubscribe link

---

[208] Art. 29 Working Party Data Portability Guidelines, 16.
[209] ibid 16.
[210] UK ICO, 'Right to data portability' (n 191) 'What Responsibilities Do We have When We Receive Personal Data Because of a Data Portability Request?'. *See also*, Art. 29 Working Party Data Portability Guidelines, 11-12.

which should be provided with each message sent to him/her), the controller must stop processing the objecting individual's personal data for those purposes, without need for any further assessment.

Under the principle of data minimisation, if there are no other lawful purposes for which the controller may process those personal data, then the data should be erased or anonymised. However, in practice, it may be important to keep a record of objections received to avoid the sending of direct marketing communications to an objecting individual in the future.[211] This is particularly relevant in the B2B marketing context, where controllers may generate leads by sourcing contact details for persons of interest within target companies indirectly (for example, from public online sources or 'data brokers'). Without a record of individuals who have objected, it is possible that an opted-out individual may be re-added to the controller's marketing mailing lists at a later date. One possible approach is to retain limited data about the objecting individual (e-mail address, phone number) and irreversibly hash those data, storing only the hashed value. When adding new sets of contact details to a mailing list, controllers can hash those new data and compare the hashes to those which are stored in their 'opt-out record'– if there is a match, the corresponding set of contact details should not be added to the mailing lists.

There is also a more general right to object under the GDPR, though it is not absolute. As laid down in Art. 21(1) GDPR, data subjects may only exercise this right in relation to processing activities which are carried out:

- On the basis of their need for the performance of a task in the public interest (Art. 6(1)(e) GDPR);
- On the basis of their need for the exercise of official authority (Art. 6(1)(e) GDPR); or
- On the basis of their need for the pursuit of legitimate interests of the controller or third parties (Art. 6(1)(f) GDPR).

Data subjects are required to justify their objection, on grounds which relate to their particular situation. For example, an individual may object to a given processing activity on the grounds that the processing is causing them substantial damage or distress, such as financial losses.[212] However, this will not trigger an immediate obligation for controllers to stop the related

[211] UK Information Commissioner's Office, 'Right to Object' 'Direct marketing' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/> accessed 23 January 2020.

[212] ibid 'Processing based upon public task or legitimate interests'.

processing activity. As noted in Art. 21(1) GDPR, controllers are allowed to continue processing if they are able to demonstrate "*compelling, legitimate grounds for the processing which override the interests, rights and freedoms of the data subject*", or if this is necessary for the controller to establish, exercise, or defend against legal claims.

Faced with such an objection, the principle of accountability suggests that controllers should carry out and document a balanced assessment, which confronts the interests pursued by the controller with the grounds raised in the data subject's objection. To demonstrate 'compelling' legitimate grounds to continue processing, the controller must present reasons for which it wishes to continue processing personal data which are reasonably and objectively more important than the interests which the data subject claims to be harmed by the processing. The controller must demonstrate this reasoning to the data subject, if and when the objection is refused, and to inquiring supervisory authorities. The controller will be held fully accountable for the decision made. Best practice dictates that the controller, whenever feasible, should restrict the processing of personal data covered by the objection while this assessment is being executed.

If an objection is ultimately deemed valid, then the controller must stop the processing activities covered by the objection. This does not necessarily require the controller to erase or anonymise those personal data, as there may be other lawful purposes for which they must continue to be processed by the controller (for example, the fact that a customer objects to the processing of his/her data by a service provider for service improvement purposes does not prevent that service provider from continuing to process those personal data where necessary to provide services to the customer).[213]

vii. Rights concerning automated individual decision-making

Art. 22 GDPR establishes certain rights for data subjects in relation to certain personal data processing activities which qualify as 'automated individual decision-making'. To qualify as such, the processing activity must involve the making of decisions pertaining to an individual via an automatic process, resulting from the collection and/or analysis of personal data (which may be provided directly by the data subject, collected from observation of the data subject's activities, or derived/inferred from information provided or observed), without a relevant level of human intervention

[213] ibid 'Do we always need to erase personal data to comply with an objection?'.

(without meaningful oversight of those decisions carried out by a human).[214] Furthermore, the decisions made must be susceptible to producing a legal effect, or a similarly significant effect, on the data subject. This will be the case where such decisions may significantly affect the circumstances, behaviour, or choices of the data subject, have a prolonged or permanent impact on the data subject, or lead to the data subject's exclusion or discrimination.[215] Examples which have been given include decisions resulting in cancellations of contracts, granting or refusing social benefits, granting or refusing admission to a country or citizenship, and also automatic refusals of credit applications and automatic selection/rejection procedures for candidates in a recruitment process, among others.[216]

The decision to target advertisements to an individual based on an automatically generated profile is generally offered as a counterexample (i.e., a case where Art. 22 GDPR is not triggered). However, the Article 29 Working Party has suggested that this may cease to be the case if, for instance, the profiling process is particularly intrusive (such as where individuals may be tracked across multiple websites, devices, and services) or subverts the expectations and wishes of the individuals concerned, or where the form of delivery of advertisements is inappropriate.[217]

Where the above criteria are met, there are additional requirements to be complied with by controllers in order to carry out these processing activities lawfully under the GDPR. It is first important to note that Art. 22(1) GDPR establishes a general prohibition to carry out automated individual decision-making, which is then limited by derogations laid down in Art. 22(2) GDPR. This therefore requires controllers to not only identify an appropriate legal basis under Art. 6 GDPR, but also an applicable derogation. Controllers must therefore ensure that:

- These activities are strictly necessary in order to enter into and/or perform a contract with the data subject (Art. 6(1)(c) and 22(2)(a) GDPR);[218]

---

[214] Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' WP251 rev. 01, 20-21 (6 February 2018) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053> accessed 23 January 2020.

[215] ibid 21.

[216] ibid 21.

[217] ibid 22.

[218] *See*, ibid 23, in which it is suggested that using an automated individual decision-making process to create a shortlist of possible candidates may be possible under the GDPR.

- They have the explicit consent of the data subject (Art. 6(1)(a) and 22(2)(c) GDPR); or
- An EU or Member State law authorises (though not necessarily obliges) the controller to perform these activities (Art. 22(2)(b) GDPR, which may be paired with Art. 6(1)(c), (d), (e) or (f) as a legal basis).[219]

If special categories of personal data are involved, then there is a further restriction which must be met by controllers under Art. 22(4) GDPR. Controllers must either obtain explicit consent from data subjects, or otherwise be in a position to demonstrate the application of the derogation set out under Art. 9(2)(g) GDPR.

In any case where the controller relies on the derogations related to the entering into/performance of a contract, or data subjects' explicit consent, the controller will be required to implement safeguards to ensure that data subjects' rights and freedoms are protected under Art. 22(3) GDPR. As a minimum, these measures should include the possibility for data subjects to request human intervention (human review of decisions, carried out by someone with appropriate authority and capability to reverse or amend decisions if needed), express their point of view, and contest decisions. Other safeguards which should be considered by controllers include implementing a process to carry out frequent reviews of the datasets, algorithms, and decision-making systems used, to control for errors, inaccuracies, or bias. Such reviews should be carried out either by the controller or by independent third parties (such as auditors), not only at the design stage of the decision-making system, but also as part of a process of continuous monitoring, with review outcomes being used to improve the system's design.[220] The incorporation of clearly-defined retention periods for personal data and profiles used in the decision-making process and the use of anonymisation/pseudonymisation techniques whenever feasible, among others, may also be considered.[221]

---

[219] GDPR, Recital 71: "*However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller.*"

[220] Art. 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the purposes of Regulation 2016/679' (n 214) 27-28.

[221] ibid 32.

V. Enforcement of the General Data Protection Regulation

Until now we have focused on laying out practical implications of the GDPR's principle of accountability, reflected in the six steps comprising the development of our proposed Data Protection Compliance Framework. The objective of this Framework, as with all measures taken by companies to address data protection requirements, is to develop practical policies, procedures, templates, notices, and records which can be used by those companies to meet the requirements of the GDPR. This includes the generation of concrete evidence which can be used to demonstrate compliance to inquiring supervisory authorities, data subjects, and business partners.

It is also important to understand what powers are given to supervisory authorities under the GDPR, analysing their shift from a position of 'gatekeeper' under the Data Protection Directive (where they were generally granted broad powers of prior consultation and authorisation, requiring controllers to notify or seek permission from supervisory authorities in order to carry out certain processing activities) to a position focused more heavily on investigation, monitoring and sanctioning. This shift comes about as a natural consequence of the principle of accountability. While a much larger degree of flexibility is granted to controllers in deciding how to carry out their processing activities in compliance with legal requirements, those same controllers are also held directly responsible for those decisions.

A. Powers granted to supervisory authorities

Supervisory authorities are given a wide variety of tasks under Art. 57 GDPR, including the monitoring and enforcing of the application of the GDPR, the handling of complaints lodged against controllers or processors, and the conduction of investigations on the application of the GDPR, among several others of varied scopes (such as promoting public awareness and understanding related to data protection, and advising on legislative and administrative measures with an impact on personal data). In order to carry out these tasks in a completely independent manner,[222] supervisory authorities are granted a set of investigative, corrective, authorisation, and advisory powers, under Art. 58 GDPR.

[222] GDPR, art 52 requires supervisory authorities to be completely independent in performing their tasks and exercising their powers, remaining free from external influence, whether direct or indirect, and neither seeking nor taking instructions in their domain of competence.

The authorisation and advisory powers granted to supervisory authorities under Art. 58(3) GDPR, are narrow and specific, as opposed to those within the Data Protection Directive. For the most part, the need for prior notification or request for authorisation from a supervisory authority in order for a controller to carry out its processing activities has been removed. However, as previously noted,[223] controllers are still required to seek prior consultation from the competent supervisory authority in the event that a concluded data protection impact assessment "*indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation*" (Recital 94 GDPR, Art. 36 GDPR), without which the intended processing may not take place. Supervisory authorities are also entitled to advise on and approve draft codes of conduct, data protection certifications, standard data protection clauses, contractual clauses/administrative arrangements which may be used to legitimise transfers of personal data to outside the EEA, and binding corporate rules.

Supervisory authorities' investigative powers, as laid out in Art. 58(1) GDPR, allow them to order controllers and processors to provide, and to obtain from those controllers and processors, any personal data and information required for those authorities to perform their tasks. They may also carry out investigations on the premises, data processing equipment and means used by controllers and processors, and trigger these investigations (which can also take the form of actual audits) as a result of a complaint received, or proactively. Companies should strongly consider establishing internal procedures which lay down practical and easy-to-follow rules for interaction with the supervisory authority, assigning roles to individuals charged with addressing information requests or assisting authority representatives during inspections, and identifying elements which can be shared with authorities in order to evidence the company's compliance (such as the company's record of processing activities, information notices, signed data processing agreements, descriptions of security measures in place, registers of data breaches, and data subject requests, and so forth). Ultimately, an inspection from a supervisory authority is the definitive test as to whether the company has adequately complied with the principle of accountability, in that it is able to produce relevant and sufficient elements to prove that it meets all requirements laid down in the GDPR.

---

[223] *See*, s. IV.C.i.: Risk assessments and data protection impact assessments.

Supervisory authorities are also able to notify controllers and processors of any GDPR infringements they may detect. This will typically trigger the exercise of the supervisory authority's corrective powers. Under Art. 58(2) GDPR, supervisory authorities may issue formal warnings and reprimands to controllers and processors, and further order those controllers and processors to take specific steps in order to correct any detected infringements within a given period of time. Furthermore, supervisory authorities are also granted specific powers to react to specific types of infringements, such as the ability to order a controller or processor to comply with a valid data subject request, to order a controller to communicate a personal data breach to the affected data subjects and to order the suspension of data flows to outside of the EEA. Finally, supervisory authorities may require certain processing activities to be temporarily or definitively limited (and may even ban a controller or processor from carrying out those activities), and impose administrative fines upon controllers and processors, in addition to or instead of taking any other corrective measures.

B. Administrative fines

The GDPR requires supervisory authorities to make an individual assessment of each case when deciding on whether or not to impose corrective measures upon an infringing controller or processor. All corrective measures at the disposal of a supervisory authority, including the imposition of administrative fines (whether autonomously, or in combination with other corrective measures) must be considered in order for the supervisory authority to select the most appropriate solution to each situation.[224] Art. 83(2) GDPR provides supervisory authorities with a list of factors which they must consider in two separate, yet related assessments. The first assessment covers whether or not to impose an administrative fine upon an infringing controller or processor, and the second covers the amount of the administrative fine to be imposed.

The first factor to be considered is the nature, gravity, and duration of the specific infringement. Most of the obligations upon controllers and processors within the GDPR are categorised, in terms of their nature, in the terms of Arts. 83(4) to (6) GDPR. These provisions set up two distinct maximum amounts for administrative fines which may be imposed, depending on the obligations which are infringed. In doing so, the GDPR indicates that the infringement of some obligations will, by its very nature, be more serious

[224] Article 29 Working Party, 'Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679' WP253 (3 October 2017) 7 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237> accessed 23 January 2020.

than the infringement of others.[225] Under the terms of Recital 148 GDPR, it is also possible for supervisory authorities, when faced with an infringement which they deem minor (in that it is understood as not posing a significant risk to the rights of the concerned data subjects), to instead resort to a reprimand or other corrective measures considered more appropriate. If an infringement has been previously addressed in an order issued by the supervisory authority, which the controller or processor failed to properly follow, this will indicate a higher level of gravity for the infringement. The number of data subjects affected is also relevant, as it may help to distinguish isolated incidents from systematic infringements or cases evidencing a lack of adequate policies, procedures, or routines on the part of the controller or processor.[226] The purposes for which the data concerned were processed will also be taken into consideration, particularly to ensure that the principle of purpose limitation was appropriately upheld.[227] Although supervisory authorities are not competent under the GDPR to award compensation to data subjects for damages suffered as a result of an infringement (as this will fall upon national courts), these actual or potential damages will influence the gravity of the infringement and, consequently, the assessment of supervisory authorities.[228] Finally, the duration of the specific infringement will also be taken into account, as it may illustrate wilful misconduct, or otherwise a failure or inability on the part of the controller or processor to implement appropriate measures to prevent the recurrence or continuation of a given infringement.[229]

Second, supervisory authorities must consider whether they are able to assign an intentional or negligent character to the infringement. Intentional breaches, which demonstrate contempt for the GDPR's provisions, will be dealt with more severely than unintentional breaches, and are therefore more likely to draw an administrative fine (and higher amounts are fined).[230] For example, the fact that the top management of a controller or processor authorised an unlawful processing activity, in spite of advice received to the contrary by their data protection officer or in contravention to existing internal policies, is a circumstance indicative of wilful misconduct. Other circumstances, such as where the cause of the infringement is due to human error, or a failure to apply technical updates to a system in a timely manner, may

[225] ibid 9.
[226] ibid 10.
[227] ibid 11.
[228] ibid 11.
[229] ibid 11.
[230] ibid 12.

be more indicative of negligence.[231] To quote the Article 29 Working Party, "*Enterprises should be responsible for adopting structures and resources adequate to the nature and complexity of their business. As such, controllers and processors cannot legitimise breaches of data protection law by claiming a shortage of resources*".[232] Companies should find appropriate means by which to meet all of their obligations under the GDPR, as a lack of resources to do so will generally not be considered a valid excuse.

Third, whether or not the controller or processor took any actions to mitigate damages caused (or the potential for damages caused) to data subjects by the infringement will be considered. This may include, for example, contacting other recipients of personal data with whom those data were mistakenly or unlawfully shared (so as to request the deletion or return of those data), or taking timely action to stop infringements from continuing or expanding.[233]

Fourth, the technical and organisational measures implemented by the controller or processor, in compliance with their obligations under Arts. 25 GDPR (on the principles of data protection by design and by default) and 32 GDPR (on security of processing), will be assessed to determine the degree of responsibility on the part of the controller or processor for the infringement occurred. The supervisory authority will consider whether the controller or processor has implemented industry standard measures, measures included within relevant codes of conduct or measures which have been considered as 'best practices' in this assessment.[234] The questions which will be asked by the supervisory authority will be four-fold:[235]

- Has the controller implemented technical measures which follow the principles of data protection by design and by default?
- Has the controller implemented organisational measures which give effect to those principles, at all levels of the organisation?
- Has the controller or processor implemented measures to ensure an appropriate level of security of the personal data processed?
- Are the controller or processor's relevant data protection routines, policies, procedures, or internal rules known and implemented at the appropriate level of management within the organisation?

---

[231] ibid 12.
[232] ibid 12.
[233] ibid 13.
[234] ibid 13.
[235] ibid 13.

Fifth, whether or not any relevant previous infringements by the controller or processor in question have taken place will be considered. The supervisory authority will assess the controller or processor's 'track record', focusing on whether the same type of infringement has been committed before, or whether other infringements have been committed in the same manner (for example, as a result of inappropriate risk assessments, a lack of response to data subject requests in a timely manner, or the insufficient implementation of appropriate policies within the organisation).[236]

Sixth, the supervisory authority will also consider to what extent the controller or processor has cooperated with the authority, so as to remedy the infringement and mitigate its potential negative impact. Legally required cooperation will not be a mitigating factor (for example, allowing the supervisory authority to access premises and equipment used in the processing of personal data). It will generally be valued positively that the controller has responded to requests from a supervisory authority during the investigation of a possible infringement in a manner which resulted in the limitation of that infringement's impact[237] (for example, by proactively suspending processing activities concerning which supervisory authorities cast doubts as to their lawfulness, until those doubts are fully resolved).

Seventh, the categories of personal data affected by the infringement will be taken into account. Key points which will be considered by the supervisory authority include whether special categories of personal data, or personal data related to criminal convictions or offences, were affected, the degree to which the affected data allows data subjects to be identified, whether those data were subjected to any sort of technical protection (including encryption) and whether those data are of the sort to cause immediate damage or distress to individuals if unduly disclosed.[238]

Eighth, the supervisory authority will assess the manner in which it was made aware of the infringement. Examples include investigations carried out by the supervisory authority, complaints received from data subjects, articles in the press, and anonymous tips or notifications made directly by the controller or processor in question. It should be noted, however, that legally required notifications will not be considered a mitigating factor (for example, the obligation for controllers to notify the occurrence of a personal data breach under Art. 33 GDPR).[239] If a legally required notification is not car-

[236] ibid 14.
[237] ibid 14.
[238] ibid 14-15.
[239] ibid 15.

ried out, or is carried out in an inadequate or incomplete manner, this may instead be considered an aggravating factor by the supervisory authority.[240]

Ninth, whether or not the controller or processor complied with corrective measures previously imposed by the supervisory authority regarding the infringement at hand will be considered, as noted above.

Tenth, the fact that a controller or processor is adherent to an approved code of conduct or an approved certification mechanism may influence the supervisory authority's decision, particularly where the code of conduct allows for effective monitoring and correction mechanisms and measures which, in themselves, are considered effective, proportionate, and dissuasive enough by the supervisory authority to lessen the need for an administrative fine. In any case, the supervisory authority's tasks and powers are not prejudiced by those of a code of conduct's monitoring body. This means that the authority is not required to consider sanctions which that body may have previously imposed upon the controller or processor in question. It may further be considered that a lack of compliance with self-regulatory measures within a code of conduct or certification mechanism further evidence the negligence or wilful misconduct of that controller or processor.[241]

Finally, the supervisory authority may also consider any other factors which, in the context of the particular case, may be deemed as aggravating or mitigating. These may include financial benefits gained or losses avoided as a result of the infringement (whether directly or indirectly). In particular, the Article 29 Working Party has stated that "*[i]nformation about profit obtained as a result of a breach may be particularly important for the supervisory authorities as economic gain from the infringement cannot be compensated through measures that do not have a pecuniary component. As such, the fact that the controller had profited from the infringement of the Regulation may constitute a strong indication that a fine should be imposed*".[242]

Having assessed all of the above factors, the supervisory authority will come to a decision as to whether or not an administrative fine is an appropriate corrective measure to be imposed, alone or jointly with others. This assessment will also be carried out to determine the amount of the specific fine, within the maximum limits set by the GDPR:

---

[240] ibid 15.
[241] ibid 15-16.
[242] ibid 16.

- Under Art. 83(4) GDPR, 10,000,000.00 EUR (ten million Euros), or 2% of an undertaking's total worldwide annual turnover of the preceding financial year (whichever of the two is greater), for infringements which are generally considered less serious;[243]
- Under Art. 83(5) GDPR, 20,000,000.00 EUR (twenty million Euros), or 4% of an undertaking's total worldwide annual turnover of the preceding financial year (whichever of the two is greater), for infringements concerning:
  - The principles of data processing, including conditions for valid consent (Arts. 5 to 7 and 9 GDPR);[244]
  - Data subject's rights (Arts. 12 to 22 GDPR);
  - Rules on transfers of personal data outside the EEA (Arts. 44 to 49 GDPR);
  - Provisions implemented by Member States to further densify the rules of the GDPR, on matters such as freedom of expression and information, public access to official documents, processing of national identification numbers, processing in the context of employment, processing for archiving/research/statistical purposes, obligations of secrecy, and processing related to churches and religious associations (Arts. 85 to 91 GDPR, as well as the applicable local provisions);

---

[243] The collection of data via information society services based on children's consent (GDPR, art 8); the rules on processing activities which do not require the identification of data subjects (GDPR, art 11); the principles of data protection by design and by default (GDPR, art 25); the rules on joint controllership (GDPR, art 26); the appointment of a representative for a controller or processor not established in the EU (GDPR, art 27); the rules on engagement of processors and sub-processors (GDPR, art 28); obligations imposed upon persons processing personal data under the authority of a controller or processor (GDPR, art 29); records of processing activities (GDPR, art 30); the obligation to cooperate with supervisory authorities (GDPR, art 31); security of processing (GDPR, art 32); notification and communication of personal data breaches (GDPR, arts 33 and 34); data protection impact assessments and requests for prior consultation from a supervisory authority (GDPR, arts 35 and 36); the rules on designation, position and tasks of the data protection officer (GDPR, art 37-39); and the rules on certification mechanisms and bodies (GDPR, art 42-43), as well as on the obligations of monitoring bodies for codes of conduct (GDPR, art 41(4)).

[244] Interestingly, neither art 83(4) or (5) expressly refer to infringements of GDPR, art 10, on the possibility for lawful processing of personal data related to criminal convictions or offences. Given, however, GDPR, art 83(5) covers infringements of the data protection principles, and that compliance with GDPR, art 10 is a requirement for the principle of lawfulness in relation to such personal data to be met, it can reasonably be argued that an infringement of GDPR, art 10 may be met with the higher of the two tiers of fines under the GDPR.

- Failure to comply with orders imposed by a supervisory authority, as well as other corrective measures, including temporary or definitive limitations on processing activities or the suspension of data flows (Art. 58(2) GDPR);
- Failure to provide access to relevant information, personal data, premises, processing equipment or means required by a supervisory authority to perform its tasks (Art. 58(1) GDPR).

- Art. 83(6) GDPR emphasises the point made by the last infringements listed in Art. 83(5) GDPR, by restating and expanding on the fact that "*[n]on-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher*".

It should be noted, additionally, that if several provisions of the GDPR are infringed in a single case, the authority may consider the maximum fine amounts set for the gravest infringement when deciding on the fine to apply in the specific case. However, it may not exceed that maximum amount, as set out in Art. 83(3) GDPR.[245]

Supervisory authorities across the EU are expected to expand upon the guidance provided by the Article 29 Working Party on this matter and develop their own guidelines for the application of fines, for the benefit of controllers and processors within their territorial scope of competence, as done, for example, by the Dutch *Autoriteit Persoonsgegevens*.[246]

---

[245] For example, if a controller fails to properly regulate a relationship with a non-EEA processor by means of a written agreement (GDPR, art 28, the infringement of which is covered by GDPR, art 83(4)) and, in doing so, allows the transfer of personal data outside of the EEA without implementing appropriate safeguards to cover the transfer, such as by entering into appropriate standard contractual clauses with the processor (GDPR, art 46, the infringement of which is covered by GDPR, art 83(5)), it will have infringed at least two separate obligations under the GDPR – in this case, the supervisory authority, having decided to impose a fine, would be able to decide on the amount of the fine within the greater of the two maximum limits set in GDPR, art 83 (that of GDPR, art 83(5)), without exceeding that maximum limit.

[246] <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-14586.pdf> accessed 23 January 2020 (in Dutch).

VI. Decisions rendered by supervisory authorities on the monitoring and enforcement of the GDPR

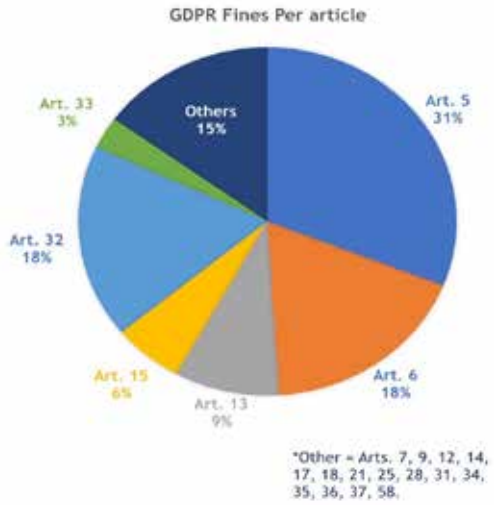

Fig. 2: GDPR Fines Overview per Article

We will now carry out an abbreviated review of supervisory authority decisions on data protection under the GDPR made public to date where administrative fines have been applied as a corrective measure. The objective of this is to provide a more practical insight into how supervisory authorities across the EEA have applied the GDPR's rules. Cases have been grouped together based on their subject-matter and include a succinct explanation of the facts of the case, the decision and the reasoning presented by the supervisory authority, as well as any relevant conclusions which may be drawn. Information on these cases has been gathered from multiple sources, including published decisions rendered by supervisory authorities (or official press releases related to those decisions), and reputable databases compiling summaries, translations, and references to decisions issued by authorities across the EU. This compilation has been carefully selected by the authors and it seeks to provide an inclusive, while not exhaustive, overview of EEA supervisory authority 'caselaw'.

In the selection process of the caselaw, more than 100 European supervisory authority enforcement actions were considered,[247] including those

[247] While the compilation of caselaw analysed and used to develop the chart and related statistics aims to be complete, it is important to point out that not all supervisory authority

which had been issued until the end of 2019, and some combined violations, eg, a sanction as a result of violations of both Articles 6 and 17. Specifically, the enforcement actions examined appear to show a concentration of violations of Articles 5, 6, and 32 GDPR. In particular, it should be noted that when combined, the violations related to legal basis (Articles 5, 6) and transparency (Articles 5, 13) constitute more than fifty percent of the enforcement actions which were analysed. The significance of these principles within the European data protection framework landscape appears to be underscored by the relative attention paid to them by the authorities, as demonstrated in the division of sanctions of the chart to the above.

A. Inadequate provision of information to data subjects and requirements for valid consent

Datenschutzbehörde – Austria; 21 December 2018[248]

An individual submitted a complaint with the Datenschutzbehörde. This complaint concerned an alleged infringement of the right to object. The individual's access to a website had been subjected to payment of a fee, upon withdrawal of his consent related to the use of cookies for marketing purposes on that website. The company had implemented two options for access to the website: one which allowed full access (subject to use of the mentioned cookies), and another which required the payment of a fee to allow access to be unlocked in full (though, in this option, no marketing cookies would be set). When accessing the website, visitors could click on a pop-up notice, or simply continue browsing the website in order for marketing cookies to be set. This could be undone by selecting an option available at the bottom of the website's privacy policy. If selected, this option would not allow the website to be used any further, until marketing cookies

decisions are rendered public, and it may also be the case that the precise facts of cases are not accessible. For this reason, the statistics and conclusions drawn from our research should only be considered as indicative of a generalised trend in sanctioning under the GDPR. Further, it is interesting to note that there are a number of 'intentions to fine' (such as the United Kingdom supervisory authority's stance in both the Marriott hotel and British Airways cases) in addition to fines made after the GDPR entered into force, with respect to previous data protection legislation, because the facts of the case preceded the GDPR.

248 The supervisory authority's decision can be accessed at: <https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=de757036-d6db-4a7f-8744-1e203d4cb84c&Position=1&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=14.12.2018&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20181130_DSB_D122_931_0003_DSB_2018_00> accessed 23 January 2020 (in German).

were set once more. Alternatively, users could accept a paid subscription to the website, which would allow complete access to the website without the setting of such cookies.

Upon investigation, the Datenschutzbehörde noted that the website would not set marketing cookies until the visitor had made a conscious decision to allow those cookies to be placed, by clicking on the pop-up notice or continuing to browse the website. The Datenschutzbehörde found that, alternatively, visitors could choose the paid subscription option which, amounting to 6.00 EUR per month, was not considered disproportionately expensive.

In its decision, given that the issue at hand related to consent around the placement of marketing cookies, the Datenschutzbehörde first considered the national Austrian law implementing Directive 2002/58/EC (the '**ePrivacy Directive**'). This is because the ePrivacy Directive serves as *lex specialis* to the GDPR, specifically regulating the processing of personal data and the protection of privacy in the electronic communications sector (with specific provisions on the use of cookies, namely Art. 5(3). Local law confirmed the requirement for consent as a legal basis regarding the use of marketing cookies but did not introduce any further requirements for the validity of this consent, nor define it more specifically. As such, the Datenschutzbehörde turned to the ePrivacy Directive itself which, in its Art. 2(f), defines 'consent' by reference to the definition given in the Data Protection Directive (which, at the time of decision, had already been repealed by the GDPR). This led the Datenschutzbehörde to consider the requirements for valid consent under the GDPR, not least of which was the need to ensure that consent can be refused without detriment to the data subject.

It concluded that the consequences imposed upon a visitor which refused to provide consent were not significantly negative. This meant that the validity of the consent given for the use of cookies was not affected (i.e., this was not enough to consider that the consent was not 'freely given'). Relevant to this conclusion was the fact that the content of the website made available to visitors was exactly the same whether they accepted marketing cookies or paid the subscription fee. The Datenschutzbehörde further noted that rather than the right to object the right at play here was the right to withdraw consent (without detriment to the data subject), under Art. 7 GDPR – and that this right was afforded to data subjects within the website's privacy policy.

Decision: The Datenschutzbehörde dismissed the complaint against the company.

This case deepens the interpretation of the requirements for valid consent under the GDPR (and, consequently, under the ePrivacy Directive). One requirement addressed in particular is the need for data subjects to be able to withdraw or refuse their consent without detriment (Recital 42 GDPR). The Datenschutzbehörde considered that this requirement may still be met where, although there is an objective detriment to the withdrawal or refusal to provide consent (such as the requirement to pay the fee in order to continue using the services), this detriment is not significant upon the data subject. This will be the case, according to this decision, where the data subject is allowed to continue making full use of the services, subject to a limited and not disproportionate payment. While this may seem very appealing for controllers wishing to create incentives to consent for the use of profiling cookies on their websites, it should be borne in mind that other supervisory authorities may not be inclined to follow the orientation of the Datenschutzbehörde. An argument that consent is not freely given when its refusal or withdrawal is subject to detriment of any kind for the data subject, is still feasible under the GDPR, and stricter supervisory authorities are likely to apply it. Therefore, controllers should carefully consider the manner in which they ask for consent from visitors to their websites for these purposes, namely by ensuring that cookies are not set without a clear, affirmative action on the part of the visitor (such as by clicking a button in a pop-up notice) and, as best practice, not creating any restrictions upon users that refuse or withdraw this consent.[249]

Commission Nationale de l'Informatique et des Libertés – France; 21 January 2019[250]

On 25 and 28 May 2018, the CNIL received group complaints from two separate associations (*None of Your Business* and *La Quadrature du Net*). These complaints concerned the data protection practices of Google LLC ('**Google**'), notably alleging that Google had not established an appropriate legal basis for the processing of personal data of users of its services for advertisement personalisation purposes. At the start of investigations, the CNIL initiated discussions with other EU supervisory authorities to determine whether any authority could be

[249] Similar decisions have also been decided by other Data Protection Authorities, such as in the Belgian DPA's decision to impose an administrative fine on 'Jubel.be'.

[250] French Commission Nationale de l'Informatique et des Libertés, 'The CNIL's restricted committee imposes a financial penalty of 50 Million euros against Google LLC' (21 January 2019) <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>. The full decision is available (in French) at: <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1> accessed 23 January 2020.

classified as the 'lead supervisory authority' under Art. 56 GDPR for this case. The conclusion on this, confirmed also after discussion with the Irish supervisory authority (considering that Google's European headquarters are located in Ireland), was that no such lead authority could be identified. This was because none of the Google subsidiaries located in Europe had any real decision-making powers concerning the advertisement personalisation activities in question (which were found to be totally controlled by the US-based Google LLC). As a result, the GDPR's 'one-stop-shop mechanism', under which the lead supervisory authority would be solely competent to handle the investigation and potential sanctioning, was found to be inapplicable to this case. This opened the floor for any supervisory authority, including the CNIL, to take a decision on Google LLC's practices.

The CNIL noted that Google did not provide information on these processing activities (including advertisement personalisation and geolocation services) to users in a manner which was easily accessible. In particular, essential aspects, such as the purposes of processing, retention periods, and categories of personal data used were spread out across several documents, requiring users to click across multiple links and pages in order to attempt to understand the processing in question. Even where users were able to access all relevant information, it was not always deemed clear or comprehensive. Purposes of processing and categories of data used were described in a vague and generic manner, providing misleading information as to the legal basis relied on by Google for these purposes (i.e., consent), and incomplete information as to retention periods was given. This resulted in an inability for users to fully understand the extent of these processing activities, which were deemed "*particularly massive and intrusive*" by the CNIL, given the number of services offered, as well as the amount and nature of data used and combined.

It was further noted by the CNIL that, although Google purported to rely on user consent for advertisement personalisation purposes, consent obtained by Google did not meet the requirements for its validity under the GDPR. Not only was insufficient information provided for the consent to be 'informed' (as seen above), but it was also found that the manner in which consent was obtained did not allow it to be considered 'specific' or 'unambiguous'. While an option to allow or disallow the use of personal data for advertisement personalisation was granted to users, the CNIL found it inappropriate that this option was pre-ticked (thereby allowing, by default, the use of personal data for these purposes). It was also deemed inappropriate that users were required to navigate through an overly complex menu in

order to be able to change that option. Further, the CNIL disapproved of Google's practice of requesting users to, prior to the creation of an account, tick in a box labelled "*I agree to the processing of my information as described above and further explained in the Privacy Policy*". This was considered as bundling various different processing purposes in a single request for consent, as opposed to presenting granular and specific consent options for users (allowing them to, for instance, specifically accept or refuse use of their data for advertisement personalisation purposes).

Decision: The CNIL imposed an administrative fine amounting to 50,000,000.00 EUR, having justified this amount on the basis of the severity of the detected infringements. These infringements reported to several data protection principles, namely, transparency, fairness, and lawfulness. It was further deemed relevant that the processing operations in question were capable of revealing important aspects of users' private lives, considering the vast amounts of personal data processed, the wide variety of services offered by Google through which those data might be collected and the potentially unlimited number of combinations and matches which could be made with those data. Adding to this, users were not offered any relevant or significant guarantees, such as the ability to control the use of their data, obtain relevant information about the use of their data, or provide valid consent. The infringements were deemed to be ongoing, rather than one-off incidents. The fact that several users affected by Google's infringing activities were located in France was deemed relevant in light of the CNIL's territorial competence, as well as the fact that Google's economic model was at least partly based on these advertisement personalisation activities.

Google was the first of the major information society service providers on the market to be the target of an administrative fine under the GDPR, and a record-breaking one at that. Controllers should pay special attention to the manner in which they present information to data subjects concerning the processing of personal data inherent to their services. It should be possible for users to have a clear picture of all of the information required by Arts. 13 and 14 GDPR in an easily accessible manner. Layered privacy policies may be an effective means of achieving this while also avoiding information fatigue, for example.[251] When relying on consent as a legal basis, controllers need to pay attention to whether all requirements for the validity of consent are met. Pre-ticked boxes cannot generate valid consent under the GDPR,

[251] *See*, for example, UK Information Commissioner's Office, 'What Methods can We Use to Provide Privacy Information?' (n 110).

nor can methods to obtain consent which are ambiguous (such as informing users, in a pop-up banner, that their personal data will be used for analytics or profiling purposes if they simply continue to browse a website). It is also important to ensure that each purpose of processing for which consent is to be used has its own, specific request for consent, instead of bundling all purposes into a single request.

Personal Data Protection Office ('UODO') – Poland; 8 April 2019[252]

The UODO investigated the personal data processing practices of a Polish company. This company had indirectly sourced personal data and subsequently processed it for commercial purposes. The company had retrieved personal data from public sources, such as the national Central Electronic Register and Information on Economic Activity. However, it had not fully informed all data subjects concerned despite having access to their postal addresses and telephone numbers. In fact, the company had sent out e-mails to around 90,000 data subjects to inform them of the company's processing activities but had not reached out to the remaining 12,000 or so data subjects due to the operational costs involved. Instead, the company had published a notice on its website in order to address transparency requirements, relying on Art. 14(5)(b) GDPR. However, the UODO considered this notice to be insufficient. Instead, the UODO clearly stated that the company should have fully informed the entire relevant data subject base on the points listed in Art. 14 GDPR (particularly, the categories of data collected, the sources used, the purposes for which those data would be processed, the retention period applied and their rights under the GDPR), in order to allow them to effectively exercise their data subject rights against the company, if so desired.

Decision: The UODO imposed an administrative penalty amounting to approximately 219,760.00 EUR upon the company.

When sourcing personal data indirectly (i.e., collecting personal data from sources other than the data subject him/herself, such as publicly available sources or data brokers), controllers must take particular care to ensure that they provide all necessary information to data subjects under Art. 14 GDPR. While it is possible for controllers to avoid direct notifications where they are able to demonstrate that this is impossible, or would require a disproportionate effort, the bar for this to be the case is set fairly high by

[252] A press release covering the supervisory authority's decision can be accessed at: <https://uodo.gov.pl/en/553/1009> accessed 23 January 2020.

supervisory authorities.[253] Therefore, whenever possible, controllers should give preference to these direct notifications as opposed to merely publishing an information notice on their website (in fact, the ideal approach is to carry out a combination of the two).

> **Commission Nationale de l'Informatique et des Libertés – France; 26 November 2019**[254]
>
> The CNIL carried out an on-premise inspection at Futura Internationale, following a complaint of a data subject received on 6 February 2018. The complaint alleged that the company had continued to solicit the data subject over the phone, even though the data subject had objected to this, both orally and in writing. Futura Internationale had fewer than 100 employees and was specialised in the thermal insulation of private homes – it made use of call centres, located outside the European Union, for telemarketing purposes. Specifically, by engaging a number of call centres located in North Africa, Futura Internationale caused a transfer of personal data outside of the European Union, related to individuals contacted by the call centres on its behalf.
>
> The on-site inspection carried out by the CNIL revealed that the company had received several written objections from data subjects regarding direct marketing communications. It further revealed that the company's files – specifically, records in their Customer Relationship

---

[253] The Article 29 Working Party, in its Transparency Guidelines notes that "*[t]he situation where it 'proves impossible' under Article 14.5(b) to provide the information is an all or nothing situation because something either is impossible or it is not; there are no degrees of impossibility. Thus if a data controller seeks to rely on this exemption it must demonstrate the factors that actually prevent it from providing the information in question to data subjects. If, after a certain period of time, the factors that caused the "impossibility" no longer exist and it becomes possible to provide the information to data subjects then the data controller should immediately do so. In practice, there will be very few situations in which a data controller can demonstrate that it is actually impossible to provide the information to data subjects*" (p. 29), and "*Where a data controller seeks to rely on the exception in Article 14.5(b) on the basis that provision of the information would involve a disproportionate effort, it should carry out a balancing exercise to assess the effort involved for the data controller to provide the information to the data subject against the impact and effects on the data subject if he or she was not provided with the information. This assessment should be documented by the data controller in accordance with its accountability obligations*" (p. 31).

[254] French Commission Nationale de l'Informatique et des Libertés, 'FUTURA INTERNATIONALE: sanction de 500 000 euros pour démarchage téléphonique illégal' (26 November 2019) <https://www.cnil.fr/fr/futura-internationale-sanction-de-500-000-euros-pour-demarchage-telephonique-illegal> accessed 23 January 2020. The full decision is available (in French) at: <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000039419459&fastReqId=461698027&fastPos=1> accessed 23 January 2020.

Management ('**CRM**') system – contained excessive comments and data on individuals, referring also to their health condition. Further, it was found that the subjects of telemarketing campaigns carried out were not adequately informed that their personal data was being processed, and that the phone conversations with the call centres were being recorded.

In 2018, the CNIL issued a formal notice to the company, requiring it to adopt necessary corrective measures in order to bring its practices into compliance with the GDPR. Futura Internationale, however, failed to provide the CNIL with a satisfactory response. The CNIL, therefore, initiated a sanctioning procedure.

It was determined that the company, also due to the persistence and severity of its compliance shortcomings, should be fined for five different GDPR violations. These included the lack of information provided to the persons contacted on the processing of their personal data and the rights from which they benefit (Articles 12, 13 and 14 GDPR), the failure to respect the right to object to data processing (Article 21 GDPR), and the failure to process data that are adequate, relevant, and limited to what is necessary for the purpose of the processing (Article 5(1)(c) GDPR). Additionally, the CNIL also considered the failure to provide appropriate safeguards in the transfer of personal data outside the European (Article 44 GDPR) and the failure to cooperate with the CNIL (Article 31 GDPR).

Decision: The CNIL imposed an administrative penalty amounting to a 500,000.00 EUR fine upon the company.

This case illustrates the importance of ensuring that data processing activities adhere to the data protection principles of Article 5 GDPR. The CNIL considered that including extensive comments and arbitrary additional information, which may have been extracted at any given time, in the company's CRM records was in breach of the principle of data minimisation. Additionally, the CNIL emphasised that adequately informing data subjects must occur in all cases where the GDPR applies, even where call centres outside of the European Union are relied upon to promote campaigns and marketing communications. In this case, information relating to the data transfers to non-EU countries must also be disclosed to data subjects, including the details of the personal data which is transferred and the criteria for their retention.[255]

[255] ibid.

Under the GDPR, data processing activities must be in line with the principles established in Article 25 (data protection by design and by default) and appropriate technical and organisational measures should be implemented in processing activities. It is also interesting to note the attention that the CNIL gave, in this case, to the obligations of cooperation with supervisory authorities (Article 31 GDPR), explicitly stating that cooperation with a supervisory authority is an obligation which, if not respected, is punishable under the GDPR,[256] and the fact that the persistence and severity of the company's GDPR violations acted as aggravating factors in the application of the penalty.

Hellenic Data Protection Authority – Greece; 31 July 2019[257]

In response to a complaint alleging that employees were required to consent to the processing of their personal data, the Hellenic Data Protection Authority carried out an *ex officio* investigation concerning the lawfulness of the personal data processing of PRICEWATERHOUSECOOPERS BUSINESS SOLUTIONS SA (PWC BS) employees.

The Hellenic DPA, considering PWC BS as the data controller, determined that the company had unlawfully processed its employees' personal data in violation of Article 5(1)(a) GDPR, insofar as it used an incorrect legal basis for the processing (employee consent), as other legal bases were more appropriate (performance of the employment contract, under Article 6(1)(b) GDPR, compliance with legal obligations, under Article 6(1)(c) GDPR, and pursuit of legitimate interests of the controller, under Article 6(1)(f) GDPR). The Authority further found PWC BS to be in violation of Articles 5(1)(a), (b), and (c) GDPR, for having falsely informed its employees that their data was being processed under the legal basis of consent (Article 6(1)(a) GDPR), when other legal bases were actually being relied on, violating the principle of transparency and the requirement to provide accurate and transparent information pursuant to Articles 13(1)(c) and 14(1)(c) GDPR.

PWC BS furthermore could not demonstrate its compliance with Article 5(1) GDPR and violated Article 5(2) GDPR (accountability), insofar as it transferred the burden of proof for compliance onto the employees (by asking them to sign a statement according to which

[256] ibid.

[257] Hellenic Data Protection Authority, Summary of Hellenic DPA's Decision No. 26/2019 (31 July 2019) <https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/SUMMARY%20OF%20DECISION%2026_2019%20(EN).PDF> accessed 23 January 2020.

> they acknowledged that the personal data processed by PWC BS was directly related to employment/labour-related purposes and needs, and that such data was relevant and appropriate for these purposes and needs).
>
> **Decision:** As a result of these violations, the DPA used its corrective powers to order the company to amend its data processing activities accordingly, within a period of three months, in order to bring them into compliance with the GDPR, namely, with respect to Article 5(1)(a), Article 5(2), and Article 6(1), and to correctly apply Article 5(1)(b)-(f) GDPR in order to effectively meet the requirements of the principle of accountability. Moreover, the Hellenic DPA considered that the corrective actions were not sufficient for this type of violation, and therefore imposed an additional "*dissuasive, proportionate, and effective*" administrative fine of 150,000.00 EUR in accordance with Article 83 GDPR.[258]

The Hellenic DPA demonstrated the importance of choosing an appropriate legal basis to process personal data in an employment relationship. Specifically, the supervisory authority shows that, in order to lawfully process employee data, a careful evaluation of the available legal bases must occur. Carrying out this process is necessary because the controller must choose the legal basis before initiating the processing, and subsequently document this choice internally (according to the principle of accountability, which also includes a demonstration of compliance).In the case at hand, PWC BS does not seem to have carefully evaluated the legal basis (or bases) that it should have relied on to process employee data. In fact, the Article 29 Working Party Guidelines on Consent clarify that consent cannot be used in the context of employment due to the inherent imbalance between an employee and its employer.[259] Notably, the Hellenic DPA stated that consent can only be relied upon in an employment relationship insofar as no other legal bases apply.[260] This would mean that once the initial choice of the legal basis has been made, it must be adhered to until the end of the processing, without switching legal basis in the duration of the processing activities. Controllers are fully responsible for making an appropriate decision on legal basis – they cannot validly seek to share or transfer responsibility for this with the data subjects. The fact that PWC BS placed the burden of proof on its employees, by having them sign a statement through which they would

---

[258] ibid.
[259] Art. 29 Working Party Consent Guidelines 7.
[260] *HDPA Decision No. 26/2019* (n 257).

acknowledge the validity of the use of their personal data, was seen as a negative factor in the supervisory authority's decision.

The appropriate legal basis is closely tied with the principle of transparency since it is one of the matters that must be clearly explained to data subjects, according to Article 13(1)(c)GDPR. In this case, the company informed the employees of the wrong legal basis since consent was not actually relied upon in order to process the personal data.

Garante per la protezione dei dati personali– Italy; 21 June 2019[261]

The Italian Data Protection Authority, the *Garante per la protezione dei dati personali*, in the course of an investigation carried out together with the Privacy Unit of the Finance Police, found that the loyalty program of Pampers required those registering online to also consent to receive advertising communications, in contrast to what is established in recitals 40, 42, and 43 GDPR and Articles 6 and 7 GDPR. The company also used the personal data of more than 1.5 million individuals for purposes other than what was disclosed to them when they signed up for the loyalty program in violation of Article 5(1)(a) GDPR.

In order to obtain a loyalty card, in fact, the company required users to provide two general consents: one for the company and one for related brands. Approximately one million email addresses were unlawfully collected and used by the company without having obtained valid consent.

The *Garante* ordered Pampers to stop its unlawful data processing and to amend its data collection policies in order to obtain free and informed consent, should the company want to pursue promotional and statistical data processing activities. The *Garante* further noted that if the company should wish to carry out further promotional campaigns, it would need to modify the data collection form on its website, in order to allow users to express their free and informed consent. Further, the company was required within 30 days to provide all the relevant information and documents related to the remedial actions that the company put in place in order to comply with the *Garante*'s orders.

Decision: The Italian DPA required Pampers to amend its practices and to comply with the order issued by the *Garante* within 30 days

[261] Garante per la protezione dei dati personali, *Provvedimento del 12 giugno 2019 [9120218]* (21 June 2019) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9120218> accessed 23 January 2020 (in Italian).

and for its unlawful processing issued an administrative penalty (unknown amount) which the company paid.[262]

This case provides insight into the importance of obtaining valid consent. The requirements for consent under the GDPR are not considered to be an additional obligation upon controllers, but rather preconditions for the lawful processing of personal data on the basis of consent. When the processing of personal data is carried out for several purposes, each distinct purpose should be separated, and consent should be obtained for each of them individually (unless another legal basis applies). The consent needs to be specific, as stated in Article 6(1)(a) of the GDPR, which confirms that the consent of the data subject must be given in relation to 'one or more specific purposes'. Specific consent, however, can only be obtained when data subjects are specifically informed about the intended purposes of the data used concerning them. Bundling general consent requests together does not meet the requirements of consent granularity laid down in the GDPR – note, in particular, Recital 43 (though with reference to the need for consent to be freely-given): "*Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.*"

Agencia Española de Protección de Datos – Spain; n.d.[263]

The Agencia Española de Protección de Datos (AEPD) fined La Liga, a Spanish soccer league, following revelations that it had violated Articles 5(1)(a) and 7(3) GDPR.

La Liga's mobile app was capable of remotely activating the microphones of devices on which the app was installed. When the app detected football match audio, it accessed location data in order to determine whether the location where the match was being shown was using 'pirated' streaming (i.e., unofficial or unauthorised streaming of matches).

The AEPD found La Liga did not abide by the GDPR's transparency and consent provisions, as users were not adequately informed that

[262] It is interesting to note that the *Garante* chose to issue this fine under the old Privacy Code, even though the GDPR was consistently referenced throughout the decision.

[263] Agencia Española de Protección de Datos, *Procedimiento Nº: PS/00326/2018, Resolución de procedimiento sancionador* (n.d.) <https://www.aepd.es/es/documento/ps-00326-2018.pdf> accessed 23 January 2020 (in Spanish). Note that no precise date was identified for this case.

their microphone would be accessed (Article 5(1)(a)), nor were they easily able to withdraw their consent for their data to be used in such a manner (in violation of Article 7(3) GDPR). The AEPD ordered La Liga to amend its app in order to notify users of its data collection practices, both upon installation of the app and each time that such collection is activated.

Decision: The Agencia Española de Protección de Datos ordered La Liga to amend its consent and data collection practices within 30 days from its order and imposed an administrative sanction of 250,000.00 EUR.

This case clarifies the importance of adequately informing data subjects on the categories of personal data that will be processed. The data subjects that had downloaded the app of La Liga, automatically activated the microphones of devices, without explaining that this would take place in clear, intelligible and easily accessible way, in a language that the intended audience was to understand.

Without transparency and an appropriate information notice given to data subjects, valid consent cannot be obtained. In this case, the data subjects were not informed that, by merely installing the app, their microphone would be accessed if a football match audio was detected. Mere installation of the app could, therefore, not be considered as an act of valid consent to the use of their phone's microphone and subsequent audio recording. It would further be questionable under the need for consent to be given in an unambiguous manner through a clear and affirmative action (as a user could install the app without being aware of the recording, and therefore the act of installation does not necessarily and clearly signify that the user consents to this), and also under the need for consent to be freely-given (as requiring consent for this processing in order to use the app, in a case where this does not appear strictly necessary for the app to be used, would run afoul of Article 7(4) GDPR).

Agencia Española de Protección de Datos – Spain; 24 September 2019[264]

The Spanish DPA fined Vueling Airlines for non-compliance with rules relating to consent for cookies. The airline's website installed

[264] Agencia Española de Protección de Datos, *Procedimiento Nº: PS/00300/2019*Resolución *R/00499/2019 de Terminación del Procedimiento por Pago Voluntario* (24 September 2019) <https://www.aepd.es/es/documento/ps-00300-2019.pdf> accessed 23 January 2020 (in Spanish).

cookies, including third-party cookies, and did not display a configuration panel or procedure to obtain or withdraw explicit user consent.

The cookie policy was formed in two layers: (1) a pop-up banner allowing only acceptance of all cookies, as well as providing brief general information, and (2) a more extensive cookie policy, informing about the use of various types of cookies and tracking technologies, and explaining how users could configure cookies via their browsers. There were no options to configure cookie preferences on the website (prior to the setting of cookies).

The AEPD noted that a management system or cookie configuration panel should be provided in a granular way in order to allow users to manage their preferences. The fine for invalid cookie consent issued, however, was later reduced after Vueling recognised its responsibility and voluntarily agreed to pay the amount due.

Decision: The Agencia Española de Protección de Datos ordered Vueling to pay an administrative fine of 30,000.00 EUR, which was later reduced to 18,000.00 EUR.

This case demonstrates that appropriate cookie consent procedures are vital to ensure compliance with data protection legislation.

Companies must seek to ensure that they collect cookie consent from users in a valid way. This means, first off, providing users with transparent and easily accessible information on the cookies used on a given website – this can be done through a pop-up banner, linking to further information in a more detailed cookie policy, for example. Users should be given the opportunity to accept all, some, or refuse all cookies at that moment – any cookies which need consent should NOT be set before users have expressly consented to them. 'Expressly' means that merely continuing the browsing of a website, closing the pop-up banner, or clicking on the cookie policy link cannot be seen as acts of unambiguous, valid consent under the GDPR. Users must also retain control over consent given, and be afforded easy-to-use options – available on the website itself – to revise the cookie preferences they have set later on (including to withdraw consent for all cookies set).

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal – Romania; 16 December 2019[265]

[265] Autoritatea Națională de Supraveghere a PrelucrăriiDatelor cu Caracter Personal, *Sancțiune pentru încălcarea RGPD* (16 December 2019) <https://www.dataprotection.ro/?page=sanctiune_pentru_incalcarea_RGPD_2020_2&lang=ro> accessed 23 January 2020 (in Romanian).

The Romanian DPA fined SC Enel Energie SA for violating the provisions of Article 5(1)(d) and (2), Articles 6 and 7, and Art. 21(1) GDPR.

The decision resulted from a complaint alleging that the company had unlawfully processed the personal data of the complainant. The company, in fact, was unable to demonstrate that it had obtained consent for sending communications to the e-mail address it used and had effectively failed to comply with the principle of accuracy. Furthermore, Enel did not take the necessary measures to disable the transmission of notifications, even after the complainant had objected to receiving further communications from Enelon several occasions.

Decision: The Romanian Data Protection Authority imposed two administrative penalties on the company, each for approximately 2,999.00 EUR.

This case shows the importance of keeping demonstrable records of consent, as required also by Article 7(1) GDPR. Consent must, at all times, be recorded in a way that allows the company to demonstrate that it has been obtained, at a later stage. As the company was not in a position to provide evidence of a valid consent for their communications, they were unable to show that they had a legal basis to use the data subject's personal data as they did. Such a lack of documentation is in breach of the principle of accountability, and may result also in presumed breaches of further principles.

B. Legal Bases

Berliner Beauftragte für Datenschutz und Informationsfreiheit– Berlin, Germany; n.d.[266]

The Data Protection Authority of Berlin found that an online bank had processed personal data of former customers without their permission.

The case came to light after the bank refused to open a new account for a former customer of the bank. The complainant suspected that the bank had stored personal data relating to them in a blacklist – however, according to German law, only the data of customers suspected of money laundering can be included in such blacklists.

[266] Berliner Beauftragte für Datenschutz und Informationsfreiheit, Jahresbericht der Berliner Beauftragten für Datenschutz und Informationsfreiheit (n.d.) <https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2018-Web.pdf> accessed 23 January 2020 (in German). Note that no precise date was identified for this case.

> In this case, however, the bank was found to have been storing personal data on all of its former clients in a blacklist. The bank justified this by alleging that it was obliged, under the German Banking Act, to take security measures against customers suspected of money laundering.
>
> The Berlin DPA concluded that, in order for the bank to prevent a new bank account from being opened by potential infringers, only those customers who were suspected of money laundering, or for whom there were other valid reasons for refusing a new bank account, needed to be listed in a blacklist – this rendered the bank's use of personal data on all of its former customers in this manner as unlawful, in violation of the principle of data minimisation and storage limitation. The DPA stated that the bank should refrain from retaining the data of former clients unless it has a legal obligation to do so.
>
> **Decision:** The Berlin DPA fined the bank 50,000.00 EUR.

This case is a pertinent example of the importance of correctly identifying a legal basis, and of the relationship between data protection and blacklists. Where the need to process personal data in connection with a legal obligation is relied on, only the strictly necessary data to comply with such obligation should be processed. Any further data used, under the same legal basis, will be excessive (thereby breaching the principle of data minimisation, as well as lawfulness – unless another legal basis can be found for them).

Blacklists inherently lead to data protection issues, specifically with reference to data quality, the right of information, right of access, and the right to rectification, as has been pointed out by the European Data Protection Supervisor.[267] As the Article 29 Working Party explained in its Working Document on Blacklists, "*entering individuals onto databases on which they are identified in connection with a specific situation or specific facts represents an intrusion*"[268] and may lead to "*adverse and prejudicial effects for the individuals included thereon and which may discriminate against a group of people by barring them access to a specific service or harming their reputation.*"[269]

---

[267] European Data Protection Supervisor, 'Blacklisting and Early Warning Systems' <https://edps.europa.eu/data-protection/data-protection/reference-library/blacklisting-and-early-warning-systems_en> accessed 23 January 2020.

[268] Article 29 Working Party, 'Working Document on Blacklists' WP65 (3 October 2002) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp65_en.pdf> accessed 23 January 2020.

[269] ibid.

The inclusion of personal data within blacklists must still be based on an appropriate legal basis, such as the need to perform a legal obligation. Having identified such a legal basis, controllers must ensure that they process the strict minimum amount of personal data needed to comply with the obligation in question (in relation to the amount of data held on any given person, but also to the persons whose data is held).

> **National Authority for Data Protection and Freedom of Information – Hungary; n.d.**[270]
>
> The Hungarian Data Protection Authority found that an inappropriate legal basis was used by the organisers of the Sziget and Volt festivals (consent, as it was not freely given) and that the controller did not comply with the principle of purpose limitation.
>
> For security-related purposes, the organisers screened hundreds of thousands of individuals, by photocopying their identity documents and taking photographs of them upon entry to the festivals. The Authority noted that data subjects were not presented with adequate information concerning the data processing (Article 13 GDPR). It further questioned whether consent – which was relied on by the organisers as the legal basis in this case – could be considered as freely-given, given that such consent was required in order to allow their attendance to the festival. Further, the quantity of data that the organisers processed was found to be excessive in relation to the declared purposes (identity document information, gender, date of birth) (Article 5 GDPR) and the retention period applied also exceeded what was permitted by law.
>
> **Decision:** The Hungarian National Authority for Data Protection and Freedom of Information fined the organisers approximately 92,146.00 EUR for violating Articles 5, 6, 13, and 17 GDPR.

In this case, given the purposes which the organisers sought to pursue and the fact that consent for this use of personal data could not feasibly be made optional by the organisers (without jeopardizing their security-related concerns), it is clear that consent was not the appropriate legal basis to rely on. If a controller is not able to ensure that a processing activity can remain purely optional for data subjects, without their suffering significant detriment if such option is not taken (or later refused), then consent should not be used.

---

[270] National Authority for Data Protection and Freedom of Information, Ügyszám: NAIH/2019/55/5 (n.d.). <https://www.naih.hu/files/NAIH-2019-55_hatarozat.pdf> accessed 23 January 2020 (in Hungarian).

Instead, the organisers could have considered alternative legal bases, as suggested also by the Authority. Where a legal obligation to perform such screenings existed, they could have sought to rely on Art. 6(1)(c) GDPR; otherwise, it could have been argued that ensuring the security of the festivals represented a legitimate interest of the organisers, under Art. 6(1)(f) GDPR (based on an appropriate legitimate interests assessment).

In any case, regardless of the legal basis chosen, the other principles within Art. 5 GDPR continue to apply – notably, whatever the legal basis a controller chooses, it must still ensure data minimisation and storage limitation.

Agencia Española de Protección de Datos – Spain; 16 August 2019[271]

The AEPD fined Avon Cosmetics for unlawfully processing the personal data of an individual.

The company had registered the individual's personal data in a delinquency file, without first conducting proper due diligence, leading to the unlawful processing of personal data. The incident came to light after a third party ordered products under the name of the individual and did not pay for the products, leading to problems for the individual with his bank. The company was not able to demonstrate that it had received consent to process the personal data of this individual, under Art. 6(1)(a) GDPR, nor that a contract had been signed between them and the person, which did not allow them to rely on Art. 6(1)(b) GDPR either. Therefore, the AEPD further concluded that Avon Cosmetics was not able to demonstrate an adequate legal basis to process personal data in this case, pursuant to Article 6 GDPR.

Decision: The AEPD imposed an administrative penalty on Avon Cosmetics of 60,000.00 EUR for having violated the provisions of Article 6 GDPR. In considering the amount of the fine, the DPA took into consideration the number of individuals involved in the incident and the fact that the company had acted in good faith.

This case shows that companies must not only carefully assess the legal basis that is relied on to process personal data, but also ensure that they are able to demonstrate the validity of their selection. This points to the need to be able to demonstrate consent, as reflected in Art. 7(1) GDPR, but also more generally to the need to be able to demonstrate the requirements for reliance on all other legal bases, as established by the principle of accountability. For Article 6(1)(b) GDPR, in particular, companies must be able to demonstrate

[271] Agencia Española de Protección de Datos, PS - 00159 (n.d.) <https://www.aepd.es/es/informes-y-resoluciones/resoluciones> accessed 23 January 2020 (in Spanish).

that an agreement is in place between them and the data subject (as parties to the agreement), and that the use of personal data is strictly necessary to allow the agreement to be performed.

The Office of the Commissioner for Personal Data Protection of Cyprus– Cyprus; 25 October 2019[272]

Following a data subject complaint against the Louis companies, the Office of the Commissioner for Personal Data Protection of Cyprus carried out an investigation on the companies' practices in using an online automated system that managed and monitored their employees' sick leave.

Specifically, this system was called the Bradford Factor. It automatically graded the sick leave days of employees, based on their duration, frequency and unplanned absences. Seeing as this system processed the dates of an employees' sick leave, as well as their frequency, the company was considered to be processing health-related data, or special categories of personal data under Article 9(1) GDPR. Additionally, the supervisory authority found that the companies were using the results from the Bradford Factor to create profiles of their employees.

The Office of the Commissioner for Personal Data Protection of Cyprus reasoned that the Louis companies indeed have the right, as an employer, to supervise their employees' sick leaves frequency or validity. However, the Authority mentioned that the grading of their employees' sick leaves in such a specific and systematic manner goes beyond the rights of the employer. Further, the employer should have exercised a legitimate interest assessment, in order to balance the companies' right to operate its business and protect it from employees that may harm its legal rights, with the data subjects' rights as employees.

In the case at hand, the Authority believed that the legitimate interest assessment carried out could only justify the use of an automated system which simply numbered the absent employees based on sick leave (for tracking purpose), but not which would automatically process their frequency or other related statistics. It was also considered that the excessive nature of the profiling of the Louis companies' employees could have resulted in inaccurate or misleading information generated about these individuals.

---

[272] The Office of the Commissioner for Personal Data Protection of Cyprus, File number 11.17.001.006.043, 25, October 2019, <http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/ACDFDC478581BEE1C22584EE002EE9C2/$file/2019apofasi%20bradford%20system%20%CE%91%CE%9D%CE%A9%CE%9D%CE%A5%CE%9C%CE%9F%CE%A0.pdf?openelement> accessed 23 January 2020 (in Greek).

> Therefore, the Authority deemed that the Louis companies had not properly established a legitimate interest which outweighed their employees' rights, and, consequently did not have a legal basis for this processing. The Louis companies were further not able to demonstrate that one of the exceptions of Article 9 applied, in relation to the health data processed.
>
> **Decision:** Following the above arguments, the Office of the Commissioner for Personal Data Protection of Cyprus ordered the Louis companies to stop use of the Bradford Factor over the next two months. Additionally, the Authority imposed a total fine of 82,000.00EUR, for breach of Articles 6(1) and 9(2). The Authority mentioned, in its decision, that the large number of data subjects (818 employees), as well as the duration of the infringement, were among the factors taken into account in calculating the penalties.

This case shows that employers will be hard-pressed to justify a systematic monitoring of employee sick leave, especially when performed through an automated system, which may result in negative circumstances for the employees. The Authority made it clear that the employer should have identified an appropriate legal basis for the processing, under Article 6 – which, in this case, could have been its legitimate interests, under Article 6(1)(f) GDPR (as acknowledged also by the Authority), were it not for the excessive nature of the monitoring performed and data collected. The Authority also reiterated the need for a full-fledged legitimate interest assessment, clearly assessing the legitimate interests of the company against the rights and freedoms of the data subjects concerned. Where this evaluation (which must show that such legitimate interests are not overridden by those of the data subjects) is lacking, Article 6(1)(f) GDPR cannot be used as legal basis for the processing.

Additionally, the case serves as an example of the importance of choosing an appropriate derogation under Article 9 (along with a legal basis, under Article 6) for processing employees' health data. It is arguable that the processing of health data, such as information related to sick leave, could have been accepted by the Authority on the basis of Article 9(2)(b) GDPR, if the companies had been able to justify this processing as needed to perform their rights/exercise their obligations as an employer, and had an automated system not been used. However, companies must always consider the least intrusive way of processing their employee's health data, in a manner that would simultaneously meet the employer's objectives and protect employees' personal data and privacy.

Datainspektionen – Sweden; 16 December 2019[273]

The Swedish DPA fined Mrkoll.se, a website that publishes personal data of Swedes above the age of 16, for violating the Swedish Credit Information Act and the GDPR.

The Mrkoll.se website had a publishing certificate which, assumedly, provided it with constitutional protection in Sweden for the majority of its publishing activities. It was therefore considered that the GDPR would not apply to the processing of personal data under those circumstances (i.e., where this is constitutionally foreseen within Sweden).

However, among the information published by Mrkoll.se on individuals, it was also indicated that certain individuals did not have records of non-payment. The Authority classified this information as information on payment defaults, which was out of scope of the aforementioned constitutional protections and, instead, covered more specifically by the Swedish Credit Information Act – including, more specifically, the references made by that Act to the GDPR. Such information could not be published, under this Act, without the Authority's prior authorisation.

Additionally, the website published information on criminal records, which are regulated under the GDPR and which under Swedish law require a specific authorisation of which the website was not in possession.

Decision: The Swedish Data Protection Authority imposed an administrative penalty of 35,000.00 EUR upon the company.

This case shows that local laws may create further requirements for the lawful processing of personal data. Even if the company might have had a legal basis to publish 'information on payment defaults' on its website under the GDPR (eg, Article 6(1)(e) or (f) GDPR), it is still not exempted from complying with any further requirements which may be imposed upon these sorts of personal data by local legislation – in this case, the need for prior authorisation from the Authority.

It is further relevant to note that criminal records data falls under a broader notion of 'judicial data', or 'personal data relating to criminal convictions and offences', for the processing of which, under Article 10 GDPR, a

[273] Datainspektionen, 'Administrative Fine of 35 000 EUR Imposed on the Swedish Website Mrkoll.se' (16 December 2019) <https://www.datainspektionen.se/nyheter/administrative-fine-of-35-000-eur-imposed-on-the-swedish-website-mrkoll.se/> accessed 23 January 2020.

specific legal authorisation, at EU or local level, must exist (alongside a legal basis, under Article 6 GDPR).

C. Video-surveillance

Datenschutzbehörde – Austria; 20 September 2018[274]

An Austrian restaurant had installed a video camera at its front entrance. This camera allowed footage to be captured on most of the public sidewalk in the area. The Datenschutzbehörde considered that the restaurant had not identified an appropriate legal basis for the processing of personal data inherent to this capture of footage. Without an appropriate legal basis, such a large-scale monitoring of a public space would have to be considered unlawful. The fact that the restaurant had not sufficiently advertised the existence of the camera to passers-by was also deemed to be in breach of the GDPR (presumably, the principle of transparency).

Decision: The Datenschutzbehörde imposed an administrative fine amounting to 4,800.00 EUR upon the restaurant owner, plus legal costs incurred in the proceedings. In deciding the amount, the Datenschutzbehörde sought to be proportionate, having stated that the moderate nature of the fine was primarily owed to the fact that the restaurant's annual income did not exceed 40,000.00 EUR.

Any controllers seeking to implement CCTV systems, for whatever purposes, must ensure that they identify an appropriate legal basis under the GDPR (in particular, where a legal obligation to resort to video surveillance does not exist, controllers should carry out and document a legitimate interests assessment to verify that they are able to leverage Art. 6(1)(f) GDPR as a legal basis). The purpose for which the CCTV system is used will also condition several different technical aspects related to the system. These include the number of cameras, position and viewing angle of the cameras, whether cameras should record footage or merely allow for live monitoring, retention periods applicable to the footage, and so on. Controllers must take particular care when pointing video cameras at public spaces, as this is considered a higher-risk form of processing, which requires particular justification. It is important to note that the systematic monitoring of publicly accessible areas on a large scale triggers the obligation for controllers to carry out a data protection impact assessment, under Art. 35(2)(c) GDPR. It is further

[274] A press release covering this decision can be accessed at: <https://www.pressreader.com/austria/salzburger-nachrichten/20180919/281801399873241> accessed 23 January 2020 (in German).

vital to ensure that data subjects are informed of the existence of CCTV cameras, the purpose for their operation and other relevant information laid down in Arts. 12 and 13 GDPR. The most common means of achieving this is through a layered approach: combining on-the-spot notices or stickers (which contain an abridged amount of the essential information, such as the identity and contact details of the controller, location of cameras and purposes of processing) with a more detailed video-surveillance notice/policy, to be made available to data subjects upon request. Controllers may further wish to consider guidance from their competent supervisory authorities which may exist in relation to the use of video-surveillance, if any, in order to ensure that they align their practices with the recommendations of those authorities.[275]

> **Office for Personal Data Protection ('Office') – Czech Republic; 7 February 2019**[276]
>
> Following a complaint submitted regarding the installation of CCTV cameras in and near the bathrooms of a shopping centre, the Office launched an investigation to assess the lawfulness of the centre's video surveillance practices. The centre had installed cameras with a view to protecting the security of the shopping centre and the health and safety of customers and retailers. The cameras were stationary and fixed in a manner which did not allow them to invade the privacy of the specific bathroom stalls used. The centre had further provided an adequate information notice regarding the use of video-surveillance, had subjected footage to appropriate security measures and had internal procedures to address any requests to exercise the right of access concerning those footage.
>
> **Decision:** With all of the above criteria having been met, the Office dismissed the complaint.

---

[275] Another useful and comprehensive reference is the European Data Protection Supervisor's Video-Surveillance Guidelines (17 March 2010). Although prepared on the basis of Regulation (EC) No. 45/2001 of the EU Parliament and of the Council, of 18 December 2000, and aimed at EU institutions and bodies, the similarities between the data processing rules in that regulation and the GDPR allow private and public sector companies to draw valuable best practices from the Guidelines, including technical recommendations on the incorporation of the principles of data protection by design and by default, the identification of legal bases and assessment of necessity/proportionality of the use of CCTV systems, the selecting, siting and configuring of these systems, footage retention, footage access, footage transfers/disclosures, security measures and the provision of information to the public, among other matters.

[276] A press release on the supervisory authority's decision can be accessed at: <https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-prostrednictvim-kameroveho-systemu-v-obchodnim-centru-spolecnost-centrum-chodov-a-s/ds-5418/archiv=1&p1=1279> accessed 23 January 2020 (in Czech).

The design (number of cameras, stationary or dynamic movement of cameras, viewing angles, positioning, and so on) and operation of video-surveillance systems, in relation to the purposes for which they are used, along with the preparation of clear and effective information notices (allowing individuals to become aware that they are under surveillance), are key factors which will be assessed by supervisory authorities, when judging the lawfulness of an implemented CCTV system.

D. Data Protection by Design and by Default; Data Protection Impact Assessments

Hellenic Data Protection Authority – Greece; 7 October 2019[277]

The Greek Data Protection Authority fined the Hellenic Telecommunications Organisation (OTE) for violating the principles of data protection by design and accuracy, and for non-compliance with the right to object.

The Authority received numerous complaints from users with respect to receiving unwanted advertising messages from the company. During the course of an investigation by the Authority, it became clear that such users/data subjects had submitted portability requests to the company, seeking to transfer their subscription to another provider, after which the company deleted their information from their "do-not-call" registry. This led to inconsistencies in the databases that the company shared with its marketing partners and resulted in the individuals being contacted despite having been previously been registered on the "do-not-call" list.

The Authority determined that this had adversely affected a significant number of individuals and that the company had infringed Article 25 (data protection by design) and Article 5(1)(c) GDPR (principle of accuracy), imposing an administrative fine of 200,000.00 EUR. Secondly, the Authority fined the company for "*failure to satisfy the right to object and the principle of data protection by design when keeping personal data of subscribers*." The second part of the fine, again consisting of 200,000.00 EUR, was administered as a result of the lack of possibility for users to unsubscribe from receiving advertising messages where it was impossible, due to a technical error, to unsubscribe via the unsubscribe link. The Authority determined that the company lacked appropriate organisational measures and as a

[277] Hellenic Data Protection Authority, 'Administrative Fines Imposed on a Telephone Service Provider, Ref. No.: 6739' (7 October 2019) <https://www.dpa.gr/portal/page?_pageid=33,43547&_dad=portal&_schema=PORTAL> accessed 23 January 2020.

result that there had been an infringement of the right to object to the processing for direct marketing purposes as per Article 21(3) GDPR and Article 25 GDPR (data protection by design).

Decision: The Hellenic Data Protection Authority fined the telecom for a total of 400,000.00 EUR for infringements to Articles5, 21, and 25 GDPR.

As stressed above, Article 25 GDPR on data protection by design and by default is one of the pillars of effective data protection in practice. This decision by the Hellenic DPA provides some insight into how supervisory authorities are considering data protection by design and how it should be practically implemented.

In essence, companies need to take measures to ensure that each of the principles laid out in Article 5 GDPR are going to be respected when plotting out a given processing activity, system, or project. The 'principles' of data protection by design and by default should not be seen as principles in themselves, but rather as means to achieve those other principles laid out in Article 5 GDPR. Inspecting Authorities wishing to determine whether these "principles" have been complied with will assess how a company's data protection practices currently function, how that company has sought to implement each of the Article 5 principles in a given project, and whether the company has any documentation or records which show that these principles were considered.

In essence, whenever a failure to meet any of the Article 5 GDPR principles can be attributed to a lack of proper planning or foresight on the part of a company, rather than an accident or ad hoc incident, it is reasonable to maintain that Article 25 may also be considered to be in breach. Companies must be aware of this, and incorporate personal data protection within the various business objectives to be met during the design phase of any new activities.

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal – Romania; 27 June 2019[278]

The Romanian DPA issued its first fine under the GDPR to Unicredit Bank SA, after having found that it had breached the provisions of Article 25 GDPR on data protection by design and by default. This

[278] Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, 'Prima amendă în aplicarea RGPD' (27 June 2019) <https://www.dataprotection.ro/?page=Comunicat_Amenda_Unicredit&lang=ro> accessed 23 January 2020.

resulted from an investigation from the Authority, following up on a personal data breach occurred.

The Authority decided that Unicredit had failed to implement appropriate technical and organisational measures, both in the determination of the processing means and the actual processing, and that the bank had failed to implement data minimisation and adequate safeguards. Failure to follow such guidelines permitted the unintended disclosure of data, which included identification numbers and addresses in addition to other personal data.

Decision: The Romanian DPA fined Unicredit for the equivalent of approximately 130,000.00 EUR for having violated Article 5(1)(c) and Article 25(1) GDPR. In its decision, it also called to the text of Recital 78 GDPR, noting the need for implementation of appropriate technical and organisational measures to ensure and demonstrate compliance and with the GDPR, through data protection by design and data protection by default.

Similarly to our conclusions above, where a personal data breach results from a company's lack of proper planning, and lack of measures implemented to address each Article 5 GDPR principle – notably, in this case, data minimisation and security – there is always a reasonable case to maintain that Article 25 GDPR has also been breached.

Therefore, the pressure on companies to take data protection into account when designing new processes (and revising existing processes) is greater – should a personal data breach occur, and this be attributed to missing, insufficient or inappropriate measures to ensure the proper processing of personal data under the GDPR, Article 25 GDPR will likely be called into question (thereby compounding the number of GDPR breaches occurred in a single case, which may increase the total amount of a potential fine).

Datainspektionen – Sweden; 21 August 2019[279]

The Swedish DPA fined a school in Skellefteå for improper use of facial recognition technology used to monitor student attendance in the context of a facial recognition pilot program.

Although the test program concerned only one class, and was carried out for a limited time, the Swedish DPA still determined that the school had processed sensitive biometric data of students in violation

[279] Datainspektionen, 'Facial Recognition in School Renders Sweden's First GDPR Fine' (21 August 2019) <https://www.datainspektionen.se/nyheter/facial-recognition-in-school-renders-swedens-first-gdpr-fine/> accessed 23 January 2020.

> of the GDPR. It noted that consent, the legal basis used for the processing, was not a valid legal basis for such processing, due to the imbalance between the controller (the school administration), and the data subjects (the students).
>
> One key point, however, was that the school was unable to show any evidence of having performed a data protection impact assessment related to the program, under Article 35 GDPR. The Authority noted, in particular, that the use of facial recognition software was disproportionate for the purpose intended; further, given the fact that the activity involved sensitive personal data (under Article 9 GDPR) and posed a high risk to vulnerable data subjects (children), a DPIA should have been carried out and the DPA should have been consulted, under Article 36 GDPR.
>
> **Decision:** The Swedish Data Protection Authority fined the school 200,000.00 SEK (approximately 18,000.00 EUR).

This case illustrates the caution with which companies must proceed, when processing biometric data for the purpose of uniquely identifying individuals (particularly when this concerns vulnerable data subjects such as children). Specifically concerning access/attendance control purposes for schools, this is a matter which requires great prior consideration, as noted also by the CNIL with respect to the use of such technologies in schools.[280]

Whenever an activity is being designed which may create a significant risk to the rights of data subjects – for example, because of the sensitive nature of the data, or the vulnerabilities of the data subjects – a DPIA should be performed. It is generally better for companies to 'be safe than sorry', in this respect. DPIAs are also a prime tool for ensuring compliance with data protection by design and by default, as carrying out a thorough assessment of a project through a DPIA will allow the company not only to identify relevant risks to individuals (and mitigate them accordingly), but also to plot out measures to ensure compliance with each of the specific Article 5 GDPR principles. Furthermore, as a DPIA is always to be documented, it can serve as evidence that data protection by design and by default have been considered for a given project – they are also, therefore, useful accountability tools.

---

[280] See the CNIL's position on the use of facial recognition in schools, 'Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position' (29 October 2019) <https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position> accessed 23 January 2020 (in French).

E. Security of processing and personal data breaches

Comissão Nacional de Proteção de Dados ("CNPD") – Portugal; 17 July 2018[281]

After receiving complaints from a regional doctor's union in Portugal, the CNPD decided to launch an investigation, alongside the national Inspectorate-General for Healthcare Activities, into the data processing practices of a Portuguese hospital. In particular, the complaints alleged that patient data was not being handled by the hospital under appropriate conditions of security. Allegedly, any hospital employee or worker with access to the hospital's systems could gain visibility on data relating to any and all of the hospital's patients, and even register comments and notes on patients' files without the appropriate authorisation to do so (which would be reserved to the doctors in charge of the patients in question).

During the course of the investigation, the CNPD detected that, although the hospital employed around 296 doctors, there were over 980 doctors, psychologists, technicians, staff and dietitians which could freely access patient data, without proper authorisation. This resulted in potential and actual access to patient data by a wide variety of non-medical professionals. Further, a large discrepancy between the actual number of doctors working at the hospital and the number of users recorded on the system as a 'doctor' (with an extended degree of data access rights as a result) was detected. The CNPD also noted a general failure on the part of the hospital to segregate their patient data from data pertaining to patients of other hospitals (given that the system used was shared with other hospitals). A lack of internal policies or rules on the creation of user accounts for the system, or on the assignment of access rights to those users, was also detected. While the hospital had employed authentication measures for system users, these did not take into account appropriate identification data which could establish a correct link between the individual user and the hospital (namely, by identifying that user as an actual doctor). Finally, the hospital had failed to consistently remove access rights pertaining to users who were no longer employed as doctors at the hospital.

The hospital attempted to contest the CNPD's findings by stating that the system put in place had been provided by the Portuguese Ministry

[281] The CNPD's decision was not made publicly available; however, a press release covering the case and its subsequent judicial appeal can be accessed at: <https://www.publico.pt/2018/10/22/sociedade/noticia/hospital-barreiro-contesta-judicialmente-coima-400-mil-euros-comissao-dados-1848479> accessed 23 January 2020 (in Portuguese).

of Health. However, the CNPD countered that the hospital, as controller, was still responsible for ensuring that the systems it uses to process personal data were compliant with the GDPR, and to take all appropriate technical and organisational measures to ensure this. The hospital further maintained that, while unused access profiles still existed on the system, these had not been removed because they were being temporarily assigned to different doctors still employed at the hospital. The CNPD did not accept this argument, instead finding that the hospital had deliberately failed to remove those unused access rights without an adequate justification for this. Finally, the hospital maintained that the system did not allow it to specifically define access rights, so that it could establish certain conditions under which certain users could access specific data. The CNPD found that, in spite of the fact that the hospital was aware of this, it continued to grant undue access rights to a wide variety of users, rather than seek alternatives.

Decision: The CNPD imposed an administrative fine amounting to 400,000.00 EUR upon the hospital. The fine was broken down by the CNPD as follows: 150,000.00 EUR for a breach of the principle of integrity; 150,000.00 EUR for a breach of the principle of confidentiality; 100,000.00 EUR for a breach of the principle of data minimisation. Furthermore, the CNPD considered that the fact that the hospital knowingly acted in contravention to the GDPR, without consulting with the Ministry of Health on the alleged system deficiencies (which could potentially have been corrected), were aggravating factors.

In order to comply with the principle of data minimisation, companies need to be sure that they control the extent to which persons within their organisation can access personal data, so that they do not have access to any more data than they strictly need in order to perform their tasks. One way to achieve this is to identify different job categories within the company and define access profiles with varying degrees of data access. Each profile can then be allowed to access the data which they strictly need to know. Rules on data access and access profile management should be formalised within internal policies and procedures, governing the assignment, amendment, and removal/deactivation of access profiles assigned. Companies should keep a record of the access profiles given to individuals, so that they can explain and justify the level of access to personal data given to all members of their organisation at all times.

Controllers must carefully assess any third-party data processing systems which they seek to implement. Controllers must make sure that those

systems offer an adequate level of technical security, in particular allowing for different access rights to be defined and managed. Controllers will not be able to shield themselves behind technical restrictions within third-party systems, as it is their responsibility to ensure that the systems they use do not create obstacles to compliance.

All of these issues are exponentially more important when handling special categories of personal data, such as health data and genetic data. These dates, by their very nature, increase the risk of the controller's processing activities to the rights and freedoms of the data subjects concerned. Access to special categories of personal data should be heavily restricted and monitored. Special categories of personal data should be segregated from other data where technically possible. The technical and organisational security measures put in place by the controller to safeguard those data should be carefully chosen, in order to minimise the risk of unauthorised access, disclosure, loss, alteration or deletion.

Information Commissioner's Office – United Kingdom; 26 November 2018[282]

An external cyber attack affected the third-party cloud-based storage services used by Uber to store personal data. The attackers were able to gain access to an Uber account's credentials and, subsequently, all files stored in the data store kept by Uber on those services. They were able to download 16 files which contained, in total, records for approximately 32 million Uber service users and 3.7 million Uber drivers. Following a request for compensation from the attackers, in exchange for revealing how they had compromised Uber's systems, Uber took measures to react to the breach. They replaced the compromised credentials and implemented a two-factor authentication system for access to its data stores, paying the sum requested by the attackers and obtaining assurances from the attackers that the downloaded data had been destroyed. Additionally, a number of security measures were implemented in the aftermath of the attack, including new credential management processes, migration of the datastore to internal repositories at Uber, and a bolstering of the authentication process to access that data store.

Upon subsequent investigation, the ICO found a number of deficiencies in the security measures implemented by Uber at the time of the breach. Among other findings, Uber was found not to have adequately

[282] The supervisory authority's decision can be accessed at: <https://ico.org.uk/action-weve-taken/enforcement/uber/> accessed 23 January 2020.

covered the risks presented by the third-party cloud-based storage solution used. This was concluded, in particular, due to Uber not having previously activated two-factor authentication (though this was an available option). Uber employees were also not expressly forbidden from re-using credentials used in Uber's systems, or on other platforms, to access the third-party cloud-based storage solution – this led to the cyberattack, as it was by collecting those re-used credentials from other sources that the attackers were able to obtain access to the accounts of 12 Uber employees.

Decision: The ICO imposed an administrative fine amounting to approximately 444,888.00 EUR upon Uber. This decision considered mitigating factors, such as the lack of evidence that the compromised personal data was actually further used or successful identity theft or fraud activities detected, the overall low sensitivity of the data breached (which did not include location data, payment card data, or dates of birth, for example), and the substantial and prompt remedial action taken by Uber to prevent the recurrence of this type of incident. However, aggravating factors were also considered, such as the lack of a notification of the personal data breach to the ICO (who learned of the breach through reports in the media) and the lack of a communication to the affected data subjects.

Appropriate precautions must be taken by controllers relying on third-party solutions to store personal data. Controllers must carry out a full assessment of potential security risks offered by those solutions and configure them to ensure that those risks are decisively addressed (or, where this is not possible, consider contacting the provider or switching to another provider which offers greater guarantees of data security). Further, a controller's internal policies on security must also be crafted in a manner that aligns with industry standards on security and, overall, avoids unnecessary risks to the integrity of the authorisation rights defined by controllers. This can be achieved, in particular, by forbidding the re-use of user credentials in company systems which are used by employees on other platforms, and by ensuring the implementation of two-factor or multi-factor authentication for access to systems whenever feasible. However, even with state-of-the-art security implemented in an effective manner, no controller is fully safe from the risk of personal data breach. Controllers should therefore bear in mind that, if such a breach occurs, a failure to report it to the competent supervisory authority in a timely manner and – where necessary – to the data subjects affected, will be considered an aggravating factor in the definition of the appropriate corrective measures to be applied.

Hellenic Data Protection Authority ('HDPA') – Greece; 27 December 2018[283]

A personal data breach, in the form of unauthorised disclosure of personal data, occurred at a Greek bank. Financial documents containing personal data were erroneously disclosed to the wrong customers. Upon becoming aware of the breach, the bank took measures to mitigate its impact, including investigating the incident, identifying the root cause of the error, establishing controls and safeguards to prevent recurrence of such errors, and notifying the customers affected (as well as the wrong recipients, who were asked not to disclose the erroneously received information further). However, the bank did not abide by the 72-hour deadline indicated in the GDPR for notification of personal data breaches to the HDPA. The notification was ultimately filed, two days after the deadline had expired, without any justification for the delay.

Decision: Considering the limited impact of the incident (which affected only 12 customers), the measures taken by the bank to address the incident and the fact that the delay in submission of the notification to the HDPA was relatively short, the HDPA considered it appropriate to issue a mere reprimand to the bank.

This case highlights that it is fundamental for controllers to take control of the material impact of a breach. In particular, controllers must implement measures to reduce or eliminate the risks a breach may cause to the rights and freedoms of data subjects. This may include contacting the affected data subjects to notify them of the occurrence when deemed appropriate. It is also important for controllers to ensure that they comply with the formal obligations related to personal data breaches which are imposed upon them by the GDPR. Unless a personal data breach is deemed unlikely to cause any sort of risk to individuals, the breach must be notified to the competent supervisory authority by a controller within 72 hours of becoming aware of it, as a rule, under Art. 33(1) GDPR. Controllers are afforded the possibility to exceed this timeframe, insofar as they are able to demonstrate objective and valid reasons for the delay.[284] In general, however, it is preferable for the control-

[283] The supervisory authority's decision can be accessed at: <https://nymitytools.nymity.com/media/en/22a7a27d-38af-4f4e-9423-a21b4467a8ba.pdf> accessed 23 January 2020 (in Greek).

[284] As noted by the Art. 29 Working Party Data Breach Notification Guidelines, 16: "*Such a scenario might take place where, for example, a controller experiences multiple, similar confidentiality breaches over a short period of time, affecting large numbers of data subjects in the same way. A controller could become aware of a breach and, whilst beginning its investigation, and before notification, detect further similar breaches, which have different causes. Depending on the circumstances, it may take the controller some time to*

ler to notify the supervisory authority in phases, by providing all available and relevant information on the breach (nature of the breach, categories and approximate number of data subjects and personal data records affected, name and contact details of the company's data protection officer or other point of contact, likely consequences of the breach and actual or potential measures taken to address the breach) within the first 72 hours, and updating the notification with additional information as it becomes relevant.

> **Garante per la protezione dei dati personali – Italy; 4 April 2019**[285]
>
> A number of Movimento 5 Stelle (Italian political party) websites were run by means of a data processor, through the Rousseau platform.
>
> In 2017, the Rousseau platform suffered a personal data breach. Upon learning of this, the *Garante* addressed the party and platform, and required the implementation of further security measures, as well as an update to the privacy notice made available on the platform, in order to improve transparency with respect to the data processing activities it carried out. A timeframe for this was provided.
>
> Nonetheless, while the privacy policy was modified in due time, the security measures implemented on the platform were not adequately amended.
>
> **Decision:** The Italian data protection authority imposed an administrative penalty on the Rousseau platform (i.e., the processor) of 50,000.00 EUR for having violated Articles 9, 24, and 32 GDPR.

The Italian data protection authority demonstrates the importance of ensuring that adequate security measures are taken in order to protect the personal data that may include political or philosophical opinions. In the case at hand, because the website was run by an Italian political party, very high standards were expected in order to ensure that this personal data will not be accessed by unauthorised persons. Due to the failure of the website to take adequate measures, the Italian data protection authority issued a fine to the processor.

---

establish the extent of the breaches and, rather than notify each breach individually, the controller instead organises a meaningful notification that represents several very similar breaches, with possible different causes. This could lead to notification to the supervisory authority being delayed by more than 72 hours after the controller first becomes aware of these breaches."

[285] Garante per la protezione dei dati personali, Provvedimento su data breach - 4 aprile 2019 [9101974] (4 April 2019) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9101974> accessed 23 January 2020 (in Italian).

This case is noteworthy in that the supervisory authority did not issue the penalty to the data controller (i.e., the political party), but to the processor (the platform). This shows that processors' liability under the GDPR can also be triggered when it comes to Article 32 GDPR, as processors are also directly required, under that Article, to ensure that they have appropriate security measures in place to secure the personal data they process.

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal – Romania; 1 October 2019[286]

The Romanian DPA fined Raiffeisen Bank SA for violating the provisions of Article 32 GDPR.

The fine was issued following a notification from the bank to the DPA of a security breach. The breach occurred when two Raiffeisen Bank employees used data from the identity documents of a number of individuals (a total of 1,177 persons), transmitted via WhatsApp by Vreau Credit SRL employees, to carry out 1,194 scoring simulations, used to determine the creditworthiness of those individuals. The scoring simulations were carried out using a platform regularly used by Raiffeisen Bank SA in its lending activities. Negative credit decisions were communicated by the Raiffeisen Bank SA employees to the Vreau Credit SRL employees, in violation of the bank's internal procedures.

The Authority fined Raiffeisen Bank SA for its failure to implement appropriate measures to ensure that the employees acting under its authority, and who had access to personal data, would only process personal data under the instructions of their employer. Further, the Authority determined that Raiffeisen Bank SA had not implemented technical and organisational security measures to ensure an adequate level of security for personal data, and had also failed to consider potential risks of connected data processing. These failures allowed unauthorised access to the personal data processed by the platform used by Raiffeisen Bank SA, as well as the unauthorised disclosure of personal data by the bank's employees.

Vreau Credit S.R.L. was also fined by the DPA for violating Article 32(1), (2) and (4), as well as Article 33(1) GDPR. This concerned failures around data security, and a lack of proper and timely notification of this breach to the Authority without undue delay, in spite of the fact that the company was aware of the breach since December of 2018.

---

[286] Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, 'Noi amenzi în aplicarea RGPD' (1 October 2019). <https://www.dataprotection.ro/?page=Comunicat_Presa_09_10_2019&lang=ro> accessed 23 January 2020.

> **Decision:** The Romanian DPA imposed an administrative fine to Raiffeisen Bank SA of 150,000.00 EUR, for violation of Article 32, and to Vreau Credit S.R.L. of 20,000.00 EUR, for violation of Articles 32 and 33 GDPR.

Under Article 5(1)(f) GDPR, principle of security calls for personal data to be securely processed by way of the implementation of appropriate technical and organisational measures. This, in turn, requires organisations to carry out risk analyses, so that they can identify the most relevant risks to the security – confidentiality, integrity and availability – of the personal data they handle. Mitigation measures, in the form of technical and organisational security measures, must then be implemented to address all such risks so as to create an adequate level of security for personal data handled.

Performing proper privacy risk assessments (which necessarily include a security risk analysis component) is a key step in the prevention of personal data breaches, and in the creation of documented evidence that appropriate security measures are in place – in other words, security measures chosen to adequately address identified risks.

However, if a personal data breach occurs, companies must act quickly to report it to the relevant stakeholders. While processors do not have a specific timeframe within the GDPR under which their respective controllers should be notified, they are still required to do so without undue delay, in light of Article 33(2) GDPR. Controllers, on the other hand, have 72 hours from the moment on which they become aware of a breach to notify the competent supervisory authority, unless they are able to determine that the breach is unlikely to cause a relevant risk to data subjects.

> **Autoriteit Persoonsgegevens – The Netherlands; 16 July 2019**[287]
>
> The Dutch Supervisory Authority issued its first fine under the GDPR in July 2019, imposing a fine on the Haga Hospital in the Hague, for careless handling of patient data and insufficient security.
>
> In particular, the Dutch DPA, after an initial investigation, determined that dozens of Hospital employees had been able to access the medical records of a Dutch celebrity being treated at the Hospital, without proper authorisation to do so. This was considered a clear violation of the healthcare provider-patient confidentiality expectations of the

[287] AutoriteitPersoonsgegevens, 'Haga Beboet Voor Onvoldoende interne beveiliging patiëntendossiers' (16 July 2019) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-patiëntendossiers> accessed 23 January 2020 (in Dutch).

celebrity, and also of the requirement under Article 32 GDPR to have appropriate measures in place to ensure data confidentiality.

The Dutch DPA thereby ordered the hospital to improve its security of patient records, namely by (1) regularly checking which individuals were accessing which medical records, so that they would be able to detect and react against unauthorised access to specific data, and (2) implementing two-factor authentication for access to the Hospital's records (eg, by combining a personnel pass with a code or password).

Decision: The Dutch Autoriteit Persoonsgegevens fined the Hospital 460,000.00 EUR for inadequate security measures and ordered the hospital to take necessary measures to rectify their GDPR compliance posture. It further noted that a failure to do so within the set time-frame would lead to the Hospital being fined 100,000.00 EUR every two weeks, up to a maximum of 300,000.00 EUR.

The Authority demonstrated, in this case, that hospitals must take particular care in defining adequate security measures to protect the personal data of their patients. Health data is a special category of personal data under Article 9 GDPR, the processing of which is inherently riskier to the rights, freedoms, and legitimate interests of data subjects; therefore, the level of security applied to health data must naturally be greater than that which would be applied to "regular", non-Article 9 or 10 data, in order to match the increased level of risk.

In particular, access management is key to ensuring confidentiality, as noted in this case. Allowing widespread and unfiltered access to patient records, even if this is contained to the employees of a hospital, is a gross violation of the principle of security, under Article 5 GDPR, but also of the principle of data minimisation (in that personal data is being accessed by more people than necessary) and, potentially, of the principle of purpose limitation (eg, if those unauthorised persons use those data for unauthorised purposes) and storage limitation (eg, if those unauthorised persons create copies of those data, and store them for excessive amounts of time). Without an appropriate system to assign access rights – based on a 'need-to-know' and 'least privilege' principle –, to monitor access to data and to revoke/review access rights as needed, companies will not be able to ensure that personal data remains confidential, to the greatest extent feasible, within their own organisation. This exposes companies to numerous breaches under the GDPR, such as those described above.

Commission for Personal Data Protection – Bulgaria; 29 August 2019[288]

During an audit carried out by the Commission for Personal Data Protection of the Bulgarian National Revenue Agency, it was found that the Agency, as a data controller, had failed to implement appropriate technical and organisational measures to ensure data security.

This resulted in the unauthorised access, disclosure, and dissemination of personal data of various Bulgarian citizens which included names, ID numbers and addresses, telephone numbers, and other contact information, and income and social security declarations, among others.

Decision: The Authority fined the National Revenue Agency 2,600,000.00 EUR, and ordered the Agency to take appropriate technical and organisational measures pursuant to the GDPR to address the situation. Suggested measures included the enhancement of the protection of personal data processing in e-services applications offered to citizens; carrying outrisk analyses of systems and processing operations; carrying out an impact assessment of the identified 'high risk' for each system, of the measures taken and for the initial launch of new information systems and applications.

In this case, the agency had not properly carried out risk assessments for the systems and operations it used. As a result, the security measures it decided to implement were inadequate, and it was not in a position to show that they had been selected to address specifically-identified risks.

The GDPR (in Articles 24 and 32 GDPR) asks of controllers and processes to follow a risk-based approach, through which relevant risks to the rights, freedoms, and legitimate interests of data subjects can be identified, and then properly addressed. Under Article 32, this means that assessments must come before the definition of security measures, so that the measures chosen can be appropriate to mitigate any and all relevant risks. This is particularly relevant when it comes to public authorities and applications/platforms they provide for widespread access by citizens – given that such processing activities are performed in the public interest, may involve large amounts of personal data on large amounts of individuals, and that data subjects

[288] Bulgarian Commission for Personal Data Protection, 'Информация за извършена проверка в Националната агенция за приходите' (29 August 2019) <https://www.cpdp.bg/index.php?p=news_view&aid=1519> accessed 23 January 2020 (in Bulgarian).

are typically under reasonable expectations that their data will be handled securely by national authorities/agencies. These factors particularly should be taken into account to correctly choose security measures to meet those expectations and ensure confidentiality, integrity, and availability of data.

> **Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal – Romania; 4 November 2019**[289]
>
> The Romanian DPA investigated ING Bank NV Amsterdam, following a notification submitted to the Authority. It found that the bank violated the provisions of Article 25(1) and 5 of the GDPR, leading to a fine being imposed.
>
> The Authority determined that the bank had failed to comply with the principle of data protection by design and by default, in that it had not adopted appropriate technical and organisational measures to ensure the security of data, regarding the automated system used to process card transactions. This affected around 225,525 customers, as defects in the security measures implemented led to the doubling of payment operations for those customers during a period of time.
>
> **Decision:** The Romanian DPA imposed an administrative fine of 80,000.00 EUR on ING Bank for violation of Article 32 GDPR.

This case is evidence of the crucial role played by data protection by design and by default, when defining and implementing appropriate security measures. A key step for implementation of data protection by design and by default, for a given processing system, is the performance of a privacy risk assessment – which, in turn, includes a component on analysis of relevant security risks. This assessment, when performed correctly and thoroughly, will allow a company to identify all relevant risks to the rights, freedoms, and legitimate interests of the data subjects concerned, including those related to data security. Based on this, the company can then use a risk-based approach to determine appropriate security measures, with an aim at mitigating those risks to adequate levels, considering all factors laid out in Article 32 GDPR.

---

[289] Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, 'Amendăpentruîncălcarea RGPD' (4 November 2019) <https://www.dataprotection.ro/?page=Amenda_ING_RGPD&lang=ro> accessed 23 January 2020 (in Romanian).

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz – Germany; 3 December 2019[290]

The Data Protection Authority of Rheinland-Pfalz imposed a fine on a hospital for several breaches of the German Basic Data Protection Ordinance, which were revealed after the occurrence of patient mix-ups during admission to the hospital.

These incidents resulted in incorrect invoicing of the patients, revealing structural technical and organisational deficits of the hospital in patient management.

Decision: The Authority imposed a fine of 105,000.00 EUR on the hospital in question for the lack of appropriate organisational and technical security measures in place. The fine was mitigated due to the hospital's efforts, in concert with the Authority, to sustainably develop and improve its data protection management practices.

This case is an interesting look into how Authorities may mitigate fines where the controller/processor shows an effort to fix mistakes pointed out to them by the Authorities. In other words, companies should be aware that a failure to implement appropriate security measures may result in fines, should any personal data breaches occur and come to the attention of an Authority; however, they should also be aware that Authorities are able, under Articles 83(2)(c), (d) and (f) GDPR, to consider several factors which may mitigate the need for sanctioning (and the amount of fines, if the Authority still considers a fine to be needed), such as actions taken to mitigate the damage suffered by data subjects, the degree of responsibility of the controller/processor for the breach (considering measures put in place), and the degree of cooperation shown in order to remedy a breach and mitigate its potential negative impact.

Information Commissioner's Office – United Kingdom; 20 December 2019[291]

The UK DPO fined Doorstep Dispensaree Ltd for failing to adequately secure special category personal data.

---

[290] Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, 'Geldbuße gegen Krankenhausaufgrund von Datenschutz-DefizitenbeimPatientenmanagement' (3 December 2019) <https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/geldbusse-gegen-krankenhaus-aufgrund-von-datenschutz-defiziten-beim-patientenmanagement/> accessed 23 January 2020 (in German).

[291] United Kingdom Information Commissioner's Office, *Doorstep Dispensaree Ltd* (20 December 2019) <https://ico.org.uk/action-weve-taken/enforcement/doorstep-dispensaree-ltd-mpn/> accessed 23 January 2020.

> Doorstep Dispensaree Ltd was a supplier of medicine to both customers and care homes, and "*left approximately 500,000 documents in unlocked containers at the back of its premises*" which included "*names, addresses, dates of birth, NHS numbers, medical information and prescriptions belonging to an unknown number of people*." Further, some of the documents which were dated from June 2016 to June 2018 suffered water damage as a result of being stored on the floor.
>
> The company was fined for "*[f]ailing to process data in a manner that ensures appropriate security against unauthorised or unlawful processing and accidental loss, destruction or damage*".[292]
>
> **Decision:** The ICO penalised Doorstep Dispensaree Ltd 275,000.00 GBP (approximately 322,788.00 EUR) and also issued an enforcement notice due to the significant GDPR violations that it committed. The ICO further required the organisation to improve its data protection stance within three months and that failure to comply with the order could result in further enforcement actions.

In this case, the company failed to accurately evaluate the risks of its practices, and to implement appropriate security measures to protect against those risks. As a result, documents containing special categories of personal data – the processing of which is inherently riskier for data subjects – were exposed to loss and accidental damage (i.e., risks from the availability and integrity perspective).

In particular, to address availability and integrity, the company might have considered retaining these data in a manner which allowed it further protection from physical elements, such as water damage. Having a digital backup of such documents, under restricted conditions of access (to avoid the mere duplication of data without any additional safeguards), is another measure which could have been considered to prevent this.

In hindsight, it is easier to establish what should have been done. Therefore, whenever an incident involving personal data takes place, companies should properly assess the root cause for the incident, and implement appropriate measures to ensure that such incidents will not happen again (or, at least, to reduce the likelihood of this).

---

[292] ibid.

F. Retention of personal data

Datenschutzbehörde – Austria; 15 August 2018[293]

An individual filed a complaint with the Datenschutzbehörde, concerning the data retention practices of a national telecommunications company. The company would retain the individual's master data (data requirement for the establishment, processing, modification, or termination of the relationship between the company and the individual), along with other personal data pertaining to the individual, for a period of 10 years, and would retain traffic data (data used to allow the individual to carry out communications or to process the billing of those communications) for 6 months.

The company claimed that it relied on the national Federal Tax Code in its definition of a retention period for master data. This Code allegedly allowed those data to be stored by telecommunications companies for up to 10 years. However, the Datenschutzbehörde noted that the relevant provisions of the Code require the company to retain data up to the maximum allowed period, and that it would still be up to the company to define an appropriate period of retention, within the maximum framework defined by the Code. It was further noted that the national Telecommunications Act required master data to be deleted at the end of the contractual relationship, with the only exceptions to this arising where further storage is necessary to settle fees, process complaints, or fulfil other legal obligations. The mere abstract possibility that a legal proceeding involving master data might be brought against the company was found to be insufficient to justify its retention for the maximum permissible period.

Further, the national Telecommunications Act allowed for further retention of traffic data, beyond the termination of the contractual relationship, only where necessary for the handling of retail or wholesale charges. Those data should be deleted or anonymised as soon as those charges were paid off and, in any case, no later than three months after their generation. Therefore, the company's six-month retention period for traffic data was found to be excessive, given a

[293] The supervisory authority's decision can be accessed at: <https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=8c5816a9-c852-4cb8-8200-38bec88cad79&Position=1&Abfrage= Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=08.08.2018&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer= DSBT_20180528_DSB_D216_471_0001_DSB_2018_00%20> accessed 23 January 2020 (in German).

lack of a justifiable need for it (as the contract with the individual had been terminated more than three months prior).

Finally, the Datenschutzbehörde found no justification for the continued storage of personal data on the individual which was neither master nor traffic data. This was considered a violation of the principle of storage limitation and data minimisation.

Decision: The Datenschutzbehörde ordered the company to limit the storage of the individual's master data to a period of seven years in order to comply with legal record-keeping obligations within the national Federal Tax Code. The company was further ordered to delete all traffic data and other personal data held on the individual.

Even where local legislation allows (but does not expressly require) the retention of personal data for a given period, companies are still responsible for defining retention periods which are adequate in light of the purposes for which those data are processed. Where continued storage of personal data is no longer strictly necessary for the purposes which motivated the collection or processing of those data, the controller should only further store those data if this is strictly required by law. Controllers wishing to further retain personal data, for example, to address potential legal claims, should take note of this decision, which suggests that only a concrete pending or active claim will allow such further retention. Where controllers decide that it is important to retain those data further, they do so on the basis of their own legitimate interests, which requires an assessment to ensure and demonstrate that the rights of individuals do not override those interests. To favour this conclusion, it is recommended, in particular, that those data are segregated from other data in use by the controller and placed under restricted conditions of access and use, so that they may only be processed in the eventuality of the need to address a relevant legal claim (and for no other purposes) until they are ultimately deleted or anonymised.

G. Geolocation tracking

Garante per la protezionedeidatipersonali ("Garante") – Italy; 15 August 2018[294]

An employee filed a complaint with the *Garante* against their company. The employee claimed that the company had installed a GPS tracking device on company vehicles without giving prior notice of

[294] The supervisory authority's decision can be accessed at: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9023246> accessed 23 January 2020 (in Italian).

this to employees. These devices supposedly continued to monitor the location of those vehicles even outside of working hours.

After investigation, the *Garante* concluded that the geolocation monitoring practices of the company were unlawful, under both the GDPR and the Italian Personal Data Protection Code. The company had stated that such devices were implemented for logistic and organisational purposes (namely, to allow the company to more efficiently allocate resources to customer sites in need of assistance, to guarantee the safety and security of the vehicles, and to prevent and react to criminal acts affecting the company's assets). The *Garante* noted, however, that the GPS tracking device collected an excessive amount of information on the vehicle's usage (including speed, position, hours of engagement and driving, break hours, and average speed), feeding such information to the company every 120 seconds. This information was considered to amount to personal data on the company's employees, given that the limited number of vehicles, each intended to carry out specific services, allowed the specific employee to whom a vehicle had been assigned to be identified. Among other conclusions, it was noted as relevant that the company had deactivated the possibility for the devices to be turned off during allowed breaks.

The *Garante* further noted that employees had not been provided all relevant information related to the processing of their data via these devices, as required by Art. 13 GDPR. Furthermore, the fact that the company retained tracking data for a period of one year was deemed excessive in relation to the purposes for which the devices were installed. This was found to be in breach of the principles of necessity and proportionality, allowing the company to continuously and unlawfully monitor the activities of its employees.

Decision: The *Garante* ordered the company to immediately cease processing all data collected and retained via these tracking devices. The *Garante* further issued orders to the third-party provider of the tracking devices, requiring the provider to inform its customers (including the company) of the possibility to modify the tracking devices so as to allow their temporary deactivation (for example, during allowed breaks or outside of working hours). The provider was also required to inform its customers that they should ensure that these devices were configured in a manner which properly considered all relevant data protection principles, including by revising the frequency with which data were collected by the devices and the data retention periods implemented.

Controllers should ensure that they correctly identify a legal basis allowing them to implement geolocation tracking devices concerning their employees. Considering that the consent of employees is unlikely to be considered freely given (which is one of the necessary requirement for consent to be valid) in this scenario, this will require the completion of a legitimate interests assessment and the definition of appropriate safeguards to protect the rights of employees. Relevant safeguards in this context include the preparation of complete and understandable information notices, as well as ensuring that the devices do not collect unnecessary or excessive data. Collection of data via geolocation tracking devices should be done at an appropriate, not overly short frequency. It should be possible for employees to turn devices off outside of working hours or during breaks. Controllers are also strongly recommended to carry out and document a complete DPIA under Art. 35 GDPR. In fact, it is common to see location tracking activities identified within supervisory authorities' 'DPIA blacklists', issued under Art. 35(4) GDPR.

H. Data subject rights

Datenschutzbehörde – Austria; 11 September 2018[295]

An individual requested deletion of his personal data from the databases of a national creditor protection association. The association complied in part: they informed the individual that certain categories of data, such as his name, date of birth, and address, would need to be further retained for documentation and communication purposes. The individual subsequently insisted upon the full deletion of his data, which the association refused.

Upon receiving a complaint from the individual, the Datenschutzbehörde investigated the matter and asked the association for its arguments supporting the refusal. The association merely stated that the need for continued storage of those data was necessary for well-known reasons. The Datenschutzbehörde was not satisfied with the reasoning provided by the association. They found that the association had not provided sufficient evidence of a lawful need to continue storing those data. It was also noted that indefinite storage of personal data, to address the possibility that an individual may need to be contacted

[295] The supervisory authority's decision can be accessed at: <https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=8c5816a9-c852-4cb8-8200-38bec88cad79&Position=1&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=08.08.2018&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20180528_DSB_D216_580_0002_DSB_2018_00> accessed 23 January 2020 (in German).

again in the future, is unlawful under the GDPR, amounting to a violation of the principle of storage limitation.

Decision: The Datenschutzbehörde ordered the association to delete all of the individual's personal data within the span of two weeks and to inform the individual once this had been completed.

Overly extensive or indefinite retention is not acceptable under the GDPR. This is true even if such retention is done for purposes which, at first glance, appear legitimate (such as the possibility that a controller might need to contact the individual once more in the future). Unless there is a concrete, actual, and demonstrable need on the part of a controller to store personal data (rather than an abstract or eventual need), the controller will generally not be able to justify continued storage of those data and should proactively delete or anonymise them at that stage.

While the scope of the right to erasure is not overly vast under the GDPR, the situation presented in this case is a clear-cut scenario of its applicability. The continued processing of the personal data in question was not necessary for any actual, lawful purposes, and so the individual was entitled to obtain their erasure from the controller under Art. 17(1)(a) GDPR.

Datatilsynet – Denmark; 12 October 2018[296]

A company operated a website which provided publicly available information (retrieved from the Danish Central Business Register) on the owners, shareholders, and senior persons in Danish companies. This company did not comply with a request for erasure submitted by an individual who sought to delete the information available on that website pertaining to the individual's previous affiliations with a number of companies.

Upon receiving a complaint from the individual, the Datatilsynet investigated the complaint. They found that the company was entitled to refuse to comply with the request. This conclusion was based on the fact that the company was providing information which was already publicly available. In fact, all information available on the company's website was retrieved in real time from the Danish Central Business Register rather than actually stored on the website. This information could already be accessed by any interested individual (through that Register). It was further concluded that the company could justify the

[296] The supervisory authority's decision can be accessed at: <https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2018/aug/klage-over-lasso-x-aps-behandling-af-oplysninger/> accessed 23 January 2020 (in Danish).

processing carried out on the basis of its own legitimate interests (Art. 6(1)(f) GDPR), as well as on the basis of the performance of a task in the public interest (Art. 6(1)(e) GDPR, as it was aggregating publicly available information of relevance regarding important persons within Danish companies). It was further noted that the individual had not presented any special reasons which would justify the deletion of the individual's data from the website, which could outweigh the interests pursued by the company.

Decision: In light of the above, the Datatilsynet decided to dismiss the complaint.

This case illustrates the limitations of the right to erasure. Data subjects are not automatically entitled to the erasure of their personal data. Instead, they may only rely on it when they are able to invoke any of the requirements for its applicability, under Art. 17(1) GDPR. Where personal data are processed by a controller on the basis of the legitimate interests of the controller (or others), or on the basis of the performance of a task in the public interest, a request for erasure will only be valid if:

- Those data are not actually necessary for the purposes pursued by the controller (Art. 17(1)(a) GDPR);
- They have been unlawfully collected or processed (Art. 17(1)(d) GDPR);
- A legal obligation to erase those data exists (Art. 17(1)(e) GDPR); or
- The data subject is able to validly object to their processing, by presenting specific reasoning pertaining to his/her situation, which must be considered as more important than (overriding) the interests for which the controller seeks to process those data (Art. 17(1)(c) and Art. 21(1) GDPR).

Datenschutzbehörde – Austria; 15 November 2018[297]

An individual filed a request for a copy of his bank statements over the five preceding years with a bank. The bank advised the individual that the provision of this information would be subject to a charge of 30.00 EUR per year of documents. Upon receiving this response, the individual filed a complaint with the Datenschutzbehörde.

The Datenschutzbehörde requested that the bank comply with the individual's request. The bank replied that it felt it appropriate to

[297] The supervisory authority's decision can be accessed at: <https://noyb.eu/wp-content/uploads/2018/06/dsb_dsgvo_auskunft.pdf> accessed 23 January 2020 (in German).

> charge the fee stated to the individual as compliance would require a significant amount of effort on the bank's part (as it was unable to electronically query some of the requested bank statements). The bank quoted, among other legal provisions, Art. 12(5) GDPR on this, stating that the charging of access fees was not forbidden under the GDPR, and was further permitted due to the nature of the request made by the individual, which allegedly amounted to harassment.
>
> However, the Datenschutzbehörde noted that Art. 15(3) GDPR requires controllers to provide a copy of a data subject's personal data to the data subject free of charge. Where this may require a substantial amount of effort on the part of a controller, the controller may extend the general one-month period for response under Art. 12(3) GDPR, but must explain and justify this to the data subject. Further, the right to charge a fee for response arises only concerning requests which are manifestly unfounded or excessive. The Datenschutzbehörde did not consider this to be the case here, as it was the first time the individual had requested a copy of this information, the request referred to specific data and there was no other means by which the individual could access those data. The fact that the request had been made in terms which the bank found to amount to harassment did not trigger the bank's right to charge a fee for response under Art. 12(5) GDPR.
>
> **Decision:** The Datenschutzbehörde ordered the bank to provide a copy of the information requested to the data subject within two weeks.

As a rule, all data subject requests must be addressed free of charge to the data subject. The scope of application of the possibility to charge an administrative fee, under Art. 12(5), appears to be quite limited. In any case, controllers will be responsible for demonstrating the 'manifestly unfounded or excessive' nature of the request, and may be ordered to comply where a supervisory authority disagrees. It will be more difficult to claim that a request is unfounded or excessive where it has not been made in a repetitive fashion and asks for specific actions to be carried out (as opposed to sweeping, general requests for copies of all personal data handled by the controller, for example). In any case, before deciding to charge fees, controllers are recommended to ask data subjects for clarification on their request or to narrow their requests for access down to specific types of data or documents. Additionally, the fact that responding to a request will require substantial effort is not, in itself, a justification for the charging of a fee, though it may allow the controller to extend the period of response by up to two additional months.

Agencia Española de Protección de Datos ("AEPD") – Spain; 5 February 2019[298]

An individual submitted a request to a non-profit healthcare assistance company for complete access to the individual's medical records and history held by that company. The company responded by providing incomplete information (in particular, some medical documentation was left out, such as the medical report from a doctor who had been consulted by the individual). Following a complaint submitted on this matter, the AEPD carried out an investigation, concluding that the company had failed to provide a legitimate reason for submitting incomplete information to the data subject in response to the request received (in fact, no justification for this was provided).

Decision: The AEPD ordered the company to respond to the data subject within ten days from the order, either providing complete access to the missing personal data or otherwise providing reasons for refusal to comply with the request. It further notified the company that a failure to do so could trigger an administrative fine under Art. 83(5) GDPR.

While companies may be able to avoid responding to a request for access in full by relying on exceptions permitted under the GDPR, such as where necessary to protect the rights and freedoms of others (Art. 15(4) GDPR), it is always necessary to invoke those exceptions when responding to a data subject, providing sufficient reasoning for the applicability of the exception to the particular case. Where this reasoning is absent or not sound, the company will be required to fully provide access to the personal data requested by the data subject.

Datenschutzbehörde – Austria; 21 February 2019[299]

Following the submission of two requests for quotes from a motor insurance company, an individual submitted a request for erasure to that company, asking that all of his personal data be excluded from their databases. In response, the company deleted a portion of those personal data and anonymised the remainder. Considering that this was not an effective means of compliance with his right of erasure, the

[298] The supervisory authority's decision can be accessed at: <https://www.aepd.es/resoluciones/TD-01341-2018_ORI.pdf> accessed 23 January 2020 (in Spanish).

[299] The supervisory authority's decision can be accessed at: <https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.html> accessed 23 January 2020 (in German).

individual submitted a complaint to the Datenschutzbehörde, which launched an investigation into the occurrence.

During the investigation, it was noted that the company had kept a record of the cancellation of the quote requests made, deleted all contact details pertaining to the individual from its systems, de-identified the remaining data held on the individual (by overwriting it with a dummy customer's data) and ensuring that such data could not be re-identified. Further, while the investigation was ongoing, the company proceeded to destroy all data held on the individual (without leaving behind any anonymous data) and remove all identifiable references to the individual. The Datenschutzbehörde found that the company had effectively ensured that re-identification of the individual was not possible without disproportionate effort, which amounted to ensuring that the information held (prior to its full destruction) did not relate to an identifiable individual.

Decision: The Datenschutzbehörde dismissed the complaint, finding that the request had been appropriately addressed.

Other than simply deleting personal data held, controllers may also consider anonymizing personal data in order to respond to a valid request for erasure from a data subject. In order for personal data to be fully anonymised, such that it ceases to be considered 'personal data', the controller must ensure that the individual to which the data relates is no longer identifiable, taking into account all the means reasonably likely to be used, such as singling out, by any person to identify that individual, whether directly or indirectly (Recital 26 GDPR). The bar for anonymisation is set very high by the Article 29 Working Party.[300] Controllers must, therefore, be cautious when deciding to de-identify personal data, rather than merely deleting it. Another effective manner of anonymising personal data is by aggregating those personal data with data collected on other data subjects, such that the result is no longer assignable to any given individual. This can be an effective means to continue drawing relevant information (for statistical or research purposes, for example) without further retention of data in an identifiable form.

Hungarian National Authority for Data Protection and Freedom of Information ('NAIH') – Hungary; 1 April 2019[301]

An individual submitted a request to a company, asking for access to personal data stored by that company related to him and for deletion

[300] *See*, Art. 29 Working Party Opinion 05/2014.

[301] The supervisory authority's decision can be accessed at: <http://www.naih.hu/files/NAIH-2019-1841_hatarozat.pdf> accessed 23 January 2020 (in Hungarian).

of personal data processed concerning him. The company responded by asking the individual to provide his birth date in order to validate his identity as a data subject. As the individual did not comply, the company closed the request for access. While the company did delete the requested personal data from its main systems, it informed the individual that it would retain those data in its backup systems, and that it was required to retain those data for a period of up to eight years due to legal obligations and its internal data management policies.

During its investigation as a result of a complaint submitted by the individual, the NAIH noted that the individual's date of birth would not have been an appropriate means for authenticating the individual as a data subject, given that the company did not previously have that information in its records. The NAIH understood that the company had made this additional information request due to its internal policies. It therefore noted that any requests for additional information to respond to a data subject request must be made on a case-by-case basis, asking only for that information which is strictly necessary to reasonably identify the individual (if any). The NAIH further noted that the company had closed the individual's request for access without informing the individual that he could resubmit such a request to the company if so desired. However, the NAIH also concluded that the company had appropriately responded to the request for deletion, by eliminating the personal data in question from its main systems within 30 days of receipt of the request and complying with legal retention obligations imposed concerning those data (which, however, were of five years, and not of eight years, as claimed by the company).

Decision: The NAIH imposed an administrative fine amounting to approximately 1,550.00 EUR upon the company, due to an inappropriate handling of the individual's request for access.

Controllers must take reasonable steps to verify the identity of an individual submitting a request for access to personal data, particularly to avoid disclosing personal data to an unauthorised person (which would result in a potentially serious personal data breach). However, these steps must be reasonable and actually necessary in the specific case. A blanket requirement for individuals to provide, eg, dates of birth or copies of national identity documents may not be appropriate in each individual case. For example, the manner in which the request is made or the information provided by the data subject may already be sufficient to allow the data subject to be identified. In particular, companies should not refuse to comply with access requests

where it is objectively and reasonably possible to identify the individual as a data subject.

Datenschutzbehörde – Austria; 28 March 2019[302]

A doctor requested the deletion of his personal data from a website which operated as a search and review portal for doctors in Austria. This portal listed information on those doctors, such as their name, professional contact details, and feedback received from patients. Upon a refusal on the part of the portal operator, the doctor referred the case to the Datenschutzbehörde, which launched an investigation.

During this investigation, the Datenschutzbehörde noted that the portal allowed doctors and physicians to present themselves and receive feedback from their patients. The portal also allowed them to respond to this feedback, flag/report any inaccurate or inappropriate remarks and comment on testimonials made. The publication of patient feedback and evaluation was considered by the Datenschutzbehörde as legitimate under Art. 6(1)(f) GDPR, in that it sought to protect the legitimate interests of other patients which may wish to seek the services of listed doctors or physicians. It further concluded that those patients' fundamental rights and freedoms could be affected if this feedback was deleted from the portal. The conclusion was that the right to erasure, under Art. 17 GDPR, could not be applied in this specific case, given that the portal operator was able to demonstrate overriding legitimate grounds to those which the data subject could invoke to justify that the processing of his personal data be stopped.

Decision: The Datenschutzbehörde dismissed the complaint.

Whenever a request for erasure can only be considered under Art. 17(1)(c) GDPR, because the other cases of Art. 17(1) GDPR do not apply, controllers are essentially asked to first consider this request as tantamount to an objection on the part of the data subject. This requires controllers to assess the particular grounds which the requester may present as justifying deletion of the personal data, and then contrast those with the interests pursued by the controller in processing those data. Where the controller is able to identify

[302] The supervisory authority's decision can be accessed at: <https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=3aa2b2eb-31e8-4a52-9071-08491287dcba&Position=1&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=04.03.2019&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20190115_DSB_D123_527_0004_DSB_2018_00> accessed 23 January 2020 (in German).

compelling interests, which override those presented by the data subject, it will not be required to comply with the request for erasure. Instead, the data subject should be informed of the reasoning behind this and of the remedies available to the data subject (such as the possibility to file a complaint with the competent supervisory authority) under Art. 12(4) GDPR.

Hungarian National Authority for Data Protection and Freedom of Information ("NAIH") – Hungary; 5 April 2019[303]

An individual complained to the NAIH that they were receiving multiple text messages from a bank regarding a loan which did not relate to them. The individual further stated that the bank had not stopped sending those messages in spite of multiple rectification requests made by the individual.

During the course of its subsequent investigation, the NAIH concluded that the bank had failed to maintain the accuracy of the personal data records it kept. It further concluded that the bank should have stopped using the phone number pertaining to the individual once its accuracy had been contested by the individual (namely, once the individual notified the bank that the loan did not relate to him). While this did not require the bank to erase that phone number, it was required to temporarily restrict the processing of that number while it assessed its accuracy. However, the NAIH conceded that, while the principle of accuracy requires effort from the bank, as controller, to ensure that their records are kept up-to-date, this cannot be achieved without collaboration from the data subjects. Therefore, considering that the bank had subsequently sent a letter to the correct customer in order to validate their phone number, the NAIH stated that that customer should have responded to the letter.

Decision: The NAIH imposed an administrative fine amounting to approximately 1,560.00 EUR upon the company. As factors justifying the fine imposed, the NAIH considered the company's annual income, the nature of the infringement (which concerned a violation of the principle of accuracy and a failure to facilitate the exercise of the right to rectification), the repeated misuse of an inaccurate phone number by the bank, the lack of response from the correct data subject to the attempt to validate his phone number (which was seen as a mitigating factor) and the bank's cooperation during the investigations.

[303] The supervisory authority's decision can be accessed at: <http://www.naih.hu/files/NAIH-2019_363_hatarozat.pdf> accessed 23 January 2020 (in Hungarian).

Unsolicited communications are frequently a cause of frustration and annoyance for recipients, which often leads to the triggering of data subject requests (typically for rectification, erasure, or objection) or, in more serious instances, complaints to supervisory authorities. When met with a request for rectification, controllers should proactively restrict the use of personal data which has had their accuracy contested (as a matter of best practice, even where this is not specifically requested by the data subject) until they are able to establish whether or not the data are accurate. This will also help to prevent situations where the controller continues to process inaccurate personal data, in violation of the principle of accuracy. It is also relevant to note that controllers are not exclusively responsible for compliance with the principle of accuracy – this responsibility is mitigated where data subjects do not cooperate to confirm or update their personal data. Controllers must still show that they have implemented reasonable measures to ensure that those data remain up-to-date (such as by reaching out to data subjects to confirm the accuracy of their data, periodically and whenever that accuracy is contested).

> **Agencia Española de Protección de Datos ("AEPD") – Spain; 14 March 2019**[304]
>
> An individual made a request to exercise the right of access to a hospital, requesting that the hospital provide a copy of the individual's medical records. In response, the hospital claimed that the records were available to be picked up at the hospital's premises and that they could not be sent to the data subject by mail or e-mail due to their sensitive nature. Unsatisfied, the individual filed a complaint with the AEPD.
>
> During the subsequent investigation, the AEPD noted that the individual in question resided in a community located far from the hospital's premises, which made it considerably difficult to pick up the medical records on-site. While the AEPD appreciated the concerns raised by the hospital, it noted that, as a controller, it is required, under Art. 12(2) GDPR, to take steps to facilitate the exercise of data subject rights, including the right of access. In practice, the hospital's refusal to share the records with the individual via mail or e-mail had the opposite effect, increasing the difficulty for the individual to exercise their rights.
>
> **Decision:** The AEPD ordered the hospital to send the records to the individual via mail or e-mail, as requested by the individual.

[304] The supervisory authority's decision can be accessed at: <https://www.aepd.es/resoluciones/TD-01346-2018_ORI.pdf> accessed 23 January 2020 (in Spanish).

It is arguable that the hospital's position in this case would have been defensible, if not for the fact that the particular circumstances of the individual in question made it difficult for the individual to gain access to the records at the hospital's premises. In any case, other alternatives could have been explored, such as the sharing of those records in an encrypted format (with the decryption key shared in a subsequent e-mail, reducing the risk of a harmful interception of the personal data, as they would be rendered unintelligible to any unauthorised third parties unless both e-mails were intercepted). The key takeaway is that controllers are simultaneously required to ensure the security of the personal data handled and to facilitate the exercise of valid requests made by data subjects, which sometimes can result in conundrums, such as that presented in this case.

I. Engagement of processors

Data Protection Authority of Hamburg – Germany; 29 January 2019[305]

A German controller engaged a processor in Spain to handle personal data on its behalf. However, in spite of multiple requests made by the controller to enter into a contract regulating the processing of personal data with the processor, no response from the processor was received. The controller turned to the supervisory authority of Hamburg for advice, to which the authority informed the controller that it was responsible for drafting a compliant data processing agreement and providing it to the processor for signature.

The controller maintained that it should not be required to draft this agreement and that the responsibility for this should be on the processor, given that the controller had no knowledge of the processor's internal processes for the handling of personal data and the costs involved in translating the document into Spanish. In response, the authority concluded that the controller was acting in violation of its obligations under Art. 28 GDPR, in that it was allowing the processing of personal data on its behalf by a processor not bound to a compliant data processing agreement.

Decision: The Data Protection Authority of Hamburg imposed an administrative fine amounting to 5,000.00 EUR upon the controller, considering as aggravating factors that the controller deliberately acted in contravention to its obligations under the GDPR and had

[305] Datenschutzbeauftrager, "BeiAufsichtsbehördeangefragt – Bußgeldkassiert!" (21 January 2019) <https://www.datenschutzbeauftragter-info.de/bei-aufsichtsbehoerde-angefragt-bussgeld-kassiert/> accessed 23 January 2020 (in German).

failed to appropriately cooperate with the Data Protection Authority on the matter, instead trying to exclude itself from responsibility for the completion of a data processing agreement with the processor.

Controllers must be sure to have a structured and ongoing approach to obtaining signed personal data processing agreements from all of the processors they engage to provide services on their behalf. This is because controllers are primarily responsible for having such agreements in place. Although it is impossible to unilaterally establish a signed agreement with an unresponsive processor, controllers should at minimum ensure that they have sent out a proposed compliant data processing agreement to the processors which they have currently engaged. Ultimately, controllers must consider terminating the engagement of processors that do not enter into data processing agreements with them, as continuing to allow such processors to handle personal data on behalf of the controller exposes the controller to liability for administrative fines as a result of the breach of its obligations under Art. 28 GDPR.

J. Automated individual decision-making

Office of the Data Protection Ombudsman ('Ombudsman') – Finland; 10 April 2019[306]

The Ombudsman decided to launch an investigation into a credit institution, following receipt of a complaint. The complaint stated that the institution did not provide sufficient notice to data subjects about the use of personal data in the context of automated decision-making. In the course of this investigation, the Ombudsman concluded that the credit institution could justify reliance on automated individual decision-making under Art. 22(2)(a) GDPR, given that it had sufficiently established this to be necessary for the conclusion of agreements with credit applicants. However, it had failed to comply with the principle of data minimisation. This was because it collected the applicant's age in connection with this processing (which was forbidden by local law, given that it is considered that the age of an applicant does not reflect upon that applicant's ability or willingness to meet their financial commitments). The Ombudsman further concluded that the credit institution had not sufficiently informed data subjects as to the logic behind the automated individual decision-making process, the consequences

[306] The supervisory authority's decision can be accessed at: <https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuojavaltuutettu-maarasi-svea-ekonomin-korjaamaan-kaytantojaan-henkilotietojen-kasittelyssa> accessed 23 January 2020 (in Finnish).

which could result from decisions made and the relevance of the data provided by individuals for those decisions.

Decision: The Ombudsman ordered the credit institution to stop collecting applicants' age in connection with these decisions, to update its data protection notices in order to provide meaningful information on the automated individual decision-making process (under Art. 13(2)(f) GDPR) and to notify the Ombudsman of the changes made within a fixed deadline.

Even where a controller is able to identify an appropriate legal basis and applicable derogation for the use of automated individual decision-making under Arts. 6 and 22 GDPR, this does not exempt that controller from continuing to comply with all other data protection principles. Personal data collected in this context should be limited to those which are adequate, relevant and necessary for the purposes for which the decisions are made. Data subjects should be fully and meaningfully informed as to the way that the automated individual decision-making process works. This should include an explanation of the types of data used and their relevance, the way in which those data will influence the final decision (without providing an overly technical explanation or compromising proprietary aspects of the algorithms used) and the possible outcomes of the process for data subjects.

K. Unsolicited marketing communications

Information Commissioner's Office ('ICO') – United Kingdom; 10 December 2018[307]

Following several reports submitted by individuals regarding the sending of unsolicited direct marketing messages by text message, the ICO initiated an investigation into the practices of a company thought to have instigated the sending of those messages. The company informed the ICO that, in connection with those marketing messages, it did not actually purchase or access any personal data on the recipients, obtain their consent, or engage in the actual sending of messages. Instead, they had tasked a service provider to collect contact details and send marketing messages on their behalf, to individuals which had purportedly opted-in to this. However, upon analysis of the privacy policies and information notices available on the websites through which this consent was said to be collected, the ICO considered that their wording was not sufficiently clear or precise. This prevented individuals

[307] The supervisory authority's decision can be accessed at: <https://ico.org.uk/media/2553957/tax-returned-limited-mpn-20181210.pdf> accessed 23 January 2020.

from being properly informed that they would receive marketing messages relating to the company. In particular, those policies and notices often did not identify the company or the service provider as recipients of the personal data collected. As such, the ICO considered that the marketing messages in question had been sent to individuals on behalf of the company in the absence of valid consent or any legal basis for currying out such data processing activity. This was found to be a violation of the UK Privacy and Electronic Communications (EC Directive) Regulations 2003 ('**PECR**'), which concerns the local implementation of the ePrivacy Directive in the UK – particularly, of the provisions of PECR governing the sending of unsolicited communications by means of electronic mail. In this case, given the *lex specialis* status of the ePrivacy Directive (and its local implementation laws) in relation to the Data Protection Directive, regarding the processing of personal data and the protection of privacy in the electronic communications sector, PECR was given focus.

Decision: The ICO imposed an administrative fine amounting to approximately 231,110.00 EUR upon the company.

Companies wishing to send direct marketing messages to individuals must ensure that they have an appropriate legal basis for this, such as consent. Those companies must also guarantee that the requirements for valid consent are met in the specific case (in particular, that at the moment when consent was provided, data subjects were sufficiently informed that their personal data would be used for the specific purpose of sending marketing communications related to the company). Companies will not be exempted from this requirement even if they do not participate in the marketing activities or associated data collection/processing activities themselves, but instead task another entity to carry these out on their behalf.

VII. Conclusions and Recommendations

This article has sought to present a model to implement a comprehensive framework to address the GDPR's data protection principles and requirements which can be followed by controllers and processors alike.

Each of the six steps comprising the Data Protection Compliance Framework is of equal importance. All steps are interconnected. The development and implementation of this framework is a cyclical process, in which activities developed to comply with one step further the activities to be performed for all others. It is a live, dynamic framework, which must be subjected to a process of continuous review and improvement in order to ensure

its continued alignment with changes to the controller/processor's processing practices, available technologies, developments in the applicable law, or the interpretations laid down by supervisory authorities, and any other material and substantive factors which can affect the risk assessments upon which the framework is based.

By understanding the scope of each of the GDPR's data protection principles, controllers will be able to take concrete steps to not only comply with those principles, but also to generate evidence regarding the manner in which this compliance is achieved. This will allow controllers to aim to meet the goals set by the principle of accountability. In turn, this ties into the requirement to ensure that those principles are incorporated into all of the controller's processing practices, systems, products, and services from the design phase and throughout their lifecycle, in alignment with the concepts of data protection by design and by default. As a means to achieve this in practice, controllers will need to assess the risks represented by each of their individual processing activities to the fundamental rights and freedoms of the data subjects concerned. Such assessments will not only allow controllers to ensure that those rights and freedoms are fully respected (in particular, by reflecting the data protection principles within all activities assessed), but also to identify and mitigate relevant risks, through the selection of appropriate technical and organisational security measures. Where mandatory or relevant, more detailed data protection impact assessments can be performed. These steps will allow the controller to adjust its internal processes in alignment with the data protection principles. This will be further complemented by the development of open and transparent means to communicate relevant information about those processes to the relevant data subjects. In tandem, and as a necessary requirement to ensure the lawfulness of all of the controller's activities, the legal bases and derogations offered by the GDPR must be understood in terms of their scope and additional requirements. This will allow controllers to select the most appropriate requirements for each of their processing purposes and to effectively communicate those legal bases to data subjects. The sixth step ties the remaining steps back to the principle of accountability, by requiring the controller to remain true to the information provided to data subjects regarding its practices. It further requires controllers to afford data subjects effective means by which they may exercise their rights under the GDPR, in order to allow data subjects to be fully empowered and able to control how their personal data is used.

Having completed all six steps of the development and implementation of a Data Protection Compliance Framework, controllers will be in a position to test the effectiveness of the measures put in place, by running simulations

– for example, controllers may test their ability to respond to each of the different rights afforded to data subjects under the GDPR, by simulating varied requests made by fictional data subjects. Controllers may also test their ability to detect, investigate, analyse, notify, and document a fictional data breach within the 72-hour deadline afforded to them by the GDPR (while also testing the security measures put in place to prevent those breaches from occurring in the first place). These exercises are a secure manner for controllers to understand whether any gaps exist in their internal procedures and to promptly address them, without jeopardising the rights and interests of data subjects. They may turn out to be instrumental in avoiding heavy sanctions from competent authorities – consider the numerous cases triggered by complaints filed by data subjects as a result of mismanagement of a request (Section 6.1.6. above) or triggered by ineffective data breach notification procedures or deficient security measures (Section 6.1.3 above) – or claims brought by data subjects seeking compensation for damages suffered as a result of an infringement of the GDPR[308].

While ensuring respect for the fundamental rights and freedoms of data subjects is an honourable cause in itself, controllers and processors will be further incentivised to follow a structured approach to data protection compliance in order to reduce the likelihood of being the target of investigative and corrective measures imposed by supervisory authorities (including administrative fines). This article has sought to call further attention to the importance of implementing correct internal procedures to address the principles of data protection, by providing an understanding as to the scope and breadth of these powers. This was sought through an analysis of the corresponding legal provisions and relevant decisions in which they have been practically applied. In particular, the cases analysed allow us to maintain that the development and implementation of an adequate Data Protection Compliance Framework is an unavoidable step for controllers and processors seeking to ensure their compliance and, therefore, avoid financial penalties under the GDPR:

- Proper completion of Step 2 will require controllers to carefully assess how each of the data protection principles is reflected in all of the processing activities they carry out, from the design stage and throughout the lifecycle of those activities. Under the principle of storage

[308] See GDPR, art 78. The possibility for data subjects to band together and seek compensation through class actions against controllers or processors, as set out in GDPR, art 80, may create a situation where even minimal damages caused to an individual data subject may, when aggregated with a sufficient number of other affected individuals, result in substantial liability for a controller or processor found responsible for those damages by a court of law.

limitation, for example, controllers will need to identify maximum storage periods for all categories of personal data handled, based on objective criteria tied to the need for continued processing of those data under defined legal bases. They will also need to ensure that procedures to ensure appropriate deletion or anonymisation of those data after those periods are completed exist – thereby avoiding claims of inadequate retention of personal data,[309] such as the case reported in Section 6.1.4, above.

- Step 3, in particular, will force controllers and processors to take an in-depth look at the context in which their processing activities are carried out (including the first- and third-party tools and systems used to execute them). This will require the performance of comprehensive assessments of the risks involved for the data subjects, and the choosing of security measures which are thought to be objectively appropriate to address those risks and ensure compliance with all data protection principles (not least of which, the principles of data minimisation and storage limitation).This will also involve assessing any processors engaged by the controller to perform those processing activities on its behalf, from the material perspective (whether they provide sufficient assurances of compliance) and formal perspective (by binding them to a data processing agreement containing the minimum obligations laid down in Art. 28 GDPR). Controllers will be enabled to identify processing activities of a higher risk to data subjects, and thereafter carry out complete data protection impact assessments covering those activities, to tackle the risks detected by technical and organisational measures which allow their mitigation to a satisfactory degree. Further, it will require controllers and processors to ensure that internal rules are established to effectively manage any security incidents affecting personal data which may be detected within their organisations. This will reasonably allow damages to data subjects to be prevented or mitigated. Furthermore, the formal rules on notification and communication of personal data breaches must be respected. These activities should allow controllers to avoid claims of deficient security measures in relation to existing risks, as well as of non-compliance with statutory breach reporting obligations

[309] It should also be noted that storing personal data for an excessive amount of time exposes controllers and processors to the possibility of a personal data breach, which is bound to be found more severe if the supervisory authority is able to establish that the controller or processor should already have deleted the personal data affected due to the lack of a justifiable need for their continued processing (as this would potentially have avoided the breach altogether).

or obligations around the engagement of processors, such as those reported in Sections 6.1.3 and 6.1.7, above.

- Successful completion of Step 4 and Step 5 will have allowed controllers to carefully assess how information about their processing activities is communicated to data subjects. In particular, care should be taken to ensure that this is done in a clear, transparent, understandable, easily accessible, and effective manner (even where data is collected indirectly, from other sources). Where consent is leveraged, particular focus on the manner in which it is relied on is recommended – thereby avoiding claims of obscure processing (owed to a lack of transparency) or invalid consent, such as those reported in Sections 6.1.1 and 6.1.9, above.
- Step 6 is focused on understanding the different rights afforded to data subjects and the taking of steps to create internal procedures to allow those rights to take effect in a practical and prompt manner. Controllers will be able to develop methodologies for response to the varied requests which may be received from data subjects, allowing them to comply with their obligations and potentially generating trust and goodwill within the requesters. Given the frequency with which claims are brought against controllers for a failure to properly address a data subject request, this step is of particular importance in avoiding investigations and potential sanctions from competent supervisory authorities, as noted above and illustrated also by the cases reported in Section 6.1.6.
- Particular processing operations, such as the use of video-surveillance, geolocation tracking, or automated individual decision-making, will be tackled from their design stage by successful completion of Step 2. Controllers will be able to ensure that these activities are configured with the data protection principles in mind before they are actually implemented, and that any potential risks to the rights and freedoms of data subjects are promptly identified and mitigated (within Step 3), with full and relevant information provided to the data subjects in question (within Step 4) and an appropriate legal basis identified (within Step 5). This should thereby assure that the controller is able to show that these activities have been planned in order to meet the requirements of the GDPR from a technical and design standpoint, while also avoiding claims of a lack of legal justification for those activities or of a failure to sufficiently inform the data subjects concerned, such as those reported in Sections 6.1.2, 6.1.5 and 6.1.8 above.

- Last but not least, Step 1 (which is at the start and end of the Data Protection Compliance Framework cycle), and the principle of accountability which it seeks to address, imposes upon controllers the obligation to keep evidence of the manner in which it has carried out all of the Data Protection Compliance Framework steps. More generally, controllers must keep evidence of the manner in which they comply with the data protection principles and other requirements under the GDPR. This, in turn, will not only move controllers towards keeping complete records (of processing activities, of processors engaged and data processing agreements signed, of data subject requests, of consent collected, of assessments carried out, of personal data breaches, and so on), but also towards ensuring that their internal policies and procedures are revisited and completed. These internal documents should establish practical actions to be followed by the different teams and departments within an organisation, in order to ensure that the controller is able to balance its regular business operations with the controls to be performed to comply with the GDPR. Maintaining these varied forms of evidence is just as important as actually complying with the rules at play, in order to allow controllers to promptly react to requests for information from data subjects and supervisory authorities. Another important objective of evidence-keeping is to convincingly demonstrate and justify that the methods and practices followed by the controller are compliant (having been designed as such), in the event that this is called into question.

Information About the Journal

The *Indian Journal of Law and Technology* (ISSN 0973-0362) is an academic journal, edited and published annually by students of the National Law School of India University, Bangalore, India. All content carried by the Journal is peer-reviewed except for special comments and editorial notes. The Journal comprises:

- the Board of Advisory Editors, consisting of professionals and academicians pre-eminent in the field of law and technology, which provides strategic guidance to the Journal;
- the Article Review Board, a panel of external peer-reviewers;
- the Editorial Board, consisting of students of the National Law School of India University, which is responsible for selecting and editing all content as well as contributing occasional editorial notes;

OPEN ACCESS POLICY

The *Indian Journal of Law and Technology* is a completely open access academic journal.

- Archives of the journal, including the current issue are available online with full access to abstracts and articles at no cost.
- Please visit the website of the Indian Journal of Law and Technology at "http://www.ijlt.in" to get additional information and to access the archives of previous volumes.

INFORMATION FOR CONTRIBUTORS

The Indian Journal of Law and Technology seeks to publish articles, book reviews, comments and essays on topics relating to the interface of law and technology, particularly those with a developing world perspective.

MODE OF SUBMISSION

Submissions can be in electronic form or in hard copy form. However, submissions in electronic form are strongly encouraged in order to expedite the submission review process. Please address submissions in electronic form to the Chief Editor of the Indian Journal of Law and Technology at "ijltedit@gmail.com".

REGULAR SUBMISSION REVIEW

The Journal shall communicate an acknowledgement to all authors shortly after the receipt of their submissions. The preliminary review of

the submissions shall be completed within four weeks of receipt in usual circumstances. The submissions that are initially accepted shall be blind-refereed by the Article Review Board. The Journal shall make due efforts to complete the entire peer-review process within a reasonable time frame. The Journal shall notify the authors about the exact status of the peer-review process as required.

EXPEDITED SUBMISSION REVIEW

This option is available to those authors who have received an offer of publication from another journal for their submissions. The authors may request an expedited submission review. However, the decision to grant an expedited submission review shall remain at the discretion of the Editorial Board. Please note that requests for an expedited submission review can only be made in relation to submissions in electronic form. All such requests must be accompanied by the following details:

- Name(s) of the author(s) and contact details;
- Title of the submission;
- Details about the journal(s) which has/have offered to publish the submission;
- Whether the offer is conditional or unconditional and, if the offer is conditional, then what conditions are required to be met for final acceptance;
- The date(s) on which the offer(s) expire(s).

The Journal shall make due efforts to accommodate the existing offer(s) and applicable deadline(s). However, upon an oiler of publication pursuant to the expedited submission review, the authors shall have to communicate their decision within five calendar days of the notification or the offer. If there is no response, then the journal shall have the discretion to withdraw the offer.

SUBMISSION REQUIREMENTS

- All submissions must be accompanied by:
  (1) a covering letter mentioning the name(s) of the author(s), the title of the submission and appropriate contact details.
  (2) the résumé(s)/curriculum vitae(s) of the author(s).
  (3) an abstract of not more than 200 words describing the submission.
- All submissions in electronic form should be made in the Microsoft Word file format (.doc or .docx) or in the OpenDocument Text file format (.odt).

- All text and citations must conform to a comprehensive and uniform system of citation. The journal employs footnotes as the method of citation.
- No biographical information or references, including the name(s) of the author(s), affiliation(s) and acknowledgements should be included in the text of the submission, the file name or the document properties. All such information can be provided in the covering letter.
- The Journal encourages the use of gender-neutral language in submissions.
- The Journal shall be edited and published according to the orthographical and grammatical rules of Indian English that is based on British English. Therefore, submissions in American English shall be modified accordingly. The Journal encourages authors to use British English in their submissions in order to expedite the editing process.
- The authors are required to obtain written permission for the use of any copyrighted material in the submission and communicate the same to the Journal. The copyrighted material could include tables, charts, graphs, illustrations, photographs, etc. according to applicable laws.

COPYRIGHT

DISCLAIMER

PERMISSIONS

ORDERING COPIES

Price Subscription (inclusive of shipping) of the IJLT is as follows:

Hard Copy for 2019	Rs. 900
Hard Copy for 2018	Rs. 900
Hard Copy for 2017	Rs. 900
Hard Copy for 2016	Rs. 800

Order online: www.ebcwebstore.com

Order by post: send a cheque/draft of the requisite amount in favour of 'Eastern Book Company' payable at Lucknow, to:

Eastern Book Company,

34, Lalbagh, Lucknow-226001, India

Tel.: +91 9935096000, +91 522 4033600 (30 lines)