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 103
II. Topic, Approach and Methodology 107
III. Structure and arguments 109
IV. The Six Steps of a Data Protection Compliance Framework 110
A. Step 1: Accountability 113
B. Step 2: Data protection by design and by default 118
C. Step 3: Risk Assessments, Data Protection Impact Assessments and Security . . . 122
D. Step 4: Information to the data subject 143
E. Step5: Legitimate basis 151
F. Step 6: Data Subject Rights . . 167
V. Enforcement of the General Data Protection Regulation 188
A. Powers granted to supervisory authorities 188
B. Administrative fines 190
VI. Decisions rendered by supervisory authorities on the monitoring and enforcement of the GDPR 197
A. Inadequate provision of information to data subjects and requirements for valid consent 198
B. Legal Bases 212
C. Video-surveillance 219
D. Data Protection by Design and by Default; Data Protection Impact Assessments 221
E. Security of processing and personal data breaches 225
F. Retention of personal data . . 238
G. Geolocation tracking 239
H. Data subject rights 241
I. Engagement of processors . . . 251
J. Automated individual decision-making 252
K. Unsolicited marketing communications 253
VII. Conclusions and Recommendations 254

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**'.

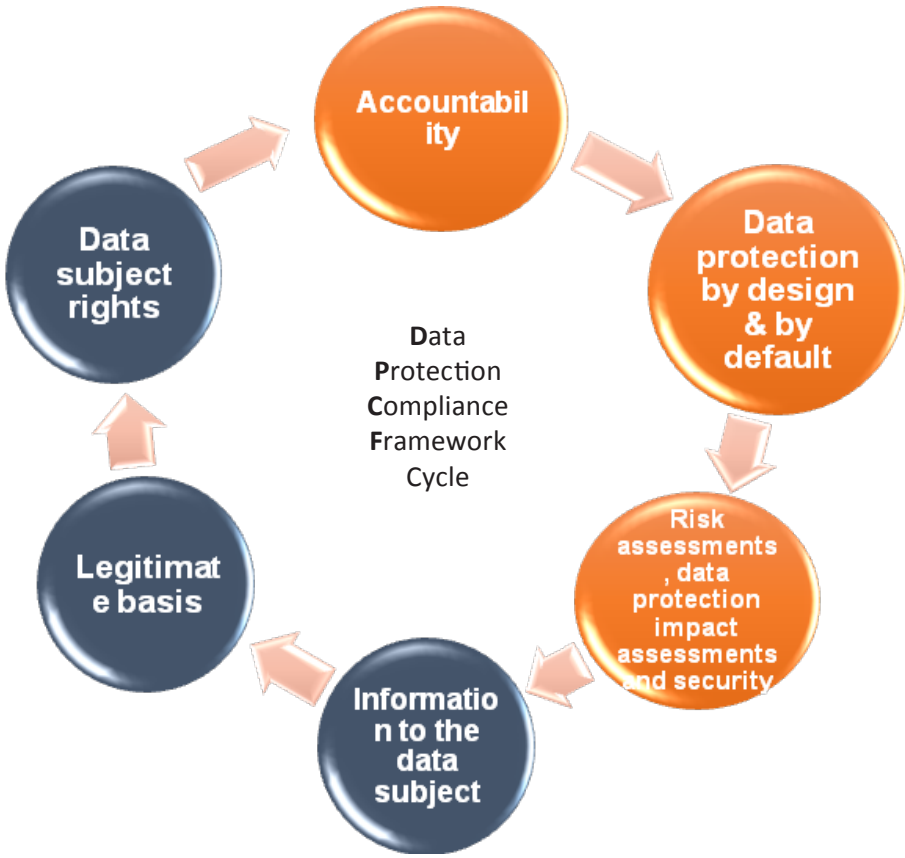

Fig. 1: The Data Protection Compliance Framework Cycle exemplifies a methodology which consists of six main steps which can be followed by entities seeking to bring their data processing practices into alignment with the GDPR through the development and practical implementation of a set of internal policies, 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-dacces-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

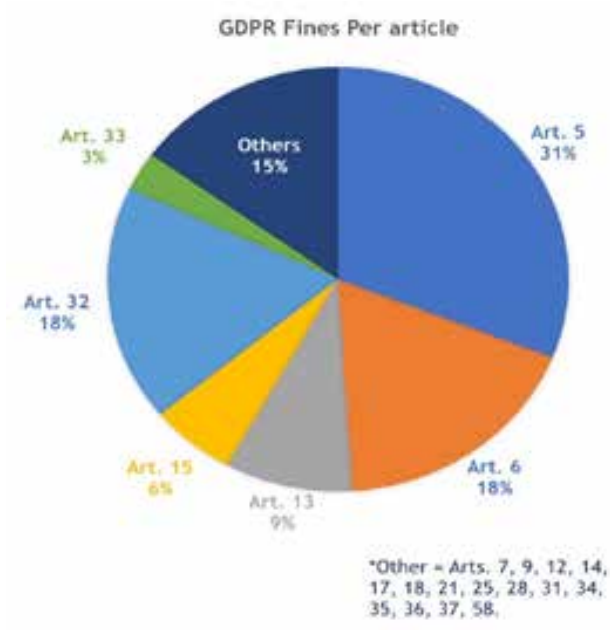

Fig. 2: GDPR Fines Overview per Article

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 Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal – Romania; 16 December 2019[265]

[265] Autoritatea Naţională de Supraveghere a PrelucrăriiDatelor cu Caracter Personal, *Sancţiune 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 Naţională 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 Naţională 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 Naţională 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 Naţională 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 Naţională 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 Naţională 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.