Jasmontaitė-Zaniewicz, Lina (Ed.); Calvi, Alessandra (Ed.); Nagy, Renáta (Ed.) et al.

**Book**

# The GDPR made simple(r) for SMEs

# THE GDPR
## MADE SIMPLE(R) FOR SMEs

EDITED BY
LINA JASMONTAITĖ-ZANIEWICZ
ALESSANDRA CALVI
RENÁTA NAGY
DAVID BARNARD-WILLS

# THE GDPR
## MADE SIMPLE(R) FOR SMEs

The GPRC label (Guaranteed Peer Review Content) was developed by the Flemish organization Boek.be and is assigned to publications which are in compliance with the academic standards required by the VABB (Vlaams Academisch Bibliografisch Bestand).

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

The content of this publication represents the views of the editors only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.


DOI: 10.46944/9789461171092

Book design: Frisco.be


VUBPRESS is an imprint of ASP nv (Academic and Scientific Publishers)
Keizerslaan 34, 1000 Brussels
Tel. +32 (0)2 289 26 56
Fax +32 (0)2 289 26 59
Email: info@aspeditions.be
www.vubpress.be

ISBN 978 94 6117 069 9 (print)
ISBN 978 94 6117 109 2 (ePDF)
ISBN 978 94 6117 110 8 (epub)
NUR 820, 980
Legal deposit D/2021/11.161/026

# Contents

## Acknowledgements

This handbook is the final outcome of the STAR II (SupporT small And medium enterprises on the data protection Reform II) research project, co-funded by the European Union within the scope of the Rights, Equality and Citizenship Programme 2014-2020 (REC-RDAT-TRAI-AG-2017), under Grant Agreement No. 814775.

The STAR II project was implemented by a partnership of the National Authority for Data Protection and Freedom of Information (NAIH) (coordinator), the interdisciplinary Research Group on Law, Science, Technology & Society (LSTS) of the Vrije Universiteit Brussel (VUB), and Trilateral Research Ltd (TRI IE) between August 2018 and December 2020.

STAR II consortium members included academics with extensive theoretical background in privacy and data protection – Lina Jasmontaitė-Zaniewicz and Alessandra Calvi – of VUB-LSTS, researcher and practitioner from TRI IE – David Barnard-Wills – who provides multidisciplinary research and consultancy services in the field of data protection; and Renata Nagy – the representative of the Hungarian Data Protection Authority, who has been actively engaged in awareness raising activities for SMEs.

The main goal of the project was to promote compliance with the General Data Protection Regulation (EU) 2016/679, commonly referred to as GDPR, by assisting Data Protection Authorities (DPAs) and Small and Medium-sized Enterprises (SMEs). To this end, the STAR II project prepared a Guidance for DPAs on running hotline services dedicated to SMEs and the handbook on European data protection law for SMEs outlining obligations and good practices concerning the processing of personal data. The STARII project materials are available at www.star-project-2.eu.

The STAR II project is a follow-up of the STAR project that developed easily customizable training materials for data protection professionals,

in particular Data Protection Officers, who are responsible for awareness-raising and the training of staff involved in processing operations.

We would like to thank Annika Linck of the European Digital SME Alliance for writing the preface. We would also like to express our gratitude to the members of the advisory board and data protection professionals who reviewed and commented on earlier versions of this handbook. In particular, we want to thank Jasmina Trajkovski (T&P Consulting), Denise Amram (LIDER Lab - DIRPOLIS Institute), Erin Anzelmo (Independent expert), Dariusz Kloza (VUB-LSTS-d.pia.lab), Carlotta Rigotti (VUB-FRC), Paul De Hert (VUB-LSTS),Vagelis Papakonstantinou (VUB-LSTS), Gábor Kulitsán, Júlia Sziklay (NAIH), Leanne Cochrane (TRI), Alan Moore (TRI) and Filippo Marchetti (TRI).

## Liability and legal disclaimer

## List of abbreviations

| | |
|---|---|
| **AEPD** | Agencia Española Protección de Datos (Spanish DPA) |
| **APD-GBA** | Autorité de protection des données – Gegevensbeschermingsautoriteit (Belgian DPA) |
| **BYOD** | Bring-Your-Own-Device |
| **CCTV** | Closed circuit television |
| **CNIL** | Commission nationale de l'informatique et des libertés (French DPA) |
| **CSIR(T)** | Computer Security Incident Response (Team) |
| **CSV** | Comma Separated Value |
| **DPA** | Data Protection Authority (supervisory authority) |
| **DPBD** | Data protection by design |
| **DPbDf** | Data protection by default |
| **DPC** | Data Protection Commission (Irish DPA) |
| **DPIA** | Data Protection Impact Assessment |
| **DPO** | Data Protection Officer |
| **EDPB** | European Data Protection Board |
| **EDPS** | European Data Protection Supervisor |
| **EEA** | European Economic Area |
| **ENISA** | European Union Agency for Cybersecurity |
| **EU** | European Union |
| **FRA** | European Union Agency for Fundamental Rights |
| **GDPR** | General Data Protection Regulation |
| **IAPP** | International Association of Privacy Professionals |
| **ICO** | Information Commissioner's Office (United Kingdom DPA) |
| **IP** | Informacijski pooblaščenec (Slovenian DPA) |
| **IT** | Information Technology |

| | |
|---|---|
| **JSON** | JavaScript Object Notation |
| **KPIs** | Key performance indicators |
| **NAIH** | Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian DPA) |
| **NGO** | Non-Governmental Organization |
| **NIS** | Network and Information Security |
| **PETs** | Privacy Enhancing Technologies |
| **PSD2** | Payment Service Directive |
| **PSI** | Public Sector Information |
| **RDF** | Resource Description Framework |
| **SME** | Small and Medium-Sized Enterprise(s) |
| **SOP** | Standard Operating Procedure(s) |
| **VDAI** | Valstybinė duomenų apsaugos inspekcija (Lithuanian DPA) |
| **WP29** | Article 29 Working Party (replaced by EDPB) |
| **XML** | Extensible Markup Language |

# Preface

The STAR II consortium has conceived this handbook as a tool which seeks to simplify the General Data Protection Regulation (GDPR) for small and medium-sized enterprises (SMEs). This handbook has set itself a very high standard for helping SMEs to comply with their legal obligations. However, making the GDPR simple for SMEs is a task that cannot be solved by a handbook alone; it requires a long-term approach and concerted efforts from public authorities, business, and society. Nevertheless, this handbook is an important stepping-stone that explains some of the main features of the GDPR (e.g. its risk-based approach and legal provisions embedding it) in a simple language. It also provides case studies and practical examples to guide SMEs.

SMEs amount to approximately 99 percent of businesses in the European Union. They are responsible for a large share of employment, and contribute substantially to economic growth. Yet, compliance with the GDPR can be problematic for SMEs, whereas noncompliance can have important repercussions in terms of fines or loss of trust. Unfortunately, many SMEs are not as well equipped as large companies when it comes to dealing with the GDPR. Legal uncertainty and interpretation resulting from the GDPR's risk-based approach constitute a problem for smaller companies, as they often lack the necessary internal resources and expertise. Many SMEs need to rely on external legal consultations to ensure that they are GDPR-compliant, which constitutes additional costs for them. Furthermore, formal aspects of the regulation, such as documentation requirements, can constitute an additional burden, due to high levels of bureaucracy associated with these obligations.

At the same time, the questionable data processing and data collection practices of Big Tech companies continue. While the GDPR awarded individuals greater rights and provided a general framework for data protection in the EU, it failed to substantially change the behaviour of

Big Tech companies that exploit personal data for their ad-based business models. The majority of digital SMEs comprising the membership of European DIGITAL SME Alliance do not follow such ad-based business models, and thus pose far less risk to the fundamental rights of individuals. Nonetheless, they were affected by the GDPR and had to implement its one-size-fits-all requirements, in spite of not having the same resources as large companies in terms of internal legal advice or finance.

In addition, a harmonized European legal space in terms of data protection is still in the making, and important challenges remain that concern the way the GDPR is applied across Europe. Whereas data protection authorities (DPAs) should inform SMEs and raise awareness, according to studies carried out in the context of the STAR II project, less than one-third of EU DPAs provide specific guidance to SMEs. Also, the capability of the DPAs to fulfil their roles depends on different factors that can change according to national circumstances (i.e. how they are equipped in terms of resources and staff). This set-up leads to uncertainties for smaller companies as to how to handle personal data, and also prevents them from benefitting from an effective uniform legal space in this area. Across Europe, DPAs and other supervisory authorities apply and interpret the GDPR differently. This may sometimes even be the case within a single country when multiple bodies enforce data protection rules. Therefore, businesses are often uncertain as to whether they comply with the provisions of the GDPR to their fullest extent. Further, while organizations seek advice from DPAs for certainty, the authorities can often only direct SMEs to recommendations and expose the consequences of possible choices; the final decision on how to address the situation is left to the organization itself, which bears the legal consequences of this.

As a representative of European small and medium enterprises in the digital sector, my organization welcomes clear and uniform rules which set the ground for a harmonized digital single market that allows companies, especially smaller ones, to operate and innovate in legal

clarity across EU internal borders and beyond. This handbook provides SMEs with important and clear guidance, and is therefore a welcome initiative to accompany SMEs on the path to better and uniform GDPR compliance and application across Europe.

*Annika Linck*
*EU Policy Manager*
*European DIGITAL SME Alliance*

# Introduction

## Background

More than two years have passed since the General Data Protection Regulation (GDPR) became applicable in the European Economic Area (EEA), which encompasses the territory of the Member States of the European Union (EU) as well as Iceland, Liechtenstein and Norway. The first round of evaluation reports by the European Commission and the European Data Protection Board consider the GDPR to be a great success.[1] Its harmonized rules for the processing of personal data have arguably improved data handling practices and enhanced individuals' awareness regarding their rights.[2] Furthermore, it is suggested that compliance with the GDPR can act as a competitive advantage, fostering consumer trust and providing new business opportunities.

However, attaining compliance and unleashing such competitive advantages requires a sound understanding of personal data protection principles and other legal notions found in the EU data protection framework. This is extremely difficult to achieve for smaller organizations, in particular, small- and medium-sized enterprises (SMEs). While the processing of personal data for many SMEs is unavoidable, it is often not their core activity and, consequently, they lack the sufficient human or financial resources to achieve adequate compliance.[3]



1 European Commission, 'Communication - Two Years of Application of the General Data Protection Regulation | European Commission' (2020) https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_en; European Data Protection Board, 'Contribution of the EDPB to the Evaluationof the GDPR under Article 97' (18 February 2020) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.

2 European Union, 'Special Eurobarometer 487a: The General Data Protection Regulation' (2019).

3 For example, personal data are processed in order to execute payments for employees, or to contact clients. CCTV systems at the premises of an SME in the footage also capture personal data.

Additionally, despite the barrage of available opinions and guidelines on the GDPR put together by regulators and data protection experts, there is a lack of practical, easy to understand and targeted guidance about data protection law for SMEs. Uncertainty over the interpretation of the revised data protection requirements is increased by those areas where national laws can diverge ('derogate') from certain GDPR provisions.

Regulators do recognize the unique challenges that SMEs face in regard to GDPR compliance, and do assist when possible. However, Data Protection Authorities (DPAs) apply the GDPR irrespective of the size of an organization. The enforcement actions taken by several DPAs across Europe demonstrate that they are willing to fine SMEs they find in breach of data protection rules in a similar manner to larger enterprises. The most illustrative examples in this regard include the 15,000 EUR fine issued by the Belgian DPA in late 2019 to an SME for not complying with information obligations stemming from the GDPR when using cookies;[4] a 20,000 EUR fine issued by French DPA to a translation company for continuously filming its employees at their workstations and thereby breaching the data protection rights of employees;[5] and a 5,000 EUR fine for a shipping company that did not conclude a data processing agreement with one of its business partners.[6]



## Structure

With this background in mind, the STAR II consortium prepared this handbook to help SMEs meet core GDPR requirements. Different

4 EDPB, 'The Belgian DPA has imposed a fine of € 15,000 on a website specialized in legal news' https://edpb.europa.eu/news/national-news/2019/belgian-dpa-has-imposed-fine-eu15000-website-specialized-legal-news_sv.

5 CNIL, Délibération SAN-2019-006 du 13 juin 2019 https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038629823/.

6 Odia Kagan, 'Hessian DPA Fines Shipping Company For Missing Data Processing Agreement' https://www.jdsupra.com/legalnews/hessian-dpa-fines-shipping-company-for-76851/.

chapters of the handbook summarize the main requirements that SMEs have to abide by to lawfully process personal data in the EU.

**Chapter 1 (Navigating support section)** provides an overview of the main public and private actors in the European data protection landscape. It describes the roles and responsibilities of public bodies and then explains how SMEs could use their support to adhere to GDPR requirements. As the scope of this handbook is limited solely to topics of particular concern for SMEs, it is important to be able to navigate among other available resources that could potentially facilitate GDPR compliance.

**Chapter 2 (Personal data protection basics)** explains the scope of data protection law and the scope of its application to SMEs. The chapter introduces concepts and principles that form the crux of personal data protection legal framework by answering the most commonly asked questions. Mastering this knowledge is essential when setting out a compliance strategy. The list of commonly asked questions is based on the NAIH's experience of running a hotline dedicated to SMEs.

**Chapter 3 (The theory and practice of a risk-based approach to personal data protection)** makes the aforementioned core concept of EU data protection law intelligible, subsequently explaining the GDPR provisions embedding it. In particular, the chapter addresses the responsibility of the controller (Article 24), principles of data protection by design and default (Article 25), documentation obligations (Article 30), security requirements (Article 32), personal data breach notifications (Articles 33 and 34), data protection impact assessment (Article 35) and the prior consultation procedure (Article 36). The final two sections of the chapter reflect on the use of codes of conduct (Article 40) and certifications (Articles 42 and 43) as tools that may make it easier for SMEs to comply with the GDPR.

Each section provides practical examples, suggestions and recommendations for further reading. Where available, we refer to relevant decisions by DPAs. This handbook is predominantly based on guidance documents issued by European data protection authorities.

**Chapter 4 (SMEs and employees' data)** addresses data protection concerns for SMEs when processing their employees' personal data.

## Method

The above-mentioned topics were found to be of particular concern for SMEs during the span of the STAR II project, and therefore form the exclusive focus of this handbook. More specifically, the project carried out interviews with representatives of 18 DPAs, 22 SME associations and 11 SMEs. Some observations were extracted from an additional 52-60 responses of SMEs to an online survey. Further substantive input was provided by the NAIH's hotline dedicated to SMEs, which responded to queries from SMEs between 15 March 2019 and 15 March 2020.

Furthermore, following the suggestions of different stakeholders interviewed by the STAR II consortium in 2019,[7] the handbook:

- includes examples and provides references to templates and guidance developed by various DPAs across the EU;
- introduces the background of risk-based provisions and then provides references to good practices, where available;
- suggests how SMEs can achieve compliance with the GDPR and how to transform this into a competitive advantage;
- targets a wide range of SMEs, regardless of their business sectors; and
- dismantles some common misconceptions about the GDPR.

Legal references without any further specification pertain to the GDPR. Hyperlinks are valid as of 21 September 2020.

7 STARII, Deliverable D2.2 – *Report on the SME experience of the GDPR* (July 2019) https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf 25.

## Bringing in added value

Many DPAs have published guidance on GDPR compliance, some of which is specifically addressed to SMEs.[8] However, SMEs interviewed during the STAR II project shared criticism of this material and reported low levels of uptake and use. Available DPA guidance documents were criticized for being overly generic and focusing on legal theory. Respondents pointed out that organizations must infer from them, and make assumptions about how the GDPR should be interpreted in their specific situation.[9] Some of the respondents noted that DPA guidance often raise more questions than they answer, and can be hard to follow in practice. Furthermore, some SME representatives shared the opinion that DPA guidance arrived too late, i.e. after the time the legislation should have come into effect.

Building on these insights, the handbook goes beyond a mere description of GDPR provisions and obligations stemming from them. It seeks to provide SME representatives with a set of proactive measures that were put forward by different DPAs and bodies across Europe. To make this handbook easy to approach, it is based around questions an SME representative might ask. In addition, it provides exhaustive references to other publicly available (open access) resources to further explain topics.



## Target audience

The handbook is addressed to SMEs. The term 'SME' includes a wide range of enterprises (e.g. a self-employed person, a family firm, partnerships and associations), which fall within the following criteria: they employ fewer than 250 persons and have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not

8 See 1. Navigating support.

9 Footnote 7.

exceeding EUR 43 million.[10] Small enterprises, employing fewer than 50 persons and whose annual turnover and/or annual balance sheet total do not exceed EUR 10 million, and microenterprises, employing fewer than 10 persons and whose annual turnover and/or annual balance sheet total do not exceed EUR 2 million, also fall within this range.

SMEs are not all the same. Recognizing this, the handbook is primarily addressed to enterprises that face structural barriers (e.g. lack of human and financial resources) in attaining compliance with the GDPR, and for which personal data processing is an auxiliary activity. More specifically, the handbook targets SME owners and their representatives dealing with data protection matters. These may include internal and external Data Protection Officers (DPOs). The handbook may be useful for SME associations and their memberships, as well as start-ups. If you are an SME and your business relies on the use of personal data, then it is important that you seek out data protection advice tailored to your activities.



10 Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises C(2003) 1422 Annex, Article 2. OJ L 124, 36-41 https://eur-lex.europa.eu/eli/reco/2003/361/oj.

# 1. Navigating support

People working in data protection often refer to the process of attaining compliance with the GDPR as a journey: 'an act of travelling from one place to another, especially when they are far apart' and also 'a long and often difficult process of personal change and development'.[11] Similarly, adhering to the GDPR requirements is not a one-off project. It is a challenging and continuous process. It requires organizations to consider their data handling practices and to identify risks arising from these. While doing so, individual specificities and the contexts in which enterprises function and process personal data must also be carefully evaluated.

The GDPR is a principle-based regulation and it leaves the issue of how to devise a compliance strategy to the discretion of the individual enterprise. While laying out such a strategy, prioritizing and planning for various measures, it is important to understand that there is plenty of support available. Some of this is provided by public authorities, while yet more has been created by the private sector. When informing yourself, however, it is important to be able to distinguish among resources and to build on reliable guidance.

For this reason, this chapter provides an overview of the main public and private actors of the European data protection landscape. It describes roles and responsibilities of public bodies and explains how SMEs could use their support to adhere to GDPR requirements. The chapter also introduces professional organizations.

11 Oxford Dictionary, OUP 2020.

## 1.1. National and regional Data Protection Authorities (DPAs)

National and regional Data Protection Authorities (DPAs), also known as supervisory authorities, are responsible for the monitoring and consistency of GDPR application. Each Member State has at least one supervisory authority.[12] However, while France, Hungary and Italy have only one supervisory authority, Germany and Spain have regional authorities in addition to a central authority. This is a consequence of their federal or devolved constitutional structure. Consequently, competences are then split between central and regional authorities.

DPAs act as enforcers, ombudsmen, auditors, consultants to policy advisors, negotiators and educators.[13] The latter role concerns raising public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data. To this end, DPAs, individually or jointly (e.g. as the European Data Protection Board), issue authoritative guidance on GDPR concepts and provisions.



Some guidance has been addressed to SMEs specifically. Based on the information provided by the STAR II interviews with DPAs as well as desktop research of all EU DPA websites, it appears that slightly fewer than one-third of EU DPAs currently provide GDPR guidance that is specifically tailored to SMEs. Upon the last review, this included the DPAs from Belgium (Autorité de protection des données - Gegevensbeschermingsautoriteit),[14] France

12 A list of European DPAs and their websites https://edpb.europa.eu/about-edpb/board/members_en.

13 Bennett, C. and Raab, C., *The Governance of Privacy: Policy Instruments in Global Perspective, MIT Press* (Cambridge MA & London 2003), 109-114. Barnard-Wills, D., Pauner Chulvi, C., and De Hert, P., 'Data Protection Authority Perspectives on the Impact of Data Protection Reform on Cooperation in the EU' (2016) 4 CL&SR 32, 587-98 https://doi.org/10.1016/j.clsr.2016.05.006.

14 *Autorité de protection des données* (APD) - *Gegevensbeschermingsautoriteit* (GBA), 'RGPD Vade-Mecum Pour Les PME' (2018) https://www.autoriteprotectiondonnees.be/publications/vade-mecum-pour-pme.pdf.

(Commission nationale de l'informatique et des libertés),[15] Ireland (Data Protection Commission),[16] Lithuania (Valstybinė duomenų apsaugos inspekcija),[17] Slovenia (Informacijski pooblaščenec),[18] Spain (Agencia Española de Protección de Datos),[19] Sweden (*Datainspektionen)*[20] and the UK (Information Commissioner's Office).[21] Some of these DPAs further distinguish guidance for micro-businesses.[22]



15 *Commission Nationale de l'Informatique et des Libertés* (CNIL), 'Guide Pratique de Sensibiliation Au RGPD' (2018) https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf.

16 *An Coimisiúm um Chosaint Sonrai*/The Data Protection Commission (DPC), 'Guidance Note: GDPR Guidance for SMEs' (2019) https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190708%20Guidance%20for%20SMEs.pdf.

17 *Valstybinė duomenų apsaugos inspekcija* (VDAI), 'Rekomendacija Smulkiajam Ir Vidutiniam Verslui Dėl Bendrojo Duomenų Apsaugos Reglamento Taikymo' (2018) https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_SVV_BDAR_2018.pdf.

18 *Informacijski pooblaščenec* (IP), 'Varstvo Osebnih Podatkov' (2018) https://upravljavec.si.

19 *Agencia Española de Protección de Datos (AEPD),* 'Facilita RGPD' https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd.

20 *Datainspektionen.* 'GDPR - Nya Dataskyddsregler' www.verksamt.se/driva/gdpr-dataskyddsregler.

21 *Information Commissioner's Office ICO),* 'Data protection advice for small organisations' https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/.

22 DPC, 'Guidance Note: Data Security Guidance for Microenterprises' (2019) https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190709%20Data%20Security%20Guidance%20for%20Micro%20Enterprises.pdf.
ICO, 'How Well Do You Comply with Data Protection Law: An Assessment for Small Business Owners and Sole Traders' (2019) https://ico.org.uk/for-organisations/business/assessment-for-small-business-owners-and-sole-traders/.

**SUGGESTION**

In principle, because the GDPR applies across the EU, an SME can use templates and tools for GDPR compliance developed by any European DPA, regardless of the place of its establishment. However, it must be considered that some national rules for processing personal data may differ. Several GDPR provisions foresee a possibility of derogations and exceptions.

## 1.2. The European Data Protection Board (EDPB)



The European Data Protection Board (EDPB) is an independent European body that contributes to the consistent application of data protection rules throughout the EU. It promotes cooperation between national DPAs. The EDPB is made up of the representatives from the European DPAs and the European Data Protection Supervisor (EDPS). Its decisions concerning cases under the consistency mechanism, certifications and codes of conduct are legally binding.

With the entry into force of the GDPR, the EDPB replaced the Article 29 Working Party (WP29) that in a similar composition, albeit in a solely advisory capacity, addressed issues relating to the protection of privacy and personal data until 25 May 2018.[23] Some of WP29 opinions concerning the GDPR's application were endorsed by the EDPB. Other WP29 opinions may be used to understand key concepts of European data protection laws.

The EDPB regularly issues opinions and guidance clarifying certain aspects of European data protection laws. These documents are not legally

23 WP29 was established under Data Protection Directive 95/46/EC.

binding, but are highly influential. While the EBPB does not provide individual consultancy services, the general guidance provided by this body can be useful for SMEs.[24] For example, the EDPB adopted guidelines on the concepts of controller and processor, on the use of consent, and on the application of data protection by design and by default principles. Some guidance focuses on specific activities, such as the processing of personal data through video devices or targeting social media users.[25]

## 1.3. The European Data Protection Supervisor (EDPS)

The European Data Protection Supervisor (EDPS) acts as the DPA for EU institutions, bodies, offices and agencies.[26] Similarly to the EDPB, the EDPS issues (non-legally-binding) opinions and general guidance upon various aspects of European data protection law. While such guidance is addressed to European institutions, bodies, offices and agencies (e.g. the European Commission or Europol), it provides practical advice that can be adapted accordingly to the reality and needs of SMEs. For example, the EDPS has issued guidelines on the use of cloud computing services and guidelines, on personal data and electronic communications in the EU institutions (eCommunications guidelines), and on security measures for personal data processing.[27]



24 EDPB, 'About EDPB' https://edpb.europa.eu/about-edpb/about-edpb_en.

25 EDPB, 'GDPR: Guidelines, Recommendations, Best Practices' https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

26 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. OJ L 295, 21.11.2018, 39–98 https://eur-lex.europa.eu/eli/reg/2018/1725/oj.

27 An overview of EDPS guidance https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en.

## 1.4. The European Union Agency for Cybersecurity (ENISA)

The European Union Agency for Cybersecurity (ENISA) supports the European institutions, Member States and the business community in addressing, responding to, and especially preventing, network and information security problems.[28] The Agency regularly issues guidance documents, some of which are specifically addressed to SMEs. These include a Cloud Security Guide for SMEs, a handbook on Security of Personal Data Processing specific to SMEs, and Guidelines for SMEs on the security of personal data processing.[29] These resources can be useful in meeting the technical security requirements under the GDPR.

## 1.5. The European Union Agency for Fundamental Rights (FRA)



The European Union Agency for Fundamental Rights (FRA) provides the relevant institutions, bodies, offices and agencies of the EU and its Member States with assistance and expertise relating to fundamental rights when implementing EU law. The right to protection of personal data is a fundamental right enshrined in Article 8 of the Charter of

28 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). OJ L 151, 7.6.2019, 15–69 https://eur-lex.europa.eu/eli/reg/2019/881/oj.

29 ENISA, *Cloud Security Guide for SMEs* (2015) https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes;
ENISA, *Handbook on Security of Personal Data Processing specific for SMEs* (2018) https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing
ENISA, *Guidelines for SMEs on the security of personal data processing* (2017) https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing.

Fundamental Rights of the EU. Therefore, the FRA publishes resources concerning this right that may be of assistance. For example, the FRA has published a handbook on European data protection law and a guide on profiling.[30] It also provides overviews of national laws implementing the GDPR requirements, such as one on the use of parental consent.[31]

## 1.6. The EU funded initiatives

The European Commission provides financial support for projects promoting compliance with the GDPR. To date, financial support has been granted through three waves of grants, totalling EUR 5 million by May 2020, with the two most recent ones specifically aimed at supporting national data protection authorities in their efforts to reach out to individuals and SMEs. Some of these projects have provided guidance and training materials in the national languages of member states.[32] For example, guidance has been provided in Danish, Dutch, French, Icelandic, Latvian, Lithuanian, and Slovenian. Within the scope of such EU-funded initiatives, guidance in English was also provided. The most illustrative examples of such guidance include 'The DPO handbook: Guidance for data protection officers in the public and quasi–public sectors on how to ensure compliance with the European Union



30 FRA/ECtHR/EDPS, *Handbook on European data protection law* (Publications Office of the European Union 2018) https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition; FRA, *Preventing unlawful profiling today and in the future: a guide* (Publications Office of the European Union 2018) https://fra.europa.eu/en/publication/2018/preventing-unlawful-profiling-today-and-future-guide.

31 FRA, Consent to use data on children https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/use-consent.

32 An overview of EU funding supporting the implementation of the GDPR https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en.

General Data Protection Regulation'[33] and a mobile application 'GDPR in Your Pocket' prepared within the scope of the SMEDATA Project.[34]

## 1.7. The International Association of Privacy Professionals (IAPP)

The International Association of Privacy Professionals (IAPP) is the world's largest global information privacy community. It provides its members with resources and guidance documents for running and managing risks arising from personal data processing. It has developed numerous resources facilitating compliance with the GDPR.[35] It also provides various training activities.



33 Korff, D. and Georges, M., *The DPO handbook - Guidance for data protection officers in the public and quasi–public sectors on how to ensure compliance with the European Union General Data Protection Regulation* (2019) https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf/a5bfc9ba-8a0c-0f88-9874-71be40be6a6d?version=1.0.

34 This application is available for download on Google Play Store and Apple App Store https://smedata.eu/index.php/mobile-application/.

35 IAPP, Overview of GDPR resources https://iapp.org/resources/topics/eu-gdpr/.

# 2. Personal data protection basics

## 2.1. What is personal data and its processing?

Understanding the concepts of **personal data** and its **processing** is fundamental for compliance with the GDPR.[36] Only the processing of personal data is regulated. This means that if the data processed is not personal, the GDPR does not apply.

A piece of information constitutes personal data if it relates to an individual human being, directly or indirectly, and hence such a piece of information is protected by law against misuse. In contrast, if a piece of information cannot be attributed to an individual, its free circulation is actually encouraged by law.[37]



36 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), OJ L 119, 4.5.2016, 1-88 http://data.europa.eu/eli/reg/2016/679/oj.

37 Cf. e.g. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, 56–83 https://eur-lex.europa.eu/eli/dir/2019/1024/oj.

**EXAMPLE**

Non-personal data may concern data about cultural works and artefacts — for example titles and authors — generally collected and held by galleries, libraries, archives and museums. It may concern data that is produced within the scope of scientific research, from astronomy to zoology. It may also include public sector information (PSI) and open data, encompassing data produced by statistical offices, information related to the presence of pollutants in the air, and governments' accounts.[38]

The GDPR includes some exemptions. Following the so-called 'household exemption', the GDPR does not apply to personal data processing carried out by a natural person in the course of a purely personal or household activity, which has no connection to a professional or commercial activity. This exemption is interpreted narrowly.



**EXAMPLES**

An individual takes a family picture for their own enjoyment.

Two co-workers exchanging their phone numbers for reasons that are not related to work are not bound by the GDPR. Whereas, if the exchange of phone numbers occurred in the context of an SME's business activities, the household exemption does not apply.[39]

Even if an SME processes only a single piece of personal data in the context of its business activities (e.g. a name of a contractual partner or their contact person to fulfil contracts of service), this processing is still subject to the GDPR.

38 Open Knowledge Foundation, 'What is open?' https://okfn.org/opendata/.

39 Article 2(2)(c) GDPR.

**Personal data** is any information related to an identified or identifiable natural person; such a person is called a **data subject.**[40] The definition of personal data is very broad.

**Any information** encompasses both objective information (e.g. identity card or social security numbers, results of blood analysis), and subjective one (e.g. opinions and assessments about a client and/or an employee).[41]

Identifiers such as a name, an identification number, location data, an online identifier or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person are considered personal data.

Information **related to** a natural person means that it is about that natural person, or objects, events, or processes that are somehow connected to that natural person.[42]



**EXAMPLES**

The service register of a car held by a mechanic contains information (personal data) related to different data subjects. For example, the name of the mechanic that worked on the car, the plate number and the engine number of the vehicle that can be linked to the owner of the serviced car.[43]

The call logs of office phones may contain personal data of different subjects, such as the employees of the company performing the

40 Article 4(1) GDPR.

41 Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (20 June 2007) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf 6.

42 Idem, 9.

43 Idem, 10.

calls; the clients called by the employees; certain third parties (e.g. potential clients of the company or administrative and other staff using the phone).[44]

'Smart metering systems' collect personal data when keeping a record of electricity consumption. Such data can reveal habits and behavioural data that may allow the identification of an individual.[45]

In principle, contacting a company (i.e. a legal person) with a direct marketing offer is not an activity subject to the GDPR, because the protection of the data of legal persons, such as companies, does not fall within the scope of the Regulation.[46] However, there are situations where this may not be the case. For example, where the name of an entity derives from that of a natural person, or where a corporate email account is used by one or several employees, whose identification may be possible from behaviour associated with that email account.[47]



To determine the **identifiability** of an individual, you have to consider all the means reasonably likely to be used to perform the identification. Factors to be considered include the capabilities of available technology at the time of the processing and technological developments, as well as the costs and the amount of time required for identification.[48]

Direct identification usually occurs by name. In turn, indirect identification is often based on a combination of several pieces of information.[49]

44 Idem, 11.

45 Papakonstantinou, V. and Kloza, D., 'Legal Protection of Personal Data in Smart Grid and Smart Metering Systems from the European Perspective' in *Smart Grid Security. Springer Briefs in Cybersecurity* (Springer 2015) https://doi.org/10.1007/978-1-4471-6663-4_2

46 Albeit in some Member States the national laws supplementing the GDPR extend the applicability of certain provisions of the Regulation to legal persons.

47 Footnote 41, 23.

48 Recital 26 GDPR.

49 Footnote 41, 13.

The possibility of identifying individuals could be affected by the application of pseudonymization and anonymization techniques to their personal data.

**Pseudonymization** is a form of processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information. Such additional information is to be stored and maintained separately, and is subject to technical and organizational measures that ensure that the personal data is not attributed to an identified or identifiable natural person.[50]

**EXAMPLE**

In the case of pseudonymization, personal data such as name, date of birth, sex, address, etc. is replaced by a pseudonym. Pseudonymization techniques include encryption with a secret key, hash function, tokenization, etc.[51]

**Anonymization** as such is not defined by the GDPR. However, the Regulation clarifies that anonymous information encompasses:

- information that does not relate to an identified or identifiable natural person; or
- personal data rendered anonymous in such a manner that the data subjects is not, or no longer, identifiable.[52]



50 Article 4(5) GDPR.

51 Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (10 April 2014) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf 20.

52 Recital 26 GDPR.

**EXAMPLE**

Anonymization techniques include two main approaches, namely randomization and generalization. The former encompasses methods that alter the accuracy of the data, such as noise addition and permutation. The latter includes practices that generalize, or dilute, the attributes of a data subject by modifying their scale (e.g. a region rather than a city, a month rather than a week), such as aggregation and k-anonymity, l-diversity/t closeness.[53]

The main difference between pseudonymized and anonymized data concerns the applicability of the GDPR to them. Even if pseudonymized data can no longer be attributed to a specific data subject (unless additional information is used) the data subject remains indirectly identifiable.[54] That is why pseudonymized data is considered personal data, and therefore subject to the GDPR.[55]

Conversely, when all identifying elements are eliminated and data is anonymized, the GDPR is no longer applicable.[56] However, in practice, distinguishing between pseudonymized and anonymized data may be difficult, especially when many services or technologies use the term 'anonymized' when they actually mean 'pseudonymized'.



53 Footnote 51, Ibid.

54 Footnote 30, 94.

55 Footnote 41, 8.

56 Cf Recital 26, footnote 30, 93.

**SUGGESTION**

When an SME decides to rely on anonymization techniques, it must consider whether full anonymization is achieved. If in doubt, it is best practice to consider data as personal data. In this way, higher protection is afforded to individuals to whom the data may refer to.

You may then question the added value of pseudonymization. Pseudonymization can be a technical measure to provide data security or to reduce the risks to data subjects.

It has been argued that current methods for anonymizing data still leave individuals at risk of being re-identified, and that the distinction between anonymized data and pseudonymized personal data is fluid, as the re-identification of individuals largely depends on the context.[57]

The concept of **processing** encompasses any operations performed on personal data, either manually or automatically, such as storage, recording, deletion, transfer, consultation, combination, etc.[58]



57 Rocher, L., M. Hendrickx, J. and de Montjoye, Y., 'Estimating the success of re-identifications in incomplete datasets using generative models', NC (2019)10, 3069 https://www.nature.com/articles/s41467-019-10933-3. Stalla-Bourdillon, S. and Knight, A., 'Anonymous data v. Personal data - A false debate: An EU perspective on anonymisation, pseudonymisation and personal data' (Brussels Privacy Symposium 2016) https://fpf.org/wp-content/uploads/2016/11/16.10.29-A-false-debate-SSB_AK.pdf.

58 Article 4(2) GDPR.

**EXAMPLES**

A hairdresser who schedules appointments in an agenda with names, surnames and phone numbers of clients is processing personal data.

The owner of a bed & breakfast processes personal data by making reservations and keeping contact details of guests in an excel file.

An employer, by communicating the details of a sick employee to the competent authority for welfare purposes, performs processing of personal data.

A recruiter, when reviewing CVs of prospective candidates for a job opening, is processing personal data.

Extracting phone numbers and email addresses from web pages to send direct marketing communications is a form of processing.



The GDPR affords higher level protection to **special categories of personal data**, which reveal:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;[59]
- biometric data (where used for identification purposes);[60]

59 'Genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person that gives unique information about the physiology or the health of that natural person, and which results, in particular, from an analysis of a biological sample from the natural person in question (Article 4(13) GDPR).

60 'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data (Article 4(14) GDPR).

- data concerning health;[61]
- a person's sex life; and
- a person's sexual orientation.[62]

When processing special categories of personal data, the controller must be able to select an appropriate legal ground for processing foreseen in Article 9 of the GDPR, following which:

- they have explicit consent of a concerned data subject;
- the processing is necessary for employment, social security and social protection (if authorized by law);
- the processing is necessary to protect the vital interests of data subject or others;
- the processor is a not-for-profit body processing such data about its members;
- the personal data has been made public by the data subject;
- the processing is necessary for legal claims or judicial acts;
- reasons of substantial public interest (with a basis in law);[63]
- the processing is necessary for health or social care (with a basis in law);
- the processing is necessary for public health (with a basis in law); or
- the processing is necessary for archiving, research and statistics (with a basis in law).



61 'Data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveals information about their health status (Article 4(15) GDPR).

62 Article 9 (1) GDPR.

63 Consider national law implementing the GDPR. An overview of national laws implementing the GDPR is provided in Annex I.

## SUGGESTIONS

When processing special categories of personal data, consider scale. If the processing of special categories of personal data is carried out on a large scale, a controller is required to conduct a data protection impact assessment (DPIA).

The notion of 'large scale' is contextual. Therefore, consider if the processing includes lots of people (a significant proportion of the population); or if it results in a large volume data; or if it is extensive and covers a large geographical area; or if it could have significant effects on individuals. If the processing meets one or more of the aforementioned criteria, then it likely counts as a large scale.

## USEFUL SOURCES

- Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (20 June 2007) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf
- Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (10 April 2014) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
- ICO, 'Anonymisation: managing data protection risk code of practice' (2012) https://ico.org.uk/media/1061/anonymisation-code.pdf

## 2.2. What are the possible roles for an SME in the processing operations?

The obligations of an SME under the GDPR depend on what they do with the personal data they process. Three scenarios can be envisioned. First, an SME may act as a **data controller** (or controller) and process personal data by itself. Second, it may instruct another entity – a **data processor** (or processor) – to process personal data on its behalf, while still acting as a controller. Third, it may process personal data on behalf of another entity, and in this way act as a processor.

Both controllers and processors must comply with specific rules,[64] but the responsibilities of the controller are higher. Controllers bear the ultimate responsibility for the processing of personal data and, in principle, can be held liable for damages arising from any infringement of the GDPR.

Processors can only be held liable if they fail to comply with obligations of the GDPR specifically directed to them OR if they acted outside of, or contrary to, the lawful instructions of the controller.[65]



64 For example, processors must be able to demonstrate compliance, keeping records of processing activities; ensure the security of processing, implementing technical and organizational measures; nominate a DPO in certain situations; notify data breaches to the controller. See FRA/ECtHR/EDPS, *Handbook on European data protection law* (Publications Office of the European Union 2018), 101, 102. Compared with the previous Data Protection Directive, the obligations posed by the GDPR on processors have increased. See Gabel, D. and Hickman, T., 'Chapter 11: Obligations of processors – Unlocking the EU General Data Protection Regulation' in White & Case LLP (ed.), *Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law* (5 April 2019) https://www.whitecase.com/publications/article/chapter-11-obligations-processors-unlocking-eu-general-data-protection.

65 Van Alsenoy, B., 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation' (2016) 7 JIPITEC 271 para 1 https://www.jipitec.eu/issues/jipitec-7-3-2016/4506.

As regards the roles in the processing operations:

1. an SME is a controller when, alone or jointly with others, it determines the purposes and means of the processing of personal data. The purposes of processing data define 'why' the personal data is being processed and the means of the processing define 'how' the data is processed.[66] If an SME determines the types of data to be processed, the period of the processing, third party access and the legal basis of the processing, then it is a controller.[67]

**EXAMPLE**

An individual beautician is operating within the premises of a spa and wellness centre. The two are different legal entities, but they agree to enter into a partnership and set up a common fidelity programme for their clients (e.g. for every spa entry, 5% discount at the beautician; for EUR 40 spent at the beautician, 5% discount on spa entry).

To join the common fidelity programme, clients are requested to give their name, surname and their email address.

For the personal data processed within the common fidelity programme, the spa and the beautician are joint controllers.

2. An SME is deemed to be a processor when it processes personal data on behalf of a controller following the controller's instructions. The processor is conceived rather as an 'agent' or 'delegate' of the controller, allowed to process personal data only in accordance with the instructions of the controller.[68] A processor must be

66 Footnote 16.

67 Article 29 Working Party, 'Opinion 1/2010 on the concepts of 'controller' and 'processor'' (16 February 2010) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf 32.

68 Footnote 65, Ibid.

legally separate from the controller.[69] Upon an authorization of the controller, a processor may engage with a **sub-processor**.[70] Controllers can decide either to process data by themselves (internally) or to outsource this activity to a processor.

**EXAMPLE**

If an employee of a pet shop is tasked with sending offers via mail to clients, the processing occurs internally. When the employee is acting within the scope of his/her duties as an employee, the employee is not a processor, but an agent of the controller itself.[71]

If the pet shop relied on a marketing company for the same activity, then the pet shop would be a controller and the marketing company a processor. The marketing company might suggest ways to process the personal data, but it would be the pet shop that makes the decision.

3. An SME is a recipient when personal data is disclosed to it, whether by a third party (namely, an entity that is not a data subject, a controller, or a processor)[72] or not. The Regulation does not lay down specific obligations or responsibilities for recipients and third parties. However, if a third party or a recipient begins to process the personal data received for its own purposes, it shall be considered

69 Footnote 67, 25.

70 Article 28(2) GDPR.

71 ICO, 'Controllers and processors' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/.

72 Article 4(10) GDPR.

a controller in regard to any processing operation on the personal data carried out for its own purposes.[73]

**EXAMPLE**

An art gallery sells a sculpture and needs to ship it to the buyer's address. To do so, the art gallery communicates to the courier the surname and home address of the client. In this case, the courier is a third-party recipient.

Who counts as a processor or controller is determined by the practical reality of what is happening with the personal data.[74] An entity that determines means and purposes of data processing *is* a data controller, regardless of what it might be formally termed (for example, in a contract). The role of an SME may change depending on the processing operations. It may be possible that an SME acts as a processor for certain datasets and as a data controller for others.

**EXAMPLE**

SME1 offers advertisement and direct marketing services to other companies. SME1 concludes a contract with SME2, whereby SME1 commits to provide advertising to the clients of SME2. In this case, SME1 is the processor – it acts on the instructions of SME2. SME2 is the data controller and therefore bears the overall responsibility for the processing. However, if SME1, obtains consent from the clients of SME2, and then uses SME2's client database for another purpose

73 European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (2 September 2020) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf 27.

74 Footnote 67, 9.

(e.g. promoting the products of SME3), SME1 is treated as the data controller for this data processing activity.

A jeweller concludes a contract with a security company, which, after installing cameras at the premises of the jeweller, also monitors them. The security company and its personnel monitoring the footage act as a processor, and the jeweller remains the controller of this processing.

If the security company exceeds the instructions of the jeweller (e.g. it stores recordings without being requested to do so), then it is considered to be the data controller. It is also likely to be in breach of the contract and process personal data unlawfully.

If the security company simply installs the cameras, then it neither qualifies as a processor nor as a controller.

The relationships between controllers and processors are governed by a contract. In other words, if a controller works with a processor or with another controller, a **written and binding contract** (called a data processing agreement) should be concluded. This contract must describe in detail the reciprocal obligations and rights, in addition to subject matter, nature, purpose, duration of the processing, types of personal data and categories of data subjects.[75] This data processing agreement must be concluded *before* the actual data processing takes place.

If a processor engages a **sub-processor**, the same data protection obligations as listed in the agreement between the controller and the (original) processor apply.[76]

75 Articles 28(3) and (9) GDPR.

76 Article 28(4) GDPR.

The contract between joint controllers specifies roles and responsibilities of the joint controllers, including the ones concerning data subjects' rights.[77]

### SUGGESTION

The European Commission and DPAs may create or adopt s**tandard contractual clauses** with regard to data processing agreements between controller and processor, and processor and sub-processor based in the EU or in third countries. DPA clauses must be approved by the EDPB.

These would essentially be templates for good practices in how to set up a contractual agreement between a controller and processor. In the event that a controller or a processor uses approved contractual clauses, only adaptation is possible.

When drafting a data processing agreement, it is worth consulting the website of the DPA where the SME is established to see if contract templates are available in the local language.

### USEFUL SOURCES

- European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (2 September 2020) https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
- ICO, 'Controllers and processors' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

77 Article 26(2) GDPR.

» Article 29 Working Party, 'Opinion 1/2010 on the concepts of 'controller' and 'processor'' (16 February 2010) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

» FRA/ECtHR/EDPS, *Handbook on European data protection law* (Publications Office of the European Union 2018) (Chapter 2 Data Protection terminology) https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

**Guidance on contracts between controller and processors**

» ICO, 'Contracts' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

» DPC, 'Controller and Processor relationships - Guidance: A Practical Guide to Data Controller to Data Processor Contracts under GDPR' https://www.dataprotection.ie/en/organisations/know-your-obligations/controller-and-processor-relationships

» GDPR.EU, 'Data Processing Agreement (Template)' https://gdpr.eu/data-processing-agreement/

» Danish DPA, 'Standard Contractual Clauses for the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)' https://edpb.europa.eu/sites/edpb/files/files/file2/dk_sa_standard_contractual_clauses_january_2020_en.pdf

» AEPD, 'Ejemplo de cláusulas contractuales para supuestos en que el encargado del tratamiento trate los datos en sus locales y exclusivamente con sus sistemas' in 'Directrices para la elaboración de contratos entre responsables y encargados del tratamiento' https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf

» CNIL, 'Exemple de clauses contractuelles de sous-traitance' in the 'Guide du sous-traitant' (2017) https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

### RELEVANT DPA DECISION

The Hessian DPA (Germany) fined a small shipping company for engaging in the processing of personal data without having a data processing agreement with one of the business partners. The shipping company was fined with EUR 5,000.[78]



78 Footnote 6.

## 2.3. What are the principles applicable to the processing of personal data?

Principles can be understood as general norms embedding values that are particularly important within a legal system.[79] The GDPR contains six principles governing the processing of personal data to which controllers are required to adhere. These are:[80]

### 1. Lawfulness, fairness and transparency

Lawfulness means that there must be a legal basis (or ground) for processing personal data.[81] Fairness can be linked to ethical personal data processing, in the sense personal data must be handled in ways that people would reasonably expect, and not used in ways that have unjustified adverse effects upon them.[82] Transparency requires informing the data subjects in clear and plain language as to how their data is being used, and what the risks, rules, safeguards, and rights connected to the processing of personal data are.[83]

### 2. Purpose limitation

Purpose limitation means that any processing of personal data must be done for a well-defined specific purpose, identified before the beginning of processing. Any further processing must be compatible with the original purpose.[84] This is the principle that prevents collection of personal data 'just in case', without any outline as to how it will be used.

79 Oxford Bibliographies Online, 'General Principles of Law' https://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0063.xml.

80 Article 5 GDPR.

81 Footnote 30, 118.

82 ICO, 'Principle (a): Lawfulness, fairness and transparency' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/.

83 Footnote 30, 118.

84 Idem, 122.

### 3. Data minimization

Data minimization entails using only the data that is adequate, relevant and not excessive in relation to the purpose for which it has been collected and/or further processed.[85]

### 4. Accuracy

Accuracy requires that personal data must be checked regularly and kept up to date, and that inaccurate data is promptly erased or corrected ('rectified' in GDPR terminology).[86]

### 5. Storage limitation

Storage limitation requires the deletion or anonymization of personal data as soon as it is no longer needed for the purposes for which it was collected.[87]

### 6. Integrity and confidentiality

Integrity and confidentiality are related to data security. They imply that appropriate technical and organizational measures to secure personal data and prevent data breaches must be set in place.[88]

Controllers are accountable for demonstrating compliance with the six principles. For this purpose, SMEs need to put in place appropriate technical and organizational measures, and be able to demonstrate what they did and its effectiveness, when requested.[89]

85 Idem, 125.

86 Idem, 127.

87 Idem, 129.

88 Idem, 131.

89 See 3.7.1 Responsibility of the controller and the principle of accountability.

**SUGGESTION**

Judges invoke legal principles such as these to interpret laws and fill in the actual or potential legal gaps when addressing legal disputes.[90] Similarly, data protection principles may support SMEs in better understanding the other provisions of the GDPR that they are required to comply with. For example, the obligation of the data controller to provide information about the processing of personal data to a data subject[91] is one of the ways in which the GDPR puts into practice the principles of lawfulness, fairness and transparency.

## 2.4. What are the possible legal bases for personal data processing?

### 2.4.1. Background

To process personal data lawfully, meaning in accordance with the principle of lawfulness, SMEs need to specify a legal basis (legal ground). The Article 6 of the GDPR foresees these legal bases:

- the data subject consented to the processing;
- the processing is necessary for the performance of a contract to which the data subject is a party;
- the processing is necessary to comply with a legal obligation existing upon the controller;
- the processing is necessary to protect the vital interests of data subjects or of another person;
- the processing is necessary for the performance of a task carried out by the data controller in the public interest or in exercising official authority; and

90 Footnote 79.

91 See 2.5 What are data subjects' rights?

» the processing is necessary for the purposes of the legitimate interests of controllers or third parties, insofar as they are not overridden by the interests or fundamental rights of the data subjects.

### 2.4.2. How to choose among different legal bases?

The choice of appropriate legal ground depends on the circumstances of the processing operation.

#### Consent

Consent can be given by the data subjects with a statement (written, oral, video, audio, etc.) or an affirmative action (a click, typing a digit, etc., but not with a pre-filled answer). The consent can be obtained electronically, as the GDPR does not specify any form. However, the data controller must be able to prove that the data subject has consented.

To be valid, consent needs to be a **freely given**, **informed**, **specific** and **unambiguous** indication of the data subject's wishes to have their personal data processed.

As consent is **freely given**, it can be withdrawn at any time by the data subjects, without any detriment.[92] Examples of detriments are disadvantage, deception, intimidation, coercion or significant negative consequences.[93] Negligible negative consequences for data subjects do not undermine their consent.

If consent is bundled up as a non-negotiable part of terms and conditions, or if it is used in a situation of imbalance of powers (e.g. in an employment context), it is presumed to have not been freely given.

92 Recital 42 GDPR.

93 European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' (4 May 2020) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf para 46, 47.

**EXAMPLES**

A minimarket offers clients a personal card for discounts. In this case, the minimarket can process the personal data of its clients on the basis of their consent, because not enjoying extra discounts is a minor negative consequence.[94]

A company launches a fitness app. In the Terms and Conditions of the app, it is stated that users must consent to the processing of name, surname, date of birth, weight, dietary requirements, and geolocation data.

In this case, the consent form shall be separated from the Terms and Conditions. Furthermore, the user should be able to choose whether they want to share all of the information requested or only some of it, as not all information is necessary for the functioning of the app.

**Informed** consent means that data subjects have to understand what they are agreeing to. Therefore, data subjects at minimum need to be given information concerning:

- identity of the controller and the purposes of the processing;
- (the type of) personal data that will be processed; and
- existence of the right to withdraw consent.[95]

**SUGGESTION**

When presenting a consent form, the data controller is required to use clear and plain language. A lengthy consent form full of legalese and technical terms does not count as informed consent.

94 Footnote 30, 145.

95 Footnote 93, para 64, 65.

**Specific** consent means that, if the data processing is performed for several purposes, the consent must be obtained with regards to each of the purposes. This is called granularity of the consent.

**EXAMPLE**

A sports centre would like to collect customers' email addresses in order to send them a monthly newsletter concerning new courses and training activities.

At the same time, the sports centre would also like to share customers' details with other partner companies (e.g. a company specialized in fitness clothing and a company specialized in supplements). In this case, the sports centre has to request consent for the two purposes separately, i.e. sending the newsletter and sharing the email addresses with the partners.



**Unambiguous** means that it must be obvious that the data subject has consented to the particular processing. Actions such as scrolling or swiping through a webpage cannot be considered affirmative actions (unless the user is asked to draw a figure with the cursor to give consent or similar), as they cannot be distinguished from other forms of interaction with the webpage.[96]

A mere 'no objection' to the processing cannot count as affirmative action.

96 Idem, para 8.

**EXAMPLE**

A catering service requires clients to create an online account to make orders and deliveries.

To finalize the registration, the client is shown three tick boxes saying, 'I agree with the terms and conditions', 'I consent to the processing of personal data', and 'I agree to receive marketing communication'. If the boxes are already ticked by default, then consent is not valid. The controller has to develop three different boxes to ensure that by default only personal data which is necessary for each specific purpose of the processing is processed.

When so-called 'information society services' (i.e. contracts and other services that are concluded or transmitted online) are offered directly to a **child**,[97] and consent is used as a legal basis, the caregiver must also consent. The GDPR foresees that parental consent is needed where the child is below the age of 16 years. However, the age requirement for consent may be as low as 13 years old and, therefore, national laws or guidance of DPAs must be consulted.[98]



97 The notion of child changes depending on national law. The GDPR considers as children those under 16 years old, but it allows member states to lower the threshold to as low as 13 years old.

98 van der Hof, S., Lievens, E. and Milkaite, I., 'The Protection of Children's Personal Data in a Data-Driven World: A Closer Look at the GDPR from a Children's Rights Perspective' in Liefaard, T., Rap, S. and Rodrigues, P. (eds.), *Monitoring Children's Rights in the Netherlands. 30 Years of the UN Convention on the Rights of the Child* (Leiden University Press 2020).

**EXAMPLE**

Italy and Austria have set the age limit for a minor to give consent for provision of information society services at 14 years old. In Germany, this threshold is 16 years, whereas some countries set the threshold to 13 years.[99]

**SUGGESTION**

Using consent as a legal basis for processing personal data is not always possible or desirable. First of all, demonstrating that consent was freely given, informed, specific and unambiguous can actually be quite challenging. Secondly, consent can be withdrawn at any time. SMEs should consider using other legal bases where these would be appropriate.

**USEFUL SOURCES**

» European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' (4 May 2020) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

» ICO, 'Lawful basis interactive guidance tool' https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/

## Contractual relationship

In certain cases, the processing of personal data is necessary for performing (or entering) a contract to which the data subject is a party.

99 Footnote 31.

**EXAMPLE**

An online shop needs to process information about customers (e.g. addresses) to deliver its products. In this case, the legal basis for the processing could be the performance of the purchase contract between the shop and the customer. An address is clearly necessary here, but other information might also count as necessary for the contract in other circumstances, for example, making sure a customer buying alcohol is old enough to do so.

## Compliance with a legal obligation

In certain cases, the processing of personal data is necessary for the data controller to comply with a legal obligation. Such a legal obligation may originate from either EU or Member State law. The law itself will determine the purposes of the processing, the specifications for determining the controller, the type of personal data processed, the data subjects concerned, and the entities to which data will be disclosed. Typically, if an SME is required by law to do something with personal data, the GDPR does not prevent them from meeting that obligation.

**EXAMPLES**

When entrepreneurs share the personal data of customers with tax authorities for fiscal purposes, the legal basis for the processing is compliance with a legal obligation.

When employers communicate to the competent national authority information about their employees for social security purposes, the legal basis for the processing is compliance with a legal obligation.

### Vital interests of data subjects or of another person

In certain cases, processing personal data is necessary to protect the vital interests of data subjects or of another person. This legal ground allows processing in situations of life and death, where the right to personal data protection is overridden by the right to life.

**EXAMPLE**

In the event of a workplace accident, the employer may share with the emergency doctors the personal data about the injured employee.

### Public interest or exercise of an official authority vested in the data controller

In certain cases, the processing of personal data is necessary for the data controller to perform a task carried in the public interest or to exercise official authority.

Exceptionally, an SME can be entrusted, under the legal regime applicable to it, with the performance of services of public interest or with an official authority. If, for the performance of these tasks, the SME is required to process personal data, the public interest and the exercise of the official authority count as legal bases.

'Public interest' should not be taken to mean, 'it would be generally good for the public if this processing happened', but rather that there is a defined public interest that can be identified.

**EXAMPLES**

A bus company provides public transportation in a town. The employees of the company acting as ticket inspectors can demand the contact details of the travellers lacking tickets, in order to issue fines. The legal basis is the exercise of official authority.

A company provides energy in a town. When the information concerning the household consumptions and usages are processed, the legal basis may be the public interest.

## Legitimate interests pursued by the data controller

In certain cases, the processing of personal data is necessary for the purposes of the legitimate interests pursued by controllers or third parties, insofar as they are not overridden by the interests or the fundamental rights of the data subjects.

The elements that SMEs must consider when using this legal basis are:

- whether they have a **legitimate interest** for the processing.
  For this, an SME has to consider if an interest is:
  - **lawful**, meaning in accordance with applicable EU and national laws;
  - sufficiently **specific**, to allow the balancing test with the interests and fundamental rights of the data subject to be carried out;
  - **real and present**, in the sense of not speculative.[100]
- whether the processing is necessary for that purpose.
- whether the legitimate interest is not overridden by the data subjects' interests, rights or freedoms.[101]



100 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' (9 April 2014) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf 25.

101 ICO, 'What is the 'legitimate interests' basis?' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/ and CJEU, C-13/16, Rigas case http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex= 0&part=1&mode=req&docid=190322&occ=first&dir=&cid=136957.

As a general criterion, the legitimate interest can be invoked as a legal basis when the data subject can reasonably expect, at the time and in the context of the collection of the personal data, that processing for that purpose may take place.[102] When the processing of personal data is strictly necessary for the purposes of preventing fraud, this constitutes a legitimate interest of the data controller concerned.[103]

**EXAMPLES**

A restaurant offers food delivery services. New clients may enjoy a free meal delivered to their home. The offer can be activated upon subscription, yet it is limited to one time per household. In this case, the company may check its database of existing clients to confirm that a new client is not from a household that has already benefited from this offer.

An online shop requires its customers to share their email addresses in order to send them updates about the execution of their orders. For this processing, the shop relies on consent. If the shop decides to use email addresses to send marketing materials, this entails a change in purpose of the processing. Consequently, the shop needs to have a legitimate basis for this new type of processing. The shop, provided that the above criteria are met, may invoke the legal basis of a legitimate interest.



102 Recital 47 GDPR.

103 Recital 47 GDPR.

### RELEVANT DPA DECISION

Even if the GDPR provides that the processing of personal data for direct marketing purposes may be regarded as being carried out for a legitimate interest,[104] this is not always the case.

For example, the Dutch DPA imposed a fine upon a tennis association for sharing its members' data with some sponsors, who used this for marketing purposes. In this case, the Dutch DPA denied that the mere commercial interest could constitute a legitimate interest.[105] However, the decision remains highly controversial.

### USEFUL SOURCES

- FRA/ECtHR/EDPS, Handbook on European data protection law (Publications Office of the European Union 2018) https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf
- APD-GBA, 'Direct Marketing Recommendations' https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/02/Recommandation_01-2020_marketing_direct1-French.pdf
- ICO, 'Direct Marketing' https://ico.org.uk/media/1555/direct-marketing-guidance.pdf
- DPC, 'Direct Marketing - What you need to know about direct marketing' https://www.dataprotection.ie/en/organisations/rules-electronic-and-direct-marketing

104 Recital 47 GDPR.

105 See the summary of the Dutch DPA decision https://www.hldataprotection.com/2020/04/articles/international-eu-privacy/dutch-dpa-imposed-a-controversial-fine-on-the-royal-dutch-tennis-association/.

» CNIL, 'La réutilisation des données publiquement accessibles en ligne à des fins de démarchage commercial' https://www.cnil.fr/en/node/119840

## 2.5. What are the data subjects' rights?

### 2.5.1. Background

Under the GDPR, data subjects have a set of rights relating to their personal data. In practice, these rights place obligations upon data controllers.[106] SMEs acting as data controllers have a responsibility to respond to queries from data subjects about the exercise of their rights. SMEs acting as processors may also play a part in this; they are likely to be requested to assist the controllers through the provision of appropriate technical and organizational measures to grant data subjects their rights when this is possible.[107]

**SUGGESTION**

The written agreement between the controller and the processor may clarify how the processor will practically assist the controller in complying with data subjects' requests.

106 Ausloos, J., Mahieu, R. and Veale, M., 'Getting Data Subject Rights Right' (2019) 10 JIPITEC 283 https://ssrn.com/abstract=3544173.

107 Article 28(3)(e) GDPR.

In principle, the data controller must reply to data subject queries 'without undue delay', and **within a month**.[108] This time limit can be extended where necessary, providing that the data subject is warned within 30 days and the delay is 'duly motivated' (e.g. due to the complexity of the issues, the number of the requests). Data subjects can present the request verbally (e.g. telephone) or in writing (e.g. email, post, social media).[109]

Not all requests from data subjects are justified. When data subjects' requests are manifestly unfounded or excessive (e.g. repetitive), the controller may either charge a reasonable fee on the basis of the real administrative costs that would arise from meeting the request (it is not possible to charge a penalty amount) or refuse to act. Still, the controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

Before following up on a request, the data controller should verify the identity of the person presenting it. This should be done in order to prevent third parties from gaining unlawful access to the personal data of others.

In some cases, requests concerning the exercise of data subjects' rights may come from third parties and not from the data subject directly (e.g. if a solicitor or a family member acts on behalf of the data subject upon their request and consent, if a data subject lacks the mental or legal capacity to manage their own affairs).[110]



108 Article 12(3) GDPR.

109 ICO, '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/.

110 Panagiotopoulos, A., 'Data subjects' requests made on behalf of others: Practical considerations on data subjects' requests and elected representatives' https://www.trilateralresearch.com/data-subjects-requests-made-on-behalf-of-others-practical-considerations-on-data-subjects-requests-and-elected-representatives/.

**SUGGESTIONS**

If a Data Protection Officer (DPO) is appointed, she is responsible for the following activities:

- addressing data subjects' requests;
- having a policy to deal with data access requests (specifying roles, internal deadlines, etc.), which increases efficiency in dealing with such requests; and
- keeping written records of the (verbal) requests received and of the follow-ups to these helps a company to demonstrate compliance with the GDPR in the event of an investigation by a DPA.

**USEFUL SOURCES**

- ICO, 'Individual Rights' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/



## 2.5.2. What are data subjects' requests, and how can these be fulfilled?

### Right to transparency and information

Data subjects must be informed, in **clear and plain language**, about:

- the main elements of processing operations (i.e. type of personal data processed, legal basis, specification of the purposes, data retention period, eventual data transfers, etc.);
- contact details of parties involved (e.g. data controllers and, if present, DPO and recipients); and
- the existence of their data subjects' rights, and how to exercise/claim these.

**SUGGESTION**

Articles 12, 13 and 14 of the GDPR contain a detailed list of information to be provided to data subjects in different processing situations. SMEs' privacy and data protection notices should meet these requirements. A clear and transparent privacy/data protection notice increases the trust of data subjects, and it may most likely reduce the number of queries submitted by data subjects.

A privacy/data protection notice must be concise, transparent, intelligible and easily accessible.

**SUGGESTION**

There are several techniques that can be used by SMEs to provide information:

- a layered approach;
- dashboards;
- just-in-time notices;
- icons;
- mobile and smart device functionalities;[111] and
- cartoons, infographics or flowcharts.[112]



111 ICO, 'Right to be informed' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/.

112 Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (11 April 2018) http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 para 18.

**USEFUL SOURCES**

- Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
- ICO, 'Right to information' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/
- An example of a template for a privacy notice https://gdpr.eu/wp-content/uploads/2019/01/Our-Company-Privacy-Policy.pdf



## Right to access

The right to access (Article 15 of the GDPR) gives a data subject the right to be told by the controller if their personal data has been processed and, if so, to obtain access to and a copy of the personal data processed.

Data access requests may come from either data subjects who are external to the organization (e.g. clients) or who are internal (e.g. employees).

The idea behind the right to access is that data subjects can check the lawfulness of data practices of a data controller.

While the right to information under Articles 13 and 14 is meant to ensure that the data subject receives a general and comprehensive picture of the processing, the right to access under Article 15 seeks to ensure that the data subject receives information on the processing of their personal data in order to control the lawfulness of processing.

When replying to a data access request, the data controller should provide the data subject with the following information:[113]

113 Article 15 GDPR.

- they should confirm the identity of the individual requesting the data to decide whether personal data concerning the data subject(s) is being processed;
- they should provide a copy of the personal data undergoing processing (in so far as this does not affect the rights and freedoms of others); and

provide information as to:

- the purposes of the processing;
- the categories of personal data concerned (e.g. contact details, credit card details);
- the (categories of) recipients (who else the data is being provided to);
- the retention period, meaning for how long personal data will be stored, or the criteria by which this is determined;
- the existence of the right to request from the controller rectification, erasure, restriction of processing, object to the processing of personal data concerning the data subject;
- the existence of the right to lodge a complaint with a supervisory authority;
- the source of personal data, where it is not collected directly from the data subject;
- the existence of any automated decision-making, including profiling, together with meaningful information about how that decision-making works ('the logic involved'), as well as the significance and the envisaged consequences of such processing for the data subject; and
- the appropriate safeguards existing in case of a data transfer to third countries or international organizations (e.g. standard data protection clauses, binding corporate rules, a code of conduct, a certification).

**EXAMPLE**

A data access request may concern a registry containing the personal data of the person advancing the request, but it may also concern personal data of others. In this case, the data controller needs to balance the right to access of the data subjects with the rights of the other people that may be affected by the disclosure of the information. The data controller cannot simply refuse to provide all relevant information, but endeavours should be made to comply with the request to as great an extent as possible. When complying with this obligation, the controller must ensure adequate protection for the rights and freedoms of others.[114] For example, access to the registry may be provided only after deleting the personal data of the other people concerned.

In providing a copy of an image containing the data subject and other people, the data controller might blur out the images of the other people before supplying that image to the requester.

**SUGGESTION**

When the data access request is broad, the controller may ask the concerned individual to clarify its scope. This could reduce the time and effort the controller needs to spend on compiling relevant data and preparing a response to the request.

Consider whether software tracking tools could be used in order to assist and to optimize costs associated with data subjects' requests.

114 DPC, 'The Right of Access' https://www.dataprotection.ie/en/individuals/know-your-rights/right-access-information.

**USEFUL SOURCES**

» ICO, '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/

» DPC, 'The Right of Access'
https://www.dataprotection.ie/en/individuals/know-your-rights/right-access-information

## Right to rectification

Data subjects have the right to demand the data controller correct ('rectify') the information concerning them. The right to rectification is useful both for the data subjects and for SMEs because this right facilitates the keeping of data that is up-to-date.

If the controller has disclosed the personal data being corrected to any other recipients, then they should communicate any rectification to each recipient, unless this proves to be impossible or involves a disproportionate effort.[115]

## Right to erasure, a.k.a. right to be forgotten (right to de-listing)

Data subjects have the right to have their personal data deleted from the records of the data controller.

The controller deletes the personal data when:

» it is no longer necessary for the purposes for which it was processed;
» it was collected in relation to the offer of information society services to children;
» it was unlawfully processed (e.g. without a legal basis);

115 Article 19 GDPR.

- the data subject withdraws consent or objects to the processing, and there is no other legal ground for the processing; and/or
- Union or Member State law requires the controller to do so.[116]

There are numerous exceptions to the right to erasure. They may include the exercise of the right of freedom of expression and information, the need to comply with a Union or national legal obligation requiring the processing, and the exercise or defense of legal claims.

If the controller has disclosed the personal data being corrected to any other recipients, then they should communicate any erasure request to each recipient, unless this proves to be impossible or involves a disproportionate effort.[117]



**EXAMPLE**

When complying with the right to erasure, all personal data in backup copies (with either the controller or the processor, as well as third parties) shall be erased. Furthermore, the ability to restore erased data shall be finally terminated by all technically feasible means.

**SUGGESTION**

In practice, to facilitate the exercise of the data subject's rights, a controller could put a form for the requesting of erasure on their website.

116 Footnote 30, 223.

117 Article 19 GDPR.

**USEFUL SOURCES**

» EDPB, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)' https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en

» An example of a request form for an erasure https://gdpr.eu/wp-content/uploads/2019/01/RIGHT-TO-ERASURE-REQUEST-FORM.pdf

## Right to restriction of processing

The data subject can ask the data controller to temporarily limit the processing of their personal data when one of the following applies:

» the accuracy of the personal data is contested;
» the processing is unlawful and the data subject requests restriction instead of erasure;
» the controller no longer needs the data for the purposes of processing (so it would otherwise be deleted), but the data must be kept for the exercise or defence of legal claims; and
» a decision is pending on the legitimate interests of the data controller prevailing over the interests of the data subject.

The controller shall communicate any restriction to each recipient to whom they disclosed the personal data unless this proves to be impossible or involves a disproportionate effort.[118] Furthermore, the controller must notify the data subject before the restriction on processing is lifted.[119]

118 Article 19 GDPR.

119 Footnote 30, 223.

**EXAMPLES**

Methods to grant the restriction of processing include:

» temporarily moving the selected data to another processing system;
» making the data unavailable to users;
» removing personal data temporarily; and
» clearly marking the data as restricted.

## Right to data portability

The idea behind the right to data portability is that data subjects should be able to easily take their personal data with them between services.

Under the GDPR, data subjects enjoy the right to data portability in situations where the personal data that they have provided to a controller is processed by automated means on the basis of consent, or where the personal data processing is necessary for the performance of a contract and is carried out by automated means. This means that the right to data portability does not apply in situations where the personal data processing is based on a legal ground other than consent or a contract.[120]

At a practical level, data subjects are entitled to have their personal data transmitted directly from one controller to another, if this is technically feasible. To facilitate this, the controller should use interoperable data formats that enable data portability for the data subject. Formats have to be machine-readable, structured, and commonly used. The GDPR does not provide recommendations on the specific format to be used to achieve data portability.

The right to data portability does not create an obligation for a data controller to adopt or maintain processing systems that are technically compatible with those of other organizations.

120 Article 20 GDPR.

Implementing data portability solutions can benefit SMEs in circumstances where such solutions would facilitate switches between service providers.

**EXAMPLE**

Structured, commonly used and machine-readable formats appropriate for data portability include CSV, XML, JSON or RDF.[121]

### Right to object

The data subject has the right to object when the processing is carried out by the data controller:

- on the basis of public interest or legitimate interest;
- for direct marketing purposes;
- in the context of information society services; and
- for scientific, historical or statistical purposes.[122]

When a data subject objects to processing in these circumstances, the data controller has to stop processing the respective personal data, unless they can demonstrate compelling legitimate grounds for the processing that override the rights of the data subject.

The controller can automate the exercising of the right to object.

**EXAMPLE**

Blocking cookies on a webpage is a way to object to the processing.

121 ICO, '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/.

122 Article 21 GDPR.

## Right to not be subject to a decision based solely on automated decision-making (or profiling)

**Automated decision-making** is the ability to make decisions by technological means without human involvement. Automated decisions can be based on any type of data. Examples of such data includes data provided directly by the individuals concerned (such as responses to a questionnaire); data observed about the individuals (such as location data collected via an application); derived or inferred data (such as a profile of the individual that has already been created, e.g. a credit score).[123]

**Profiling** is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

If such decisions have legal effects or produce significant effects, and therefore have a significant impact on the lives of individuals, the data subject has the right to not be subjected solely to these automated decisions.

**EXAMPLES**

A company relies on an automated system to calculate the annual bonus to be paid to its employees. The payment of a bonus produces significant effects on a person; it determines the amount of the annual bonus. Therefore, the final decision on the bonus must be scrutinized by a human.

123 Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (22 August 2018) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 8.

Unless a company is popular enough to receive thousands of job applications, it must not fully rely on automated recruitment systems. It must keep a human in the loop. The recruitment is deemed to produce significant effects on a person.

**USEFUL SOURCES**

» Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (22 August 2018) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053



## 2.6. The obligation to appoint a Data Protection Officer (DPO)

### 2.6.1. Background

With the adoption of the GDPR, both controllers and processors may be required to appoint a **Data Protection Officer** (DPO). The concept of a DPO is not a new one, and the WP29 previously argued that the DPO is a cornerstone of accountability.

### 2.6.2. Is the appointment of a DPO mandatory for SMEs?

In practice, the requirement to appoint a DPO will not typically apply to SMEs. At the same time, it should be noted that, contrary to a popular belief, it is not the size of a company that determines whether it has a legal obligation to appoint a DPO, but rather it is determined by the core data processing activities the organization conducts. These are the personal data processing activities essential to achieving the company's goals. The appointment of a DPO therefore concerns SMEs acting as either controllers

or processors. They may decide to opt for an internal (appointing a member of staff) or external (hiring in a DPO as a service) DPO.

The main role of a DPO is that of ensuring that the organization processes the personal data of its staff, customers, providers, or any other person in compliance with the applicable data protection rules.[124]

Having a DPO is mandatory in certain cases, where:

1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity.

This requirement may be applicable to SMEs that fall within the scope of the definition of public authorities. They include *l*egal persons governed by public law or by private law, which are entrusted, under the legal regime applicable to them, with the performance of services of public interest and which are, for this purpose, vested with special powers beyond those which result from the normal rules applicable in relations between persons governed by private law.[125]



**EXAMPLE**

If an SME provides services of a public nature, such as transport services, water and energy supply, road infrastructure, broadcasting, public housing, etc., then it may be considered to be a public authority. Determining if an SME is a public authority is important, as this may necessitate the appointment of a DPO.

2. the core activities of the SME consist of processing operations which, by their nature, their scope, and/or their purpose(s), require regular and systematic monitoring of data subjects on a large scale.

124 EDPS, 'Data Protection Officer' https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en.

125 See, for example, CJEU, Case C- 279/ 12, Fish Legal and Shirley, para. 42 and case law cited therein http://curia.europa.eu/juris/liste.jsf?language=en&num=C-279/12.

**Core activities** refer to the main business pursued by an SME. It may be that the core activity of the SME is inextricably linked with data processing (e.g. if the SME is an App developer). At the same time, certain data processing activities, while possibly being essential or necessary to a business, are considered ancillary (e.g. paying employees or having standard IT support activities).

**Monitoring** entails tracking individuals' usage of the internet.[126] The monitoring is **regular and systematic** when it is ongoing, or occurring at particular intervals of time, and is pre-arranged, organized, or methodical, taking place as part of a general plan for data collection or strategy.

Activities that may constitute regular and systematic monitoring of data subjects include: operating a telecommunications network; providing telecommunications services; email retargeting; data-driven marketing activities; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; webscraping; monitoring of wellness, fitness and health data via wearable devices.

The factors determining whether the processing is carried out on a **large scale** are the number of data subjects concerned (either as a specific number or as a proportion of the relevant population); the volume of data and/or the range of different data items being processed; the duration, or permanence, of the data processing activity; the geographical extent of the processing activity.

126 Recital 24 GDPR.

**EXAMPLES**

Large-scale activities encompass the processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards), and the processing of real-time geo-location data for statistical purposes by a processor specialized in providing these services.

A medium-sized tile manufacturing company subcontracts its occupational health services to an external processor, which has a large number of clients. The processor needs to designate a DPO because the processing is on a large scale. However, the manufacturer itself is not necessarily under an obligation to designate a DPO.[127]

3. the core activities of the SME consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Special categories of data are those listed in Article 9 of the GDPR. They include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation.

**EXAMPLES**

» A medical laboratory that performs blood tests must appoint a DPO.
» A law firm focusing on criminal trials or a health clinic – but not an individual lawyer or a health care professional – must appoint a DPO.[128]

127 Article 29 Working Party, 'Guidelines on Data Protection Officers ('DPOs') (13 December 2016) https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A 9.

128 Personal data should not be considered to be processed on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyers (Recital 91 GDPR).

» An SME running a dating app, which collects a barrage of sensitive data about its users, is required to have a DPO.

## 2.6.3. Who should be a DPO?

A DPO may either be an **employee of the SME** or an **external expert**. It is fundamental that a DPO is **independent**, and the following is ensured:

» the DPO shall be provided with all the necessary resources to carry out their tasks, in terms of money, time, workforce, time to devote to professional development, etc.;
» the DPO shall not receive instructions for the undertaking of their tasks;
» the DPO shall not be dismissed or penalized for the performance of their tasks;
» the DPO shall report to the highest level of management; and
» the DPO should not have any conflicts of interest in respect to other tasks and duties (e.g. determining objects and purposes of the processing, representing the SME in legal proceedings).

To ensure the independence of the function, at a practical level, an employee acting as a DPO must have no doubts regarding their role.

**SUGGESTION**

Within SMEs, individuals often perform multiple roles. A DPO role cannot be assigned to individuals acting as:

» chief executive officer;
» chief operating officer;
» chief financial officer;
» chief medical officer;
» head of marketing department;
» head of Human Resources; and
» head of IT department.

The level of expertise of a DPO needs to match the sensitivity, complexity and amount of data that an organization processes. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, a DPO may need a higher level of expertise and experience.

The GDPR neither imposes an obligation for certification of a DPO, nor does it encourage such certification voluntarily.

### 2.6.4. What tasks can be assigned to a DPO working for an SME?

The GDPR lists the following tasks that can be assigned to a DPO:

- **informing and advising** the SME on the obligations arising from the GDPR and other EU or national data protection provisions.
- **monitoring compliance** of the SME with the GDPR, other national and EU data protection provisions, and with the SME's own policies regarding the protection of personal data. The latter may concern assignment of responsibilities, awareness-raising and training of staff involved in personal data processing operations and auditing. Awareness raising and training can potentially reduce compliance costs (e.g. trained employees can handle personal data responsibly and take appropriate measures to prevent unauthorized access).

**EXAMPLE**

The DPO can collect information to identify processing activities; analyse and check the compliance of processing activities; inform, advise and issue recommendations to the controller or the processor.[129]

129 Footnote 128, 24.

The DPO themselves cannot be considered personally responsible for the controller or processor's non-compliance with data protection requirements.[130]

» **providing advice** where requested as part of **data protection impact assessments (DPIA) and monitoring** the performance of a DPIA;

**EXAMPLE**

An SME can ask a DPO to advise:

» if they should carry out the DPIA process;
» the method they should use to do it;
» whether to outsource the DPIA process or not;
» the risk mitigation measures they need to apply;
» whether the DPIA has been correctly carried out and if its conclusions (whether or not to go ahead with the processing and what safeguards to apply) comply with data protection requirements.[131]

The DPO cannot perform the DPIA themselves, as this task would be incompatible with the independence requirement. The DPO entrusted with the undertaking of the DPIA would combine the functions of an assessor and an auditor of the DPIA process. Nevertheless, the DPO can play a fundamental role in assisting the controller.

» **cooperating with the supervisory authority** (i.e. a DPA);
» acting as the **contact point for the supervisory authority** on issues relating to processing and consulting, where appropriate, with regard to any other matter;

130 Ibid.

131 Idem, 25.

**EXAMPLE**

When notifying a DPA of a data breach, the controller is required to provide the name and contact details of its DPO as a contact point.

However, the DPO cannot represent its SME in a court in case of proceedings about data protection compliance, as this would be incompatible with the independence required from this function.[132]

» **handling data subjects' requests and complaints**; and
» **fulfilling other tasks and duties**, providing that they do not result in a conflict of interests.

**EXAMPLES**

A DPO can be tasked with creating and maintaining a register of the processing activities, under the responsibility of the controller or the processor. Such records should be considered as one of the tools enabling the DPO to perform their tasks of monitoring compliance and informing and advising the controller or the processor.[133]

A DPO can provide advice on the data-sharing agreements to be concluded between controllers and processors, (joint) controllers or processors and sub-processors.

A DPO can help an SME to adhere to a code of conduct or to obtain a relevant certification.[134]

132 Garrido-Fontova, J., 'The DPO cannot represent the controller in proceedings before the authority according to the Greek DPA' (31 January 2020) https://quickreads.kemplittle.com/post/102fxw0/the-dpo-cannot-represent-the-controller-in-proceedings-before-the-authority-accor.

133 Korff, D. and Georges, M., *The DPO handbook - Guidance for data protection officers in the public and quasi–public sectors on how to ensure compliance with the European Union General Data Protection Regulation*, 152.

134 Idem, Tasks 10-11.

### 2.6.5. Can an SME share a DPO with other organizations?

Yes, appointing a joint DPO may be a practical solution for a group of SMEs. The GDPR allows for this, providing that the DPO is easily accessible from each establishment.

The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects, the supervisory authority, and, also, internally within the organization.

### 2.6.6. What should be considered before appointing a DPO?

- Even if not all SMEs have to appoint a DPO, it may be useful to have an expert in data protection working within the enterprise.
- When the SME is entrusted with the performance of services of public interest, even if it is not mandatory, it is recommended that the SME designates a DPO.[135]
- The level of expertise needed by a DPO depends on the risks arising from the processing operations.

**SUGGESTIONS**

Keeping written documentation explaining why an enterprise chose (not) to appoint a DPO, and why their level of expertise was deemed appropriate, may help an SME to demonstrate compliance in the event of an investigation by a DPA.

Similarly, when an SME decides to pursue an activity against the advice of the DPO, it should document the reasoning behind its decision. Maintaining such a record can demonstrate compliance with the GDPR in the event of an investigation by a DPA.

135 Footnote 129, 24.

Even if no legal obligation exists, companies can appoint a DPO or task a competent employee with this role on a voluntary basis to help with data protection compliance.[136]

### USEFUL SOURCES

- Article 29 Working Party, 'Guidelines on Data Protection Officers (DPOs)' (5 April 2017) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
- Korff, D. and Georges, M., The DPO Handbook - Guidance for data protection officers in the public and quasi–public sectors on how to ensure compliance with the European Union General Data Protection Regulation (2019) https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook. pdf/a5bfc9ba-8a0c-0f88-9874-71be40be6a6d?version=1.0

### RELEVANT DPA DECISIONS

A German SME active in the telecommunications sector was fined by the Federal DPA because it did not comply with the legal requirement under Article 37 of the GDPR of appointing a data protection officer despite repeated requests to do so. The fine of EUR 10,000 was deemed to be proportionate, taking into account that the company is a micro-enterprise.[137]

136 STAR Training materials: Topic 5 – Role of the DPO.

137 EDPB, 'BfDI imposes Fines on Telecommunications Service Providers' (18 December 2019) https://edpb.europa.eu/news/national-news/2019/bfdi-imposes-fines-telecommunications-service-providers_es.

# 3. The theory and practice of a risk-based approach

## 3.1. Background

A risk-based approach to personal data protection builds upon the idea that respecting data protection principles is not in itself sufficient to protect the fundamental rights and freedoms of individuals.[138] There are many, many ways in which personal data might be processed, and the reality of data processing can be complex. For this reason, compliance with the data protection principles needs to be supplemented with risk analysis and the management of risks.[139] In other words, the risk-based approach aims to give data protection principles more substance and to tailor them to specific and evolving data processing situations.[140]

While there is uncertainty surrounding the meaning of risk within the GDPR, **following the risk-based approach, data controllers and processors are required to assess and act upon risks to individuals arising from personal data processing activities**. This may include a series of coordinated activities to evaluate, control and mitigate risks.[141]

138 Principles related to the processing of personal data are listed in Article 5 of the GDPR and encompass: lawfulness; fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality.

139 Gellert, R., 'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection' (2016)2 EDPL 481, 482, 483, 484.

140 Ibid.

141 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' (3 October 2017) http://ec.europa.eu/newsroom/document.cfm?doc_id=47711 6.

The four basic steps of risk management are:

1. identification
2. analysis
3. evaluation
4. treatment.[142]

## 3.2. What is a risk in the GDPR?

The understanding of 'risk' in law – and specifically in European data protection law – is still evolving.[143] To date, talking about or working with 'risk' was more common in the areas of finance, technology, economics and natural sciences. In general, risk evaluation can be 'subjective'[144] and 'objective',[145] as well as voluntarily undertaken,[146] societally imposed,[147] discrete and pervasive.[148] Any risk can be evaluated from different perspectives (e.g. technological, economics, psychological).[149]

The perception of risk is variable, being affected by different attitudes, how information is given and portrayed, and the familiarity of the person with an activity or hazard.[150] Other elements that can play a role are the degree to which an individual feels in control, whether an individual is exposed to an activity voluntarily, or the perceived benefits of an activity.[151]

142 ISO 31000:2018(en), Risk management – Guidelines https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en.

143 Beck, U., *World at Risk* (Polity 2009) 6.

144 Subjective risk assessment entails non-expert perceptions by the public.

145 Objective risk is assessed scientifically by experts and is probabilistic.

146 For example, by taking some medication, such as contraception.

147 For example, a nuclear power plant.

148 The latter includes risks that are bound to happen, such as an earthquake.

149 Baldwin, R. and Cave, M., *Understanding Regulation: Theory, Strategy, and Practice* (OUP 1999) 139.

150 Slovic, P., 'Perception of Risk', *Science*, 236.4799 (1987) 280-85 https://doi.org/10.1126/science.3563507.

151 Ibid.

The GDPR does not contain a definition of `risk' but the WP29 suggests that **'a 'risk' is a scenario describing an event and its consequences, estimated in terms of severity and likelihood'.**[152]

More specifically, in data protection law, risks relate to **threats to the rights and freedoms of individuals whose personal data is being processed** (i.e. data subjects) or natural persons in more general terms. Such threats are not limited to the right to protection of personal data or privacy, but involve other fundamental rights, such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience, and religion.[153] This understanding of risk is quite different to other forms of business risk, where the risk is assessed with reference to the firm.

**EXAMPLE**

Keeping the medical records of a patient accurate and up to date is not just a matter of data accuracy. Inaccurate or outdated information in a medical record can prejudice the health or the life of the patient, creating a risk to their rights and freedoms.

## 3.3. What does cause risks?

Risks to the rights and freedoms of natural persons may result from personal data processing activities that could lead to physical, material, or non-material damage to an individual.[154]

152 Footnote 141, Ibid.

153 Ibid.

154 Recital 75 GDPR.

**EXAMPLES**

Personal data processing activities can cause risks 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, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage;
- data subjects might be deprived of their rights and freedoms, or prevented from exercising control over their personal data;
- personal data is processed in a way that reveals 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;
- 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;
- personal data of vulnerable natural persons, in particular of children, are processed; or
- processing involves a large amount of personal data and affects a large number of data subjects.[155]



155 Recital 75 GDPR.

**SUGGESTIONS**

To identify risks, an SME may, for example:

» seek advice from its DPO, if it has appointed one;

» consult knowledge bases;[156] and/or

» perform interviews and brainstorming with relevant stakeholders.[157]

## 3.4. How can risks under the GDPR be evaluated?

Under the GDPR, different risk levels trigger the application of legal requirements. The Regulation distinguishes at least three types of risk situations affecting the rights and freedoms of individuals deriving from the processing operations:

1. low-risk situations;
2. risky situations; and
3. high-risk situations.

One company can have multiple processing operations of personal data in place, and they may each have different risk levels associated with them.



156 CNIL, 'PIA Knowledge bases' (2018) https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf.

157 Ball, H., '7 Ways to Identify Risks' https://projectriskcoach.com/7-ways-to-identify-risks/.

**EXAMPLES**

As a general rule, from a data protection perspective, certain business sectors are presumed to be riskier than others, for example: health care services; solvency and creditworthiness; creation and use of profiles (profiling); political, trade union and religious activities; telecommunications services; insurances; banking and financial companies; social services activities; advertising; large-scale CCTV (Closed Circuit TV or video surveillance of major infrastructures such as railway stations or shopping centres).

Similarly, the processing of certain types of data entails high risks, for example: personal data revealing ethnic or racial origin; political opinions or religious beliefs data; trade union membership data; genetic data; biometric data for the purpose of uniquely identifying a natural person; data concerning physical or mental health; data concerning a natural person's sex life or sexual orientation; personal data relating to criminal convictions and offences; geolocation data.

Also, certain types of processing operations entail risks, for example: creating or analysing profiles; large-scale advertising and trade promotion to potential clients; provision of services for the operation of public networks or electronic communications services (Internet Service Providers, ISPs); management of associates or members of political parties, trade unions, churches, religious confessions or communities, charities and other non-profit organizations with a political, philosophical, religious or trade union purpose; management, sanitary control or supply of medicines; health or sanitary history).[158]

Other sectors and activities might still be high-risk, but these areas have historically had a tendency to raise risks and cause problems for people so are considered to be high-risk by default.

158 AEPD, 'Facilita RGPD' https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd.

Typically, the risk level is assessed by combing the likelihood or probability (of the risk to materialize) and the severity (of the consequences due to the materialization of the risk).[159] The GDPR specifies that likelihood and severity are to be determined considering: nature (i.e. inherent characteristics or type), scope (scale and range), context (i.e. circumstances), and purposes (i.e. aims) of the processing operations.[160]

Risk can be assessed qualitatively or quantitatively, or by combining the two. Quantitative risk assessment requires very precise values, namely the definition of the probability of each single risk factor's occurrence (expressed in a scale 0-1), and the quantitative definition of its severity. Qualitative risk assessment, in turn, assumes the impossibility of attaining such precise values, and expresses likelihood and severity in scales. In most cases, the risks to the rights and freedoms of natural persons are suited to qualitative evaluation.[161]



159 Rossi, P., 'How to Link the Qualitative and the Quantitative Risk Assessment', in PMI® Global Congress—EMEA, 2007 https://www.pmi.org/learning/library/link-qualitative-quantitative-risk-assessment-7375; Kloza, D. et al., 'Data protection impact assessment in the European Union: developing a template for a report from the assessment process' (2020) d.pia.lab Policy Brief https://cris.vub.be/en/publications/data-protection-impact-assessment-in-the-european-union-developing-a-template-for-a-report-from-the-assessment-process(2300a8d5-7e5d-4e63-86cb-51288e2eaca4).html.

160 Recital 76 GDPR; European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (13 November 2019) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf para 27.

161 Footnote 159.

## EXAMPLE

For qualitative risk assessment, an exemplary severity scale of 1-5 could be:[162]

| Value | Severity of impact on rights and freedom of data subjects |
|---|---|
| **S1** | Low - Mere inconvenience/Annoyance |
| **S2** | Moderate - Minor physical, material or non-material damage to rights and freedoms of data subjects (e.g. stress, feeling of loss of control of personal data, minor economic loss, etc.) |
| **S3** | Medium - Physical, material or non-material damage to rights and freedoms of data subjects (e.g. restrictions to exercising rights) |
| **S4** | High - Significant physical, material or non-material damage to rights and freedoms of data subjects that can only be overcome by data subjects with difficulty |
| **S5** | Critical - Irreversible physical, material or non-material damage to rights and freedoms of data subjects |

Whereas a likelihood scale 1-5 could be:[163]

| Value | Likelihood of occurrence |
|---|---|
| **L1** | Remote - it does not seem possible that the selected risk sources will materialize |
| **L2** | Unlikely - it seems unlikely that the selected risk sources will materialize |
| **L3** | Occasional - it seems possible that the selected risk sources will materialize |
| **L4** | Likely - it seems highly possible that the selected risk sources will materialize |
| **L5** | Frequent - it is almost certain that the selected risk sources will materialize |

162 As interpreted from CNIL, 'PIA Knowledge bases' (2018) https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf.

163 Ibid.

The corresponding risk matrix could be:

| | | | | | |
|---|---|---|---|---|---|
| L5 | 5 | 10 | 15 | 20 | 25 |
| L4 | 4 | 8 | 12 | 16 | 20 |
| L3 | 3 | 6 | 9 | 12 | 15 |
| L2 | 2 | 4 | 6 | 8 | 10 |
| L1 | 1 | 2 | 3 | 4 | 5 |
| | S1 | S2 | S3 | S4 | S5 |

**Risk level or magnitude** (obtained by multiplying likelihood and severity)

Low risk – ≤ 2;
Moderate risk – between 3 and 4;
Medium risk – between 5 and 9;
High risk – between 10 and 16;
Critical risk – ≥ 17.

These scales and risk matrix are only to be seen as indicative. Controllers may establish different scales (e.g. 1-3, 1-4). In the risk matrix, they can identify different values for low risk, moderate risk, etc. (e.g. low risk ≤ 1, critical risk ≥ 25).

An example of a data protection risk registry:[164]

| ID | Risk description | GDPR provision | Description of possible impact on data subjects | Likelihood | Severity | Magnitude[165] | Explanation and remediation |
|---|---|---|---|---|---|---|---|
| 1 | Unauthorized repurposing | Art. 5 | Personal data is processed for purposes other than those originally identified | 2 | 4 | 8 | |
| 2 | | | | | | | |
| ... | | | | | | | |

164 Inspired by the AEPD 'Practical Guide for DPIAs' https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf 23, 33.

165 Magnitude = Likelihood X Severity.

## SUGGESTION

Keep a registry of risks related to the processing operations presents several advantages. First, going through the process of completing it raises awareness in an organization as to potential data protection issues associated with a project, and allows identification and mitigation of data protection risks. It also supports the choice of the most appropriate technical and organizational measures to ensure data security and data protection by design. Second, it can facilitate the performance of a data protection impact assessment (DPIA) when required, and may help an organization to demonstrate compliance with the law in the event of a regulatory investigation or audit.[166]

## USEFUL SOURCES

- ISO 31000:2018 Risk management — Guidelines https://www.iso.org/standard/65694.html
- ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management https://www.iso.org/standard/75281.html
- Finish Office of the Data Protection Ombudsman, 'Risk assessment and data protection planning' https://tietosuoja.fi/en/risk-assessment-and-data-protection-planning
- AEPD, 'Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales sujetos al RGPD' https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf

166 DPC, 'Risk-based approach': https://dataprotection.ie/en/organisations/know-your-obligations/risk-based-approach.

## 3.5. What are the provisions embedding a risk-based approach in the GDPR?

The risk-based approach is embedded in the following GDPR provisions:

- Article 24 on the responsibility of the controller (which is related to the principle of accountability);
- Article 25 on data protection by design and by default;
- Article 30 on the obligation for documentation (records of processing activities);
- Article 32 on the security of processing;
- Articles 33 and 34 on personal data breach notifications;
- Article 35 on the obligation to carry out an impact assessment (DPIA); and
- Article 36 on prior consultation.

While the formulation of the risk-based approach varies to some degree in the above-listed articles, in essence, it aims to ensure that, **whatever the level of risk involved in the processing of personal data, data protection principles and data subjects' rights are respected.** In practice, this means that the data controllers and processors need to **adjust the data protection obligations to the risks presented by a data processing activity.**[167]

Typically, the risk-based approach is conceptualized in the GDPR through the following elements:

- current standards (in terms of technical and organizational measures) for the means of processing;
- the cost of implementation;
- the nature, scope, context of the processing;
- purposes of the processing; and
- risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.[168]

167 Kuner, C., Bygrave, L. and Docksey, C., *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020) 26.

168 Footnote 160, 9.

The risk and the assessment criteria are the same: **the assets to protect are always the same (the individuals, via the protection of their personal data), against the same risks (to individuals' rights and freedoms), taking into account the same conditions (nature, scope, context and purposes of processing).**[169]

## 3.6. How can a risk-based approach benefit SMEs?

Risks for data subjects do not depend on the size of the controllers, but on the nature, scope, context and purpose(s) of the processing operations.

Considering compliance with the GDPR through the lens of a risk-based approach is particularly useful for SMEs for the following reasons:

- SMEs enjoy certain freedom in determining the techniques to be used to perform the risk analysis and to evaluate the level of risk of the processing operations. Likewise, SMEs are free to choose the measures to mitigate such (high) risks;
- It allows flexibility when adhering to data protection requirements. It does not prescribe or demand a particular measure to comply with the law. Instead, it requires that the SME understands the data processing operation by considering its nature, scope, context, and purposes, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons whose personal data is being processed. In practice, this means that the GDPR grants SMEs enough margin to customize technical and organizational solutions to their specific needs.[170]

169 Ibid.

170 Footnote 14.

» It allows to overcome, to a certain extent, the one-size-fits-all approach. The measures to be adopted by an SME that only performs low-risk data processing can be far more limited than those to be adopted by an SME whose business activities are based on high-risk data processing operations in order to comply with the GDPR.

Although the risk-based approach is easy to identify in the text of the GDPR, it can still be tricky to apply in practice. As suggested by the European regulators, the risk-based approach may include the use of baselines, best practices, and standards. These might provide a useful toolbox for controllers to tackle similar risks in similar situations (situations determined by the nature, scope, context and purpose(s) of the processing). It is therefore worth understanding what practices and solutions already exist in your industry or field.

## 3.7. A risk-based approach in practice

### 3.7.1. Responsibility of the controller and the principle of accountability

#### Background

The accountability principle establishes that 'the controller shall be responsible for, and be able to, demonstrate compliance with' the other principles relating to the processing of personal data and the GDPR. Processors are also expected to be accountable, as they have to comply with obligations related to accountability and assist the data controller in a number of their compliance requirements.[171] Hence, the principle is relevant for any SME, regardless of their role in the processing operations.

171 For example, processors have to keep a record of the processing activities (Article 30(2) GDPR); appoint a DPO in certain situations (Article 37 GDPR); implement technical and organizational measures to ensure the security of processing (Article 32 GDPR). See FRA/ECtHR/EDPS, *Handbook on European data protection law* (Publications Office of the European Union 2018) 135, 136.

In the field of data protection and privacy, accountability is considered to be a form of enhanced responsibility[172] or a proactive demonstration of an organization's capacity to comply with the GDPR.[173] Accountability can boost transparency and confidence for both data subjects and regulators, and ensure greater transparency of business practices.[174]

The actual recognition of the principle of accountability within the GDPR marks a shift from a primarily reactive approach to proactive compliance and practice.[175] Whereas (mere) compliance entails that an SME meets certain rules, the accountability principle goes further: SMEs have to actively demonstrate their commitment to protecting personal data.[176] For example, a risk assessment, or the evaluation of the 'appropriateness' of technical and organizational measures, cannot be reduced to mere 'box-ticking' exercises.[177]

## What does an SME need to do to be accountable?

An SME acting as a data controller is responsible for implementing appropriate technical and organizational measures, including data protection policies, to ensure and demonstrate that its processing activities are compliant with the requirements of the GDPR.



172 Bennett, C., 'The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats' in Guagnin, D. et al. (eds.), *Managing Privacy through Accountability* (Springer 2012) 46.

173 Alhadeff, J., van Alsenoy, B. and Dumortier, J., 'The accountability principle in data protection regulation: origin, development and future directions', in Guagnin, D. et al. (eds.), *Managing Privacy through Accountability* (Springer 2012).

174 Ibid.

175 De Hert, P. 'Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law' in Guagnin, D. et al. (eds.), *Managing Privacy through Accountability* (Springer 2012).

176 Ibid.

177 Kloza, D. et al., 'Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals' (2017) d.pia.lab Policy Brief https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf.

When taking such measures, the controller has to consider the nature, scope, context, and purposes of the processing, as well as the risks to the rights and freedoms of natural persons, of varying likelihood and severity.[178]

Even an SME acting as a processor has to provide sufficient guarantees of implementing appropriate technical and organizational measures in a way that facilitates the processing's meeting of the requirements of the GDPR and ensuring of the protection of the rights of data subjects.[179]

**SUGGESTION**

Keeping written documentation about the technical and organizational measures in place that explains why the measures were chosen is an effective way to demonstrate compliance with the law.

## What are the other examples of accountability measures?

A (non-exhaustive) list of accountability measures includes:

- adopting and implementing data protection policies at the organizational level of an SME;
- implementing the principles of data protection by design and default (Article 25),
- concluding written agreements between (joint) controllers, controllers and processors, and processors and sub-processors, specifying reciprocal roles and responsibilities;
- maintaining documentation of the processing activities (Article 30);
- implementing appropriate security measures (Article 32);
- maintaining a procedure to respond to requests for access to personal data;
- publishing privacy notices online;

178 Article 24 GDPR.

179 Article 28(1) GDPR.

- having a data protection incident response plan in place (Article 35);
- recording and, where necessary, reporting personal data breaches to DPAs and data subjects;[180]
- carrying out data a protection impact assessment (DPIA) (Article 35);
- adhering to codes of conduct, which focus on the proper application of the GDPR in different processing sectors and different kinds of enterprises; and
- adhering to certification mechanisms, seals and marks, which promote different organizations' compliance with GDPR requirements.[181]

These (accountability) measures need to be continuously revised and updated to reflect the reality of the processing operations. Hence, accountability requires a continuous effort from controllers and processors.

### What are the advantages of accountability for an SME?

The accountability principle focuses on taking measures that deliver real protection in practice. Adhering to this principle provides incentives for businesses to keep their data in order[182] and to keep track of the data processing operations occurring within an organization. Furthermore, it may foster the implementation of innovative technical and organizational measures, including data protection notices, within an SME.

Finally, accountability of a controller can increase levels of trust between SMEs and their clients, creating a competitive advantage. An SME can show how it is doing the right thing with regard to customers' data.



180 Articles 33 and 34 GDPR.

181 EDPB, 'Accountability tools' https://edpb.europa.eu/our-work-tools/accountability-tools_en.

182 Vera Jourová 'Speech at the 'Computers, Privacy and Data Protection' Conference 2019' SPEECH/19/787 https://ec.europa.eu/commission/presscorner/detail/fr/SPEECH_19_787.

**USEFUL SOURCES**

» Article 29 Working Party, 'The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data' (1 December 2009) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

» Article 29 Working Party, 'Opinion 3/2010 on the Principle of Accountability' (13 July 2010) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

## 3.7.2. Data protection by design and data protection by default

### Background

With the entry into force of the GDPR, the principles of Data Protection by Design and Data Protection by Default (DPbD and DPbDf) became legal obligations for controllers.

**RELEVANT DPA DECISION**

The Baden-Württemberg DPA issued a fine of EUR 20,000 to an SME operating a chat portal for failing to take appropriate technical and organizational measures. The passwords of the users were stored in plain text and not as a hash value. This resulted in a data theft of 333,000 users.[183]

183 Cf. (in German) 'LfDI Baden-Württemberg verhängt sein erstes Bußgeld in Deutschland nach der DS-GVO' (22 November 2018) https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/.

The underlying objective of DPbD and DPbDf obligations is to integrate privacy throughout the lifecycle of various technologies and applications that process personal data. At the same time, the practical implementation of DPbD and DPbDf is tremendously complex because of the uncertainty surrounding the meaning of these principles.[184]

This approach is an advantage for SMEs. They are not bound to adopt predefined measures to comply with DPbD and DPbDf principles, but can instead adopt customized solutions.

### What does data protection by design entail?

The principle of data protection by design requires the controller to implement both organizational and technical measures to ensure that the requirements of the GDPR are embedded in the processing activity, in an effective manner, at the time of its initiation, as well as in its later stages (including tenders, outsourcing, development, support, maintenance, testing, storage, deletion, etc.). It is an expression of a lifecycle thinking applied to the processing activity.[185] The idea here is to avoid the design of a practice, process, service or product that involves personal data, with an attempt to 'bolt on' data protection subsequently being made as an afterthought.

When implementing data protection by design, the controller has to take into account:

» the nature (i.e. the inherent characteristics of the processing operations), the scope (scale and range (e.g. if they concern sensitive data) of the processing operations), the context

184 Veale, M., Binns, R. and Ausloos, J., 'When data protection by design and data subject rights clash' (2018) https://doi.org/10.1093/idpl/ipy002. Jasmontaite, L., Kamara, I., Zanfir-Fortuna, G., & Leucci, S. Data Protection by Design and by Default: European Data Protection Law Review 4(2) (2018) https://doi.org/10.21552/edpl/2018/2/7

185 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 3-4.

(circumstances of the processing) and the purposes/aims of the processing;[186]
- the current standards and capabilities of the existing technical and organizational measures, which can vary greatly;
- their cost of implementation, including money, time and human resources; and
- the risks of varying likelihood and severity to the rights and freedoms of natural persons deriving from the processing operations.

In particular, the controller must:
- implement appropriate technical and organizational measures and necessary safeguards into the processing. An example of such a measure (the only one mentioned in the GDPR) is pseudonymization;
- implement data protection principles[187] and integrate the necessary safeguards into the processing to meet the requirements of the Regulation and protect the rights of data subjects.[188] Another example of the 'by design' approach is the performance of a DPIA;[189]
  - in an effective manner; and
  - at the time of the determination of the means for processing, at the time of the processing itself, and also with a view to the phase following its conclusion (lifecycle thinking).

The technical or organizational measures referred to in Article 25 can be anything – from the use of advanced technical solutions to the basic training of personnel on how to handle personal data (of customers, colleagues, etc.) – that could be done by the DPO. Yet, some DPAs (e.g. the DPC) expect as a minimum the implementation of encryption as a technical solution, whenever possible, where personal data is stored or moved.

186 Footnote 160, para 27.

187 Article 5 GDPR.

188 Chapter III Rights of the data subject GDPR.

189 Footnote 184, para 10.

There is no requirement for sophisticated measures, as long as they are appropriate for implementing the data protection principles effectively.[190] This means unfortunately, that there are no specific measures that automatically ensure compliance with the GDPR.

To comply with DPbD and DPbDf, an SME may consider implementing Privacy Enhancing Technologies (PETs).

PETs encompass a wide range of solutions, incorporating both traditional data security technologies (e.g. anonymization, encryption cryptography, for personal data both being stored or moved) and other tools aimed at a more general strengthening of data protection: for example, antitracking tools for web browsing, dashboards and other user interfaces for the management of consent can be considered, as well as tools that enable data subjects to audit the enforcement of the data protection policy of a controller or to customize the terms and conditions of privacy policies.[191]

The use of PETs may create a competitive advantage for SMEs that seek to attract data-protection-aware clients.

Furthermore, the development of new PETs may represent a business opportunity for SMEs. Even if DPbD is only a legal obligation for controllers, producers of the products, services, and applications for which the processing of personal data is a central component should be encouraged to take into account the right to data protection when developing and designing such products, services, and applications,

190 Footnote 160, para 9.

191 See Kenny, S., 'An introduction to Privacy Enhancing Technologies' (1 May 2008) https://iapp.org/news/a/2008-05-introduction-to-privacy-enhancing-technologies/; 'Privacy Enhancing Technologies – A Review of Tools and Techniques' https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/; and Shen, Y. and Pearson, S., 'Privacy Enhancing Technologies: A Review' https://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf.

in order to ensure that controllers and processors can fulfil their data protection obligations.[192]

ENISA is currently working on establishing a PET repository and a tool to assess the maturity of these technologies.[193]

### How to evaluate the appropriateness and effectiveness of data protection by design measures?

The appropriateness of the measures is strongly related to their effectiveness. Effectiveness means that controllers must be able to demonstrate that the measures chosen are suitable to achieve the goals of DPbD, having regard to the actual processing operations.

It is therefore not enough to implement generic measures solely to document DPbD compliance; each implemented measure must have an actual effect.[194] The measures should be robust and be able to be scaled up in accordance with any increase in risk of non-compliance with the data protection principles.

To demonstrate the effectiveness of the measures adopted, controllers may opt for the use of key performance indicators to merge the business objectives of SMEs with the data protection ones.

**EXAMPLE**

To establish SMART (Specific, Measurable, Attainable, Relevant, Time-bound) key performance indicators (KPIs) in terms of data protection by design measures, it is important that an SME considers:

» What is the desired outcome pursued with the measure (e.g. grant clients/data subjects more privacy and demonstrate compliance with the GDPR)?

192 Recital 78 GDPR.

193 ENISA, *ENISA's PET maturity assessment repository* (2019) https://www.enisa.europa.eu/publications/enisa2019s-pets-maturity-assessment-repository.

194 Footnote 160, para 14.

- Why does the desired outcome matter (e.g. to have a competitive advantage compared to other SMEs providing similar services, or avoid sanctions)?
- How will the progress be measured?

KPIs may include metrics. Metrics may be quantitative, such as the reduction of the level of risk related to the processing operations (e.g. from high to medium); the reduction of complaints of data subjects (e.g. indicate that, after the adoption of the measure, the number of complaints has been reduced by X%); the reduction of response time when data subjects exercise their rights (e.g. indicate that, after the adoption of the measure, the response time has been reduced by X%); or qualitative, such as the evaluations of performance (performed by e.g. the DPO (when appointed) or an external audit company); the use of grading scales, or expert assessments. Alternatively, controllers may provide the rationale behind their assessment of the effectiveness of the chosen measures and safeguards, but they will be held accountable for this.

When establishing and defining KPIs, an SME may consider:

- How to reduce risks of ongoing personal data processing operations (e.g. adopting PETs or recruiting additional staff)?
- Who are the responsible staff for implementing KPIs?
- What are the business objectives of your target (e.g. the reduction of data subjects complaints by X%)
- How often to review progress and readjust KPIs?[195]

Adherence to certifications, although this does not ensure the effectiveness of the measure *per se,* can be used as a support to demonstrate compliance.

195 Badawya, M. et al., 'A survey on exploring key performance indicators' (2016)1 FCIJ, 47-52; 'What is a KPI?' https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator.

## What does data protection by default entail?

Controllers shall also implement appropriate technical and organizational measures ensuring that, by default, only the personal data that is necessary for each specific purpose of the processing is processed.

A 'default', as commonly defined in computer science, refers to the pre-existing or preselected value of a configurable setting that is assigned to a software application, computer program, or device. Such settings are also called 'presets' or 'factory presets', especially for electronic devices.[196] Hence, 'data protection by default', in technical terms, refers to the choices made by a controller regarding any pre-existing configuration value or processing option that is assigned in a software application, computer program, or device that has the effect of adjusting, in particular, but not limited to, the amount of personal data collected, the extent of its processing, and the period of its storage.

The idea here is that, typically, a data subject making default choices should have their data adequately protected.

## What are some examples of measures implementing data protection by default?

To implement technical measures putting in practice data protection by default, SMEs can, for example:

» customize the personal data to be provided by their clients depending on the services requested (which affects the amount of personal data collected);

196 Footnote 160, para 39.

**EXAMPLE**

If a bookshop considers also selling books online, both in paper and in e-book formats, it presents customers with different versions of its order page. If it provides access to a digital book, it does not need to know the physical address of the customer.

» adopt clear policies concerning data deletion (i.e. affecting the period of storage);

**EXAMPLE**

A sports centre is required by law to ask clients to provide medical authorization for enrolment. The certificates should be destroyed as soon as the membership expires (unless otherwise required by law).

» avoid pre-ticked boxes that nudge the clients to accept the provision of extra services (i.e. affect the extent of processing).

**EXAMPLE**

When setting up cookies on its website, a company avoids pre-ticking the boxes for unnecessary cookies.

To implement organizational measures aimed at data protection by default, SMEs can establish access control policies governing employee access to personal data. This means limiting the number of employees who can have access to personal data based on an assessment of necessity, and also ensure that personal data is accessible to those who need it when necessary.

## EXAMPLES

A company may consider preventing access to clients' data by its human resources department because this is not necessary for the performance of their tasks.

A hotel manager may not disclose the contact details of guests to the cleaning or restaurant staff, as this is not necessary for them to perform their job.

## USEFUL SOURCES

- ENISA, ENISA's PET maturity assessment repository (2019) https://www.enisa.europa.eu/publications/enisa2019s-pets-maturity-assessment-repository
- 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
- European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (13 November 2019) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

### 3.7.3. Records of processing activities and other documentation

#### Background

Keeping a record of processing activities is a very useful means to understand the implications of any processing, whether existing or planned. The record facilitates the factual assessment of the risk to individuals' rights of the processing activities performed by a controller or processor, and the identification and implementation of appropriate security measures to safeguard personal data.

For many micro-, small-, and medium-sized organizations, where data processing does not represent the core business, maintaining a record of processing activities may not necessarily be a burdensome activity. Conversely, it could be a tool to strengthen the good governance of an SME. Good records help in the preparation of an accurate data protection notice and provision of information to data subjects.

#### What does documentation require?

Both controllers and processors are required to keep records of their processing activities, albeit with some differences. Documentation requirements for processors are less extensive.

**EXAMPLE**

The documentation, for SMEs acting as controllers should include information about the following:

- the name and contact details of the controller/representative/DPO;
- the purpose(s) of the processing;
- the categories (e.g. clients, employees, etc.) of data subjects and personal data processed (e.g. contact details, unique identifiers, social security number, etc.);
- the categories of recipients (e.g. marketing service providers) with whom the data may be shared, specifying if they are outside the European Economic Area (EEA) or an international organization;

» in the case of international data transfers (sending personal data outside the EEA), the identification of the country outside the European Economic Area or the international organization to which personal data is transferred;
» where possible, the applicable data retention periods; and
» where possible, a description of the security measures (e.g. encryption) implemented in respect to the processed data.

For SMEs acting as processors, the information must include:

» the name and contact details of the processor/representative/DPO/controller on behalf of which the processor is acting;
» categories of processing carried out on behalf of the controller;
» in the case of international data transfers, the identification of the country outside the European Economic Area or the international organization to which personal data is transferred; and
» where possible, a description of the security measures implemented in respect to the processed data.

**SUGGESTION**

Although not expressly required, it is best practice to also include in the register the legal basis governing the processing of personal data or its transfer to countries outside the EEA.[197] The register may also include written data-sharing agreements between the (joint) controller(s), the controller and the processor, the processor and the sub-processor.

The GDPR does not explicitly require controllers to maintain detailed records of all data transfers. Yet, keeping documentation falls under scope of the principle of accountability, and allows the controller to demonstrate the lawfulness of data processing. This obligation can be best met by recording all the details of personal data transfers. This also supports the notification of recipients if data needs to be rectified or erased in order to enact a data subject's rights.

197 See Section 2.4 What are the possible legal bases for personal data processing?

When discussing documentation, several alternative terms are used, such as, an inventory, a register, and a data management plan. Upon request, these records must be disclosed to the supervisory authority (DPA). Keeping accurate documentation of processing activities can be useful for an entity if it needs to demonstrate compliance.

The documentation of processing activities must be kept in writing.[198] The controller (and the processor) chooses whether to keep such records in paper or electronic form.

**SUGGESTION**

Maintaining documentation electronically has the advantage of allowing it to be easily modified by addition, removal and amendment. Paper documentation is, however, regarded as appropriate for SMEs and micro-enterprises.

In principle, SMEs are exempted from the obligation to keep a register of processing activities when:

- the processing is not likely to result in a risk to the rights and freedoms of data subjects;
- the processing is occasional (i.e. not regularly/frequently undertaken); or
- the processing does not include special categories of data or personal data relating to criminal convictions and offences.

In practice, however, most SMEs will have to keep documentation of data processing activities.

198 Based on the opinions and guidance provided by the UK DPA (ICO), the French DPA (CNIL) and the Irish DPA.

**EXAMPLES**

A paper factory regularly processes personal data in the context of sales and HR. Even if the company has fewer than 250 staff, it must still document these types of processing activities, because they are not occasional. Furthermore, most employees' files include special categories of personal data.

An insurance company occasionally carries out an internal staff engagement survey. Since the company does not perform this particular processing activity often, it does not need to document it as part of its record of processing activities. However, if the company occasionally performs profiling activities across its customer database, for insurance-risk classification, then the company must document such processing. This processing entails profiling – a risky processing operation.[199]

A tattooist may be legally required to ask for their clients' medical certificates before tattooing them. In this case, the tattooist keeps a record of the processing activities concerning the health-related data of their clients.

A commercial activity (e.g. bar, pub, restaurant, hairdresser, beautician) with at least one employee keeps a record of processing activities in relation to the processing of the employee's data.[200]



199 'Who needs to document their processing activities?' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/who-needs-to-document-their-processing-activities/#who2.

200 'FAQ sul registro delle attività di trattamento' https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento.

**SUGGESTION**

Even for SMEs falling within the exemption, it would be convenient to maintain a record of the occasional processing activities. This way, it would be much easier for them to cooperate with DPAs if an investigation is initiated, and to demonstrate compliance with GDPR requirements.[201]

Processors and controllers can put in place a single set of shared records that they can quickly make available to the DPA upon request. If an organization simultaneously acts as both controller and processor for a particular activity, the records may be split up to correspond to those respective roles.[202]

## What are the other types of documentation required by the GDPR?

Other than keeping a record of the processing activities, other types of documentation should also be kept in writing. These support processors and controllers in their duty of demonstrating their accountability and compliance with the GDPR.

Some are expressly required by the GDPR, others are best practices. For example:

- keeping a registry of data protection risks;
- concluding written agreements between (joint) controllers, controllers and processors, and processors and sub-processors, specifying reciprocal roles and responsibilities;
- keeping track of DPO advice (e.g. mail, written opinions, etc.);
- keeping track of the decision on the (non-)appointment of a DPO;

201 APD-GBA, 'Recommandation n° 06/2017 du 14 juin 2017' www.autoriteprotectiondonnees.be/publications/recommandation-n-06-2017.pdf.

202 Ibid.

- keeping track of the technical and organizational measures adopted in the various phases of the processing operations;
- keeping track of the DPIA process;
- keep track of data breaches, including the reasons leading to such a breach, its effects, and the remedial action(s) taken;
- keeping track of the measures taken in order to ensure the rights of the data subjects;
- keeping track of the measures taken in order to meet the principles of data processing; and
- keeping track of the legal bases and reviews of these.

## USEFUL SOURCES

- European Data Protection Supervisor, 'Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies' https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en

**Templates of registers of processing activities**

- ICO https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/
- CNIL https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement
- Korff, D. and Georges, M., The DPO handbook - Guidance for data protection officers in the public and quasi–public sectors on how to ensure compliance with the European Union General Data Protection Regulation (2019) https://www.dpoprof.it/pdf/normativa/THE%20DPOHANDBOOK.pdf 158

**SUGGESTION**

When downloading a template for documentation purposes prepared by a DPA, an SME should consider whether it acts as a controller or as a processor within the particular processing operation(s), as the information required will differ.

## 3.7.4. Security of processing

### Background

Controllers and processors are requested to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Such measures may include, but are not limited to, the following:

- the pseudonymization and encryption of personal data;
- 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;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

### How is the security obligation related to other provisions?

Security obligations also require the controller wishing to engage a processor under contract to undertake due diligence and assess whether the guarantees offered by the processor are sufficient. A controller must only engage a processor where they have faith in their ability to comply with the obligations under GDPR.

Within the due diligence process, the controller may take into account whether the processor provides adequate documentation proving compliance with data protection principles found in privacy policies,

records management policies, information security policies, external audit reports, certifications, and similar documentation. The controller should in particular take into account the processor's expert knowledge (e.g. technical expertise when dealing with data breaches and security measures) and reliability, as well as its resources. A site visit may also be necessary. After carrying out the due diligence process, the controller should be able to make a decision on the basis of sufficient evidence demonstrating that the processor is suitable, and it can then enter into a binding arrangement.

This due diligence process is not a one-time effort. The controller has an ongoing obligation to check whether the processor is compliant and meeting their obligations by means of auditing, either by using their own staff or a trusted third party. When outsourcing the processing of personal data (e.g. for the provision of technical assistance or cloud services), the controller must conclude a contract, another legal act, or binding arrangement with the other entity, which sets out clear and precise data protection obligations and the nature of the processing in a detailed data processing agreement.

**SUGGESTION**

Keeping written documentation of the due diligence process explaining why the controller considered the processor suitable may be useful to demonstrate compliance and accountability in the event of an investigation by a DPA.

### What organizational security measures can an SME take?

» Carrying out a risk assessment of personal data at hand. Such a risk assessment would focus on the risks arising from an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed. In short, the assessment would anticipate risks that a

data breach could affect data subjects.

- Build a culture of security awareness within the organization by participating in training activities.
- Have an information security policy foreseeing the role of each user and the required permission levels. Such an access control policy would define roles that may be given access to personal data, and in this way limit access to data that is necessary for that role (e.g. system administrator accounts). Furthermore, such a policy could be used to demonstrate responsible behaviour of the controller (Article 24) and facilitate compliance with the GDPR requirements.

**SUGGESTION**

A DPO could play a significant role in setting organizational security measures by awareness-raising, training, and regular auditing of staff handling personal data.



## What technical security measures can an SME take?

Technical security measures are sometimes thought of as the protection of personal data held in computers and networks. Whilst these are of obvious importance, many security incidents can be due to the theft or loss of equipment, the abandonment of old computers or hard-copy records being lost, stolen, or incorrectly disposed of. Technical measures must, therefore, include both physical and computer or information technology (IT) security.

When considering physical security, the following elements are relevant:

- the quality of doors and locks, and the protection of the business premises by means such as alarms, security lighting and/or CCTV;
- the access control to business premises as well as the supervision of visitors;
- the disposal of any paper and electronic waste; and
- the secure storage of IT equipment, particularly mobile devices.

In the IT context, technical measures may sometimes be referred to as 'cybersecurity'. This is a complex technical area that is constantly evolving, with new threats and vulnerabilities constantly emerging.

When considering cybersecurity, factors to be looked at include:

- system security – the security of the networks and information systems used by the company, especially those which process personal data;
- data security – the security of the data held within the systems (e.g. ensuring appropriate access controls are in place and that data are held securely through the use of suitable levels of encryption);
- online security – e.g. the security of the website and any other online service or application used by the company; and
- device security – including policies on Bring-Your-Own-Device (BYOD).

## What level of security is required?

The GDPR does not define security measures that an SME should have in place. Controllers and processors are only required to have a level of security that is 'appropriate'. Both controllers and processors need to consider the appropriateness in relation to the risks to the rights and freedoms of natural persons, current technological capabilities, and costs of implementation, as well as the nature, scope, context, and purpose of the processing.

This reflects both the GDPR's risk-based approach and the fact that there is no 'one size fits all' solution to information security. It means that what is 'appropriate' for each controller and processor depends on their circumstances, the processing in which they are engaged, and the risks it presents to their organization as well as to the rights and freedoms of data subjects. Where special categories of data are processed (such as health data) or personal data relating to minors, higher levels of security are expected to be implemented and documented.

Before deciding on appropriate measures, an SME needs to assess its personal data risk. An SME should review the personal data held and the way this information is used, in order to assess how valuable, sensitive, or confidential it is – as well as the damage or distress that could be caused if the data was to be compromised.

Other factors to consider are:

- the nature and extent of the organization's premises and computer systems;
- the number of staff, and the extent of their access to personal data; and
- if any personal data is held or used by a processor.



**USEFUL SOURCES**

- ENISA, Handbook on Security of Personal Data Processing specific for SMEs (2018) https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing
- ENISA, On-line tool for the security of personal data processing https://www.enisa.europa.eu/risk-level-tool/
- ISO/IEC 27001:2013 https://www.iso.org/standard/54534.html

## 3.7.5. Personal data breach notification

### Background

A **personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.[203] Breach of the GDPR by lack of an adequate legal basis for a processing operation or providing inadequate information

203 Article 4(12) GDPR.

to data subjects does not create obligations related to personal data breach notifications. Furthermore, a breach of information security which does not compromise personal data also does not fall within the scope of this obligation.[204] That is why not all security incidents are considered personal data breaches, but every personal data breach entails a security incident. Among the most common causes of data breaches, are negligence, accident or technical failure, and intentional acts by internal or external actors.[205]

When the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the controller is required to notify the competent DPA. When the risk to the rights and freedoms is high, the notification about a personal data breach should also be communicated to the data subject.

An obligation to notify of a personal data breach is both an accountability obligation and an obligation that requires taking 'additional measures when specific risks are identified'.[206] While being an accountability obligation, a data breach notification is also part of a controller's obligations, which 'can and should be varied according to the type of processing and the privacy risks for data subjects.'[207] Identification of risk of a personal data breach in the data protection impact assessment would require controllers to put appropriate measures in place to 'treat risk' by modifying, mitigating, retaining, removing, or sharing it.



204 European Data Protection Supervisor, 'Guidelines on Data Breach notifications for the European Union Institutions and Bodies' (21 November2018) https://edps.europa.eu/sites/edp/files/publication/18-12-05_guidelines_data_breach_en_0.pdf para 25.

205 Idem, para 29.

206 Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' (30 May 2014) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf 3-4.

207 Ibid.

## Under what conditions is a notification to the DPA required?

The GDPR requires that in situations where the data breach is likely to result in a risk to the rights and freedoms of natural persons, 'the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority'.[208]

At a minimum the notification must include:

- a description of the nature (e.g. deliberate, accidental, loss, destruction, etc.) of the data breach;
- the categories and approximate number of data subjects involved (if possible);
- the categories and approximate number of personal data records (if possible);
- the contact details of the DPO that will act as the contact point with the DPA;
- a description of the likely consequences of the data breach; and
- the measures the controller will implement to address the breach, to eventually mitigate its adverse effects.



**SUGGESTION**

If not all information about a data breach is available at once, it can be provided to the relevant DPA in phases.

To implement this obligation, the controller must become aware of the personal data breach. This means that the controller must have an internal procedure allowing them to confirm that there has been a breach of security concerning personal data. The GDPR does not specify the practical aspects of such a procedure.

208 Article 33(1) GDPR.

However, for smooth running and management, any entity handling information, including processing personal data, must have appropriate governance or organizational structures in place, where roles and responsibilities of individuals involved are specified in internal policy and strategy documents.

Such documents can be developed based on standards, guidelines, and models provided by external sources. Yet, they must consider relationships within the entity, its values and culture, as well as its contractual relationships. This contextual awareness, in combination with awareness of a data breach risk, is essential when developing an information incident response policy and plan, which can include obligations stemming from the GDPR as well as other regulatory frameworks (e.g. NIS Directive or the Payment Services Directive (PSD 2)).

**SUGGESTION**

An information incident response policy should be created before an incident occurs, so that it can be used if a data breach is detected.

The GDPR requires that all data breaches, regardless of whether these are notified to the DPA or communicated to the data subjects, are documented. Such documentation should furthermore include effects and remedial actions taken in response to a personal data breach.

### What documentation could help an SME to prepare for a data breach?

Having the following documents in place could assist in the event of a (personal) data breach:

1. A **policy** is a high-level document outlining the goal and objective of the incident response program, the scope of the program across the organization, program roles, responsibilities, and authority, and how program outputs, such as incident communication and reporting, will be managed.

2. A **plan** is a formal document outlining how the high-level policy document will be implemented and operationalized within the organization. Core elements of a security incident response plan include communication protocols that will be used to manage the sharing of incident updates and reports with internal and external stakeholders, metrics for measuring the effectiveness of the program, events that would trigger an update to the plan, and a strategy to improve and mature the plan over time.

3. **Standard Operating Procedures** (SOPs) are documents containing technical step-by-step actions that the CSIRT (Cyber Security Incident Response Team) will take to manage specific incidents. SOPs help minimize incident management errors and ensure a consistent and repeatable incident management capability. SOPs traditionally also include the forms and checklists that will be used by CSIRT members in the execution of the CSIR plan.[209]



## Under what conditions is a notification to affected individuals required?

Individuals have to be notified when the breach is likely to result in a high risk to their rights and freedoms. The threshold for the notification to individuals is higher than for notifications to DPAs, so that individuals are protected from 'unnecessary notification fatigue' and do not receive notifications about all breaches.[210]

The following elements can help to determine if the breach entails a high risk:

» **The type of breach**: the WP29 deems that the level of risk presented by data breaches depends upon whether the breach concerns the principle of confidentiality, the principle of integrity and/or

209 Fowler, K., *Data Breach Preparation and Response: Breaches Are Certain, Impact Is Not*, Kindle (Syngress 2016) 50.

210 Article 29 Working Party, 'Guidelines on Personal Data Breach Notification under Regulation 2016/679' (3 October 2017) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 23.

the principle of availability.[211] However, data breaches typically have different motivations: they can be financially motivated cybercrimes, cyber espionage (concerning national security or economic interests), or acts aiming to publicly humiliate someone without any intention of achieving financial gains.[212]

» **The nature, sensitivity, and volume of personal data**: the risk evaluation largely depends on the sensitivity of personal data that was subject to a data breach. However, this sensitivity is often contextual (e.g. a name and address could be sensitive if it concerns an adoptive parent), similarly to considerations concerning the volume of breached data. While typically the larger the volume of data breached, the greater the impact that may be anticipated, 'a small amount of highly sensitive personal data can have a high impact on an individual.'[213] It is also recognized that while data breaches concerning health data, identity documents, and credit card details entail risks, the possibility of combining this data creates higher risk than a single piece of information, as it could subsequently facilitate identity theft.[214]

» **Ease of identification of individuals**: when evaluating risks associated with a data breach, it is also important to consider whether the identification of individuals who were subject to a breach is going to be easy. In this regard, the controllers should consider whether the compromised data can be matched with other datasets, and what kinds of security measures have been implemented (e.g., what is the level of hashing, encryption, or pseudonymization).



211 Ibid.

212 Wolff, J., *You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches*, Kindle (MIT Press 2018) Location 2743 of 6938.

213 Footnote 208, 24-26.

214 Ibid.

- **The severity of consequences for individuals**: the WP29 argues that by taking into account the nature of the personal data involved in a breach (e.g., access to special categories of data, financial data) controllers can anticipate the potential damage to individuals.
- **Special characteristics of the individual**: the controller, when evaluating the impact on individuals, needs to consider, for example, if the breach concerns personal data about vulnerable individuals. Vulnerable data subjects may include children (they can be considered as being incapable of knowingly and thoughtfully opposing or consenting to the processing of their data), employees (in relation to their employers due to the subordinate power relationship that exists between them), and other vulnerable segments of the population requiring special protection (e.g. mentally ill persons, asylum seekers, the elderly, medical patients, etc.). Even if individuals are not part of a group that might automatically be considered vulnerable, an imbalance of power in their relationship with the controller can cause vulnerability for data protection purposes, if such individuals would be disadvantaged in the event that the processing of personal data is not performed.
- **Special characteristics of the controller**: the WP29 suggests that '[t]he nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach.'[215]

**EXAMPLE**

A private clinic may process special categories of data that – if accessed without authorization – may be used to cause harm to its patients (e.g. by blackmailing them).

- **The number of affected individuals**: finally, the controller needs to assess the amount of personal data that was compromised. In

215 Ibid.

general, it is argued that large-scale data breaches will have a more severe impact. However, a personal data breach involving special categories of personal data of one person can have a severe impact as well.[216]

As the GDPR matures, different DPAs have begun to express different thresholds for the reporting of breaches. The Irish Data Protection Commission, for example, provides guidance with more specific scenarios explaining when notifications concerning personal data breaches should be made by the controller.[217]

### SUGGESTION

In case of a data breach, consult the relevant DPA website to obtain a notification form. It often includes questionnaires facilitating risk assessment.

### USEFUL SOURCES

- Article 29 Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679' (3 October 2017) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
- European Data Protection Supervisor, 'Guidelines on personal data breach notification for the European Union Institutions and Bodies' (5 December 2018) https://edps.europa.eu/sites/edp/files/publication/18-12-05_guidelines_data_breach_en_0.pdf

216 While in principle large scale data breaches will have a more severe impact, a personal data breach involving data of one person can have a severe impact as well.

217 DPC, 'A Practical Guide to Personal Data Breach Notifications under the GDPR' (2019) https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf.

» Irish Data Protection Commission, 'A Practical Guide to Personal Data Breach Notifications under the GDPR' https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf

### 3.7.6. Data protection impact assessment (DPIA) and prior consultation

#### Background

A requirement to conduct a DPIA is a new addition to the EU data protection framework. It builds on the rich experience of conducting impact assessments in other fields (e.g. privacy impact assessment, environmental impact assessment, regulatory impact assessment).

To be effective, impact assessments are carried out at the early stage of a project (proactive initiative), at the phase of planning or designing, with the aim of anticipating the potential beneficial and adverse (i.e. negative) impacts of such a project. Impact assessments help decision-makers find the best and most beneficial solutions for the development and deployment of initiatives.[218] To be practical, impact assessment must be scalable, flexible, and applicable for large organizations, consortiums, or small- and medium-sized enterprises. Furthermore, they are not one-time efforts; they need to be periodically revised to make sure they reflect the changes in the reality surrounding the project.



218 E.g. environmental impact assessments originated from Green movements in the 1960s (read more at: 'International Association for Impact Assessment: Principles of Environmental Impact Assessment Best Practice' https://www.eianz.org/document/item/2744) and social impact assessments (SIA) were developed in the 1980s. SIAs aim to ensure that developments or planned interventions maximize the benefits and minimize the costs of those developments, including, especially, costs borne by the community (for more information read: 'The Interorganizational Committee on Guidelines and Principles for Social Impact Assessment: Guidelines and Principles for Social Impact Assessment https://www.tandfonline.com/doi/abs/10.1080/07349165.1994.9725857').

Accordingly, a DPIA process under GDPR also has to begin before the start of personal data processing operations, and ideally already at the design or planning phase. A DPIA cannot be used retrospectively to justify a particular decision (e.g. buying a drone, installing CCTV). Conversely, the DPIA has been conceived as a tool to shape the envisaged processing operations, to ensure that controllers are thinking about data protection implications from the outset and adopt the most privacy-friendly approach possible, in order to minimize the negative consequences that the processing operations could have on the fundamental rights and freedoms of data subjects and natural persons.

DPIAs, as with other types of impact assessments, constitute a **best-efforts obligation**. It is impossible to reduce negative consequences to zero in absolute terms, but SMEs have to react to them to the best of their ability, depending upon current technological capabilities and their available resources.[219] Yet, the protection of personal data and compliance with the GDPR must be ensured.[220]

## Who has to perform a DPIA?

A DPIA is only mandatory for SMEs acting as controllers, and only for certain processing operations. Whilst the processor and the DPO should assist, the controller bears overall responsibility for the DPIA process.

**SUGGESTION**

SMEs acting as processors may choose to perform a DPIA voluntarily for the following reasons: to enhance their awareness of the data processing operations and the functioning of their systems; to ensure that their organizational standards are complied with; to increase their trustworthiness; to demonstrate commitment towards data protection; to demonstrate sufficient guarantees to controllers.

219 Footnote 176, 2.

220 Article 35(7)(d) GDPR.

A DPIA can also be useful for assessing the data protection impact of a technology product (e.g. if the SME develops a piece of hardware or software, or if it offers data shredding and sanitizing services or cloud-based storage).[221]

As to the **assessors**, i.e. the persons or companies who perform the assessment in practice, the controller can choose to outsource the DPIA or to perform it themselves relying on in-house expertise.

### When is a DPIA mandatory?

Not all processing operations require a DPIA, only those '**likely to result in a high risk to the rights and freedoms of natural persons, taking into account the nature, scope, context, and purposes of the processing'**. The GDPR refers to rights and freedoms of natural persons, not just of data subjects, because a processing operation can present risks to natural persons whose personal data is not processed.

**EXAMPLE**

In the case of self-driving vehicles, a pedestrian may not be a data subject, but they are still a natural person whose life and health are endangered by the self-driving car.

Among the rights and freedoms that can be put at stake by the processing operations are:

- the data subject's rights as listed in the GDPR (e.g. right to access, right to erasure, rights to data portability, etc., see 2.5 What are data subjects' rights?);
- other fundamental rights and freedoms, such as respect for private and family life, home and communications; freedom of thought,

221 Footnote 141, 8.

conscience, and religion; freedom of expression and information; freedom to conduct a business; right to an effective remedy and to a fair trial; right to cultural, religious and linguistic diversity; right to non-discrimination; and many more.[222]

It is at the controller's discretion to determine whether the envisaged processing operations fall within the pre-defined high-risk criteria.[223]

However, certain elements may qualify the processing operations as 'likely to result in a high risk' for natural persons.

**EXAMPLES**

There is an **inherent high risk** in processing operations entailing:

1. evaluation or scoring, including profiling and predicting;
2. automated decision-making with a legal or similar significant impact;
3. systematic monitoring;
4. sensitive data or data of a highly personal nature (e.g. financial data, geolocation data);
5. data processed on a large scale;
6. matching or combining datasets;
7. data concerning vulnerable data subjects (e.g. children, asylum seekers, elderly people, patients);
8. the use of innovative or new technological or organizational solutions (e.g. artificial intelligence, wearable devices);

222 For other examples of fundamental rights, please refer, *inter alia*, to the Charter of Fundamental Rights of the European Union https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT, the European Convention on Human Rights https://www.echr.coe.int/Documents/Convention_ENG.pdf and to the constitutional documents of Member States.

223 Footnote 176, 3.

9. situations where the processing in itself 'prevents data subjects from exercising a right or using a service or a contract.' (e.g. denying service to a (potential) customer due to their profile).

The controller may use these criteria to evaluate if the processing operations entail a high risk for DPIA purposes, but they are not applicable when the controller has to evaluate whether to notify an individual of a data breach.[224]

The GDPR provides three examples of processing operations that, by their nature, entail high risks to rights and freedoms of individuals. They are:

a. the systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

**EXAMPLES**

An insurance company relying on profiling to build insurance-risk classifications and determine premiums should perform a DPIA.

A company relying on an automated system for checking CVs for recruiting should perform a DPIA.

A retailer relying on an automated system to quantify bonuses for employees on the basis of their individual performance at work should carry out a DPIA.

224 Footnote 141, 6.

b. the processing of special categories of data on a large scale, or of personal data relating to criminal convictions and offences;

**EXAMPLES**

A private health clinic processing its clients' data should perform a DPIA.

A company developing a dating app collecting information about the sexual preferences of its users should perform a DPIA.

A company developing a period tracker that is going to provide individualized cycle tracking with calendar and associated individualized predictions, reminders and notifications should perform a DPIA.

c. the systematic monitoring of a publicly accessible area on a large scale.

**EXAMPLES**

A security company providing CCTV monitoring services in a shopping centre or a public transport station should perform a DPIA.

A care home for mentally disabled people that is implementing a surveillance system based on high resolution cameras combined with a software capable of detecting abnormal behaviour of guests should conduct a DPIA.

A company that monitors the metadata (meaning the information pertaining to data) related to the use of its applications in order to improve its services should conduct a DPIA.

A company developing a mobile application specifically for celiac individuals that, on the basis of the geolocation of the device, suggests the closest shop where they can buy gluten-free products, should conduct a DPIA.

National DPAs compile and publish lists of processing operations that always require a DPIA. A DPIA is mandatory when the envisaged processing operations are included in this list.[225]

**SUGGESTION**

The lists of processing operations requiring a DPIA vary per country. Therefore, consult the website of the national DPA.

In principle, codes of conduct may also act as a guide to whether a DPIA is required or desirable.

**EXAMPLES**

Situations that may require carrying out a DPIA:

- a jeweller planning to implement a tool to monitor access to a safe combining the use of fingerprints and facial recognition;
- a biotechnology company offering genetic tests directly to consumers to assess and predict disease/health risks;
- a company monitoring social media data to create profiles of clients or employees;
- eHealth app developers;
- a company implementing an automatic staff appraisal for assigning bonuses to its employees to increase salaries;
- an insurance company ranking clients for the purpose of providing them with insurance services; and
- a private investigation service that handles data concerning criminal convictions and offences.

225 Article 35(4) GDPR.

## When is a DPIA not required?

The GDPR foresees the following situations where a DPIA process is not required:

» When the data processing operations are included in the list of data processing operations not requiring a DPIA compiled by the DPA(s) to whose jurisdiction(s) the controller is subject.

**SUGGESTION**

The lists of processing operations (not) requiring a DPIA may be found on the website of the national DPA.

» When the personal data is processed (1) in order to comply with a legal obligation or in the public interest; (2) on the basis of EU law or the Member State's law; and (3) when an impact assessment essentially satisfying the conditions laid down in the GDPR has already been performed in the context of the adoption of that legal basis (albeit in very few cases will this be relevant for SMEs).

» When processing operations concern personal data from patients or clients by an individual physician, other health care professional, or lawyer, they are not required to carry out a DPIA because they are not processing personal data on a large scale.

Just because there is no obligation to conduct a DPIA does not mean that a controller's general obligation to implement measures to appropriately manage risks to the rights and freedoms of data subjects is diminished. The requirement to have appropriate technical and organization measures to mitigate the likelihood and severity of risks forms a part of general controller obligations, data protection by design and by default, and data security. This requirement exists regardless of whether the requirement to conduct a DPIA applies or not.

In case of doubt as to whether to conduct a DPIA or not, it is best practice to consult a DPO or person responsible for personal data processing operations, in order to determine whether there is a need to conduct the DPIA process.

### When is a new (revised) DPIA required?

The risk-based approach entails that controllers must continuously assess the risks created by their processing activities in order to identify when a type of processing is 'likely to result in a high risk to the rights and freedoms of natural persons'.[226] In practice, this means that the DPIA needs to be periodically revised. The revision of a DPIA is not only useful for continuous improvement, but also critical to maintaining the level of data protection in a changing environment over time.

A new (i.e. revised version of a) DPIA could be required if the risks resulting from the processing operations change, for example, because a new technology or organizational solution has been introduced or because personal data is being used for a different purpose.[227] Data processing operations can evolve quickly, and new vulnerabilities can arise. In this sense, data breaches and security incidents could increase awareness regarding risks connected to the processing operations and trigger a revision of the DPIA. A new DPIA may also become necessary because the organizational or societal context for the processing activity has changed, for example, when new rules on data protection or data protection impact assessments are adopted in the jurisdiction where the controller is operating, when the effects of certain automated decisions have become more significant, or again when new categories of data subjects become vulnerable to discrimination.

226 Footnote 141, 6.

227 Idem, 13-14.

Each of these examples could be an element that leads to a change in the risk analysis concerning the processing activity at hand. Conversely, certain changes could lower the risk as well. For example, a processing operation could evolve so that decisions are no longer automated or when a monitoring activity is no longer systematic. In that case, the review of the risk analysis undertaken can show that the performance of a DPIA is no longer required.

## How should a DPIA be conducted?

The GDPR provides controllers with a lot of flexibility in determining the precise structure and form of the DPIA. Many methods for conducting the DPIA process exist, originating from the public and private sectors and academia alike.[228]

The steps marked with * are not expressly required by the GDPR, but have emerged as either best practice or for practical reasons.

| | | | | |
|---|---|---|---|---|
| Step 1 | *Screening (threshold analysis).* | a. Stakeholder involvement | b. Documentation | c. Quality control |
| Step 2* | *Scoping* | | | |
| Step 3* | *Planning and preparation* | | | |
| Step 4 | *Description* | | | |
| Step 5 | *Appraisal of impacts* | | | |
| Step 6 | *Recommendations* | | | |
| Step 7 | *Prior consultation with a supervisory authority (DPA)* | | | |
| Step 8 | *Revisiting* | | | |

228 The method presented in this handbook builds on Kloza, D. et al., 'Towards a method for data protection impact assessment: Making sense of GDPR requirements' (2019) d.pia.lab Policy Brief https://cris.vub.be/files/48091346/dpialab_pb2019_1_final.pdf A sample template is provided in Kloza, D. et al., 'Data protection impact assessment in the European Union: developing a template for a report from the assessment process' (2020) d.pia.lab Policy Brief https://cris.vub.be/en/publications/data-protection-impact-assessment-in-the-european-union-developing-a-template-for-a-report-from-the-assessment-process(2300a8d5-7e5d-4e63-86cb-51288e2eaca4).html.

The first six steps are consecutive, while the final two steps are prospective, in the sense that they are triggered only if certain conditions are met. Steps A, B and C are ongoing, in the sense that stakeholder consultation, documentation, and quality control have to be reflected in all of the other phases.

**Step 1: *Screening* (*threshold analysis*)**

In this step, the controller, with the help of the DPO if appointed, drafts a preliminary description of the envisaged processing operations. Based on that, it should be possible to determine if the DPIA process is required (i.e. the processing operations are likely to result in a high risk for the rights and freedoms of natural persons) or not (because the processing operations are not likely to result in a high risk, or an exemption applies). If the latter, then it is best practice for the SME to document the decision by issuing a statement of non-significant impact, explaining why the DPIA was not performed.

**Step 2: *Scoping****

In this step, the controller determines:

a. the benchmark, i.e. what aspects of the fundamental right to personal data protection (e.g. the exercise of data subjects' rights, the conditions of the consent) and what other fundamental rights are likely to be affected by the envisaged data processing operation(s);

b. which stakeholders to involve in the process. They must include, at least: the concerned data subjects and their representatives (e.g. NGOs),[229] the DPO,[230] and the processor;[231]

c. which techniques will be used for assessing the impacts. The GDPR mentions only assessment of the necessity and proportionality of the processing operations and the risk appraisal for the rights and freedoms of natural persons. However, these can be combined with

229 Article 35(9) GDPR.

230 Article 39(1)(c) GDPR.

231 Article 28(3)(f) GDPR.

other techniques. For example, scenario analysis (to compare the possible different outcomes of the processing operations with the adoption of different mitigation measures) or cost-benefit analysis (to identify the mitigation measures to address the impacts having regard to the (economic) resources available to the controller);

d. what other evaluation techniques need to be used (if any). For example, if the initiative affects the environment, together with the DPIA, environmental impact assessment (EIA) may be warranted or required by law. Similarly, if an initiative affects human health, a health impact assessment may be required by law, or an ethics impact assessment may be desirable.

**Step 3: *Planning and preparation****

In this step, the controller specifies:

a. the objectives/goals of the assessment process;

b. the criteria for the risk acceptance (risk criteria) and for justifying the necessity and proportionality of the processing operations;

c. the resources necessary to conduct the DPIA, in terms of time, money, workforce, knowledge, know-how, premises and infrastructure;

d. the procedures and time frames of the assessment process, to define the (reciprocal) responsibilities of the actors involved DPIA process, set deadlines and calendarize the milestones;

e. the criteria for choosing the team of assessors, their roles and responsibilities;

f. the modalities to ensure the continuity of the assessment process, regardless of any disruptions such as changes in the parties involved in the assessment process (e.g., controller, processors, assessors); natural disasters; utility failures, etc.; and

g. the criteria triggering the revision of the process. As well as a change in the level of risk,[232] others are possible. For example, the controller may establish periodic reviews of the DPIA process.

**Step 4: *Description***

In this step, by widening the preliminary description, the envisaged processing operation(s) are described both contextually and technically. The nature, scope, context, and purposes of the processing operations are clarified, as well as any legitimate interest pursued by the controller.[233]

**Step 5: *Appraisal of impacts***

In this step, the necessity and proportionally of the envisaged processing operation(s), and the risks to the rights and freedoms of individuals stemming therefrom are assessed.

For the necessity and proportionality test, each data processing operation is assessed against personal data protection principles. These are: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality.

For the risk assessment, a typical method requires, first of all, a risk to be identified and described; second, the risk must be analysed to determine its level/magnitude; third, the risk must be evaluated: the results of risk analysis are compared with risk criteria (cf. *Step 3b)* in order to determine whether the risk and its level are acceptable, if any mitigation measure is to be recommended, and/or whether any risk needs to be treated as a priority.

**Step 6: *Recommendations and remediation***

In this step, mitigation measures to address the risks identified in the previous step and to demonstrate compliance with the law are suggested.

232 Article 35(11) GDPR.

233 Article 35(7)(a) GDPR.

For each data protection principle not satisfied in the previous step, the assessor(s) recommends measures to satisfy these principle (e.g. not to collect a certain type of personal data, in order to comply with data minimization; to reduce the data retention period).

Risk can be mitigated by manipulating either its likelihood or probability, e.g. by eliminating the exposure to a risk or severity (e.g. preparing a response plan should the risk materialize), or both. Risks can be avoided, mitigated, transferred (to another entity, e.g. outsource, insurance etc. or in time) or accepted. Residual risk is the risk that remains if there is no measure available to mitigate it and triggers a prior consultation with a DPA (*cf.* Step 7).

The mitigation measures can be both technical and organizational. They can include defining policies and procedures for the protection of data; allocating defined roles and responsibilities as to the processing of personal data; establishing access control policies to personal data; creating a data breach response plan; setting up a business continuity plan; implementing logging and monitoring of data access; using a data deletion and disposal tool; etc.[234]

**SUGGESTION**

To demonstrate compliance, it is best practice to include the risks identified, their appraisal and their mitigation measures within a register.

Furthermore, the register of risks, as well as the DPIA report, may be shared with the competent DPA for purposes of prior consultation.

**Step 7: *Prior consultation with a supervisory authority (or DPA)***

In a scenario whereby the residual risk related to the processing

234 ENISA, Handbook on Security of Personal Data Processing (December 2017) https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing Annex A.

operations remains high despite the adoption of mitigation measures, but the controller decides they still want to go ahead with the processing operations, then the SME must consult the competent DPA. In principle, as an outcome of the prior consultation, the DPA will provide non-legally-binding written advice. Nevertheless, the GDPR expressly foresees that the DPA could also use its powers (e.g. start an investigation, issue warnings).

**SUGGESTION**

Check your DPA website for a prior consultation form.

**Step 8: *Revisiting***

Revisiting (part of) the DPIA process (or reversing the statement of non-significant impact) is mandatory when there is a change in the level of risk of the processing operations.

**a. *Stakeholder involvement***

To ensure the decision making process is complete and inclusive, stakeholders are to be involved in all parts of the DPIA process. The controller should the views of the DPO, of the processor and, where appropriate, of the data subjects and of their representatives. Other stakeholders may also be included (e.g. information security officer, if present). The views of the stakeholders are sought and taken into consideration (this is very useful for identifying risks to the rights and freedoms of the data subjects, which might not be apparent to the data controller themselves), but stakeholders cannot decide about the DPIA. Any final decisions are down to the controller.

**b. *Documentation**

Keeping intelligible records, in writing or another permanent format, of all activities undertaken within the assessment process, is the easiest way to demonstrate accountability and compliance with the law. It is best practice to also keep track of the advice given by the stakeholders, DPO included, and of the reasons why such advice was (not) followed.

**c. *Quality control**

The DPO is expressly tasked with monitoring the performance of the assessment process.[235]

**SUGGESTION**

To ensure that the DPIA process adheres to a given standard of performance, an SME can use a progress monitoring tool.

**USEFUL SOURCES**

» Working Party 29, '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, (3 October 2017)
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

» ENISA, Handbook on Security of Personal Data Processing specific for SMEs (2018)
https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

» ISO 31000:2018 Risk management — Guidelines
https://www.iso.org/standard/65694.html

235 Article 39(1)(c) GDPR.

» To consult the lists of data processing operations (not) requiring a data protection impact assessment, it is possible to either visit the websites of the national data protection authorities or use the EDPB Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions

**Templates for DPIA**

» CNIL, AEPD and ICO have published templates for DPIAs. The latest versions of these templates are available on the regulators' websites.

» Kloza, D. et al., 'Data protection impact assessment in the European Union: developing a template for a report from the assessment process' (2020) d.pia.lab Policy Brief https://cris.vub.be/en/publications/data-protection-impact-assessment-in-the-european-union-developing-a-template-for-a-report-from-the-assessment-process(2300a8d5-7e5d-4e63-86cb-51288e2eaca4).html

**Software for DPIA**

» CNIL https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil



## 3.7.7. Codes of conduct

### Background

The Member States, the European DPAs, the EDPB, and the Commission encourage the drawing up of codes of conduct that are intended to contribute to the proper application of the GDPR, taking into account the specific features of various processing sectors and the specific needs of SMEs. Codes of conduct are aimed at improving standards by clearly setting out best practices for the processing of personal data

in a specific sector or business. They can concern either controllers or processors.

While codes of conduct are voluntary sets of rules that are developed by an organization representing a sector or category of controllers or processors (e.g. an association, a chamber of commerce), compliance monitoring with reference to a code of conduct will be carried out by a body which has an appropriate level of expertise regarding the subject matter of the code, which is accredited for such a purpose by the competent supervisory authority.[236]

The European Gaming and Betting Association (EGBA) has been among the first to publish a Code of Conduct on data protection which, once approved, will establish dedicated sector-specific rules and best practices to ensure compliance with the GDPR in the online gambling sector.[237] The Code of Conduct prepared by EGBA has been sent for approval to the Maltese Data Protection Authority. It may take up to two years for this code to be reviewed and approved by the European data protection authorities and the European Data Protection Board.

Codes of conduct must go beyond the principles foreseen in the GDPR. They 'must materially specify or enhance the application of data protection law to a certain sector or processing activity'.[238] In practice, this means, for a DPA to approve a code of conduct applicable in its territory, or for the EDPB to approve a code of conduct applicable across several jurisdictions, or for the Commission to approve a code of conduct concerning transfers to third countries, such a code must specify the application of the GDPR and address the following:



236 For the latest developments concerning such bodies, see updates on the EDPB website.

237 'EGBA Demonstrates Commitment To GDPR With Sectoral Code Of Conduct For Data Protection' https://www.egba.eu/news-post/egba-demonstrates-commitment-to-gdpr-with-sectoral-code-of-conduct-for-data-protection/.

238 'Codes of conduct' https://www.dataprotection.ie/en/organisations/codes-conduct.

- fair and transparent processing;
- the legitimate interests pursued by controllers in specific contexts;
- the collection of personal data;
- the pseudonymization of personal data;
- the information provided to the public and to data subjects;
- the exercising of the rights of data subjects;
- the information provided to, and the protection of, children, and how the consent of the holders of parental responsibility is to be obtained;
- the measures and procedures referred to in Articles 24 and 25 and the measures to ensure the security of processing referred to in Article 32;
- the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;
- the transfer of personal data to third countries or international organizations; and
- out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects about the processing.



## What are the advantages of codes of conduct?

Where a relevant code of conduct exists, opting for it could be beneficial for an SME as it could facilitate its compliance with the GDPR requirements. This is particularly the case where data processing practices share many commonalities across a sector. It may be a cost-effective way of reducing sources of non-compliance, and therefore the risk of fines.

## How to select the appropriate code of conduct?

When selecting a code of conduct under the GDPR, an SME should pay particular attention and evaluate whether it addresses the needs arising from the personal data processing operations that it runs.

**SUGGESTION**

An SME should check whether the code of conduct has been approved by a DPA, or, where appropriate, by the EDPB or the European Commission. National codes of conduct will be published and made available on the public register of approved codes of conduct on the relevant DPA website; European codes of conduct will be published by the EDPB and, where relevant, by the European Commission.

**USEFUL SOURCES**

» European Data Protection Board, 'Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679' (2 April 2019) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf

## 3.7.8. Certification

### Background

The Member States, the DPAs, the EDPB, and the European Commission encourage the establishment of data protection certification mechanisms and data protection seals and marks for the purpose of demonstrating compliance with the GDPR. Such mechanisms can concern processing operations by controllers and processors.

The criteria by which to evaluate if a certification is within the scope of the GDPR are:

1. The certification concerns the processing operation. More precisely, when assessing a processing operation, the components to consider are the personal data (material scope of the GDPR); the technical systems and the infrastructure (such as hardware and software, used

to process the personal data); and processes and procedures related to the processing operation(s).

2. The certification concerns personal data and privacy in a broad sense;

3. The voluntary nature of the certification; and

4. The performance of third-party conformity assessment. Certification can only be issued by a certification body accredited by the National Accreditation Body or by the competent supervisory authority, on the basis of criteria approved by that supervisory authority or by the EDPB. This means that self-certification schemes are excluded from the scope of Article 42 of the GDPR.[239]

### What are the advantages of certifications for SMEs?

SMEs, both when acting as controllers and as processors, can benefit from certifications for the following reasons.

First, certifications can enhance trust of data subjects and clients, both in business-to-consumer and in business-to-business relations, offering them greater transparency about the way(s) in which personal data is processed by controllers and processors.[240]

Second, certifications can reward privacy-aware technologies developed or employed by SMEs.[241] Building upon these two aspects, certifications can offer a competitive advantage for SMEs that opt for a certification scheme.[242]

---

239 Kamara, I. et al., 'Data Protection Certification Mechanisms: Study on Articles 42 and 43 of the Regulation (EU) 2016/679: final report' https:// ec.europa.eu/info/study-data-protection-certification-mechanisms_en 4, 5.

240 Ibid.

241 Products and systems cannot be certified as such for being GDPR compliant, but they are part of the evaluation for awarding the certification for data-processing activities. See Kamara, I. https://iapp.org/news/a/four-gdpr-certification-myths-dispelled/.

242 Ibid.

Furthermore, in case of international data transfers (outside the EEA), a certification can be used as a means by which to demonstrate that appropriate safeguards are in place for a controller or processor not subject to the GDPR. In this case, the existence of certification can act as a legal basis for data transfers.[243]

The use of certifications does not prove compliance with the GDPR, but they can be used by controllers and processors as a way of demonstrating the implementation of appropriate technical and organizational measures; the existence of sufficient guarantees for processor-controller and sub-processor-processor relations.[244]

### How should you choose between different certifications?

At the time of writing, there are no approved GDPR certification schemes at a domestic or an EU level. National and international certification schemes exist, but these cannot be considered certification schemes under the GDPR. In other words, even when data-protection-related, these certifications are not specifically tailored to the GDPR's requirements.[245]

Existing national and international certifications differ greatly in scope. Some of them are fully related to data protection, while some are partially related to data protection, and yet others concern single aspects of data protection (e.g. cybersecurity). Certification models can be multisector (where they do not differentiate among businesses) or single-sector (designed for specific business activities, such as cloud computing). Even within the multisector ones, there are multiple SME-friendly models. Some apply a pricing policy tailored to the size of

243 Ibid.

244 European Data Protection Board, 'Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation' (4 June 2019) https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-12018-certification-and-identifying-certification_en para 13.

245 Footnote 239.

the applicant, while others apply a free-of-charge or discount policy to all certification candidates.[246]

When national and European certification schemes are approved, they will be divided between comprehensive GDPR schemes, covering the full breadth of the GDPR; and single-issue schemes, focusing on particular GDPR sub-topics (e.g. data protection by design, child consent, etc.).[247]

For SMEs, certifications covering all facets of the GDPR may be easier and more cost-effective than single-issue schemes, but it has to be borne in mind that all certifications have limited validity. Certifications have to be subject to revision when the legal framework of the jurisdiction they refer to is amended, terms and provisions are interpreted by judgements of the European Court of Justice, or current technical capabilities evolve.[248] In fact, the GDPR sets a limit of the validity of a certification at 3 years.



**USEFUL SOURCES**

- European Data Protection Board, 'Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation' (4 June 2019) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf
- Kamara, I. et al., 'Data Protection Certification Mechanisms: Study on Articles 42 and 43 of the Regulation (EU) 2016/679: final report' https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en and Annexes https://ec.europa.eu/info/sites/info/files/certification_study_annexes_publish_0.pdf

246 Footnote 237, 4-5.

247 Ibid.

248 Footnote 242, para 75.

# 4. SMEs and employees' data

From a data protection point of view, in an employment relationship, the employer plays the role of the data controller, whereas the employee is the data subject.

Many activities routinely performed in the employment context entail the processing of workers' personal data, some of which belongs to the special categories of personal data as listed in Article 9 of the GDPR (e.g. trade union membership, health-related information). Processing employees' personal data is one of the most common data processing activities conducted by SMEs.

**EXAMPLES**

Personal data processing at work may include the following activities: reviewing application forms and work references; compiling payrolls; sharing employees' data with competent authorities for tax or social benefits purposes; keeping records of sickness, annual leave, unpaid leave and special leave, and related appraisal forms; maintaining records relating to promoting, transfer, training and disciplinary matters; maintaining a registry related to workplace accidents.
It is worth noting that monitoring of emails, calls and workspaces for security purposes does involve the processing of personal data of employees.[249]



249 Article 29 Working Party, 'Opinion on the processing of personal data in the employment context' (13 September 2001) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48sum_en.pdf 1.

The GDPR allows Member States to specify rules for personal data processing in the employment context. Member States are entitled to adopt rules concerning e.g. employees' consent, the recruitment process, and the implementation of employment contracts.[250]

**SUGGESTION**

Considering that a Member State's rules governing personal data processing in the employment context may differ, SMEs are recommended to consult the national implementing rules of the GDPR and the guidance issued by their DPA.



## 4.1. What are the possible legal bases for processing the personal data of employees?

Similar to other processing operations, to process the personal data of their employees, SMEs need a legal basis.[251] In general, the use consent for the processing of personal data in the employment context is not appropriate for this purpose: the economic and power imbalance between employer and employees make it difficult for employees to provide consent that would be considered 'free'.[252] Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw consent without detriment.[253]

250 Article 88 GDPR and Recital 155.

251 See 2.4 What are the possible legal bases for personal data processing?

252 Footnote 30, 330.

253 Article 29 Working Party, 'Opinion on the processing of personal data in the employment context' (2001) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48sum_en.pdf 2.

The more appropriate legal bases could be:

» the performance of a contract to which the employee is party.

**EXAMPLE**

The employer must meet obligations under the employment contract, such as pay the employee.[254]

» the compliance with a legal obligation to which the employer is subject.

**EXAMPLES**

There are situations where the employer must communicate personal data of the employee for social security, welfare, or tax purposes. Another example of this could be a situation, where the employer is legally obliged to obtain a certificate of good conduct of (prospective) employees, or check their qualifications.

» the legitimate interest of the employer, insofar it is not overridden by the interests or fundamental rights and freedoms of a data subject.

**EXAMPLES**

A recruiter browses a publicly available database (e.g. LinkedIn or similar) and contacts a person to offer a job interview. An estate agent communicates to a client the contact details of one of their workers to schedule an appointment.

254 Article 29 Working Party, 'Opinion 2/2017 on data processing at work' (23 June 2017) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 7.

## 4.2. When and what monitoring activities are permissible?

Modern technologies enable employees to be tracked over time, across workplaces and their homes, through many different devices such as smartphones, desktops, tablets, vehicles, and wearables.[255]

Monitoring activities are forms of personal data processing that can occur during the recruitment process (e.g. if an employer checks data of aspirant employees on social media), for the length of the contractual relationship (e.g. video surveillance, GPS on vehicles used by employees) and even after the end of the working relationship (e.g. if an employer monitors former employees' LinkedIn profiles to ensure that they are not infringing a non-competition clause).[256]

In certain situations, the employer may be legally obliged to perform certain forms of tracking (e.g. install tracking technologies in vehicles to be sure that a driver does not exceed a certain number of driving hours per day).

In other cases, the employers may have a legitimate interest in monitoring employees (e.g. for security reasons; for safety reasons; to prove unlawful conduct of an employee). However, monitoring employees poses risks from a fundamental rights perspective. Systematic or occasional monitoring can infringe upon the privacy rights of an employee, and limit employees' channels by which they could inform employers about irregularities or illegal actions of superiors and/or colleagues threatening to damage the business or workplace.[257]

255 Ibid.

256 Ibid.

257 Ibid.

## EXAMPLE

An employer, who seeks to install a GPS in a company car to control the progress and circumstances of work of the employees, may invoke the legitimate interest as a legal basis.

However, the employer must first evaluate whether the data processing is necessary for the purposes designated, and whether its implementation by a GPS device is proportionate to the limitations imposed on the rights of the employees.

Employers must inform their employees of the installation of tracking devices in the company cars and must make clear that, while the employees use the vehicle, their movements are recorded.

The situation would be different if the employees were allowed to use company cars for private purposes, too. In this case, the employer could not invoke the legitimate interest because the implementation of a GPS device that would track a company car at all times would be disproportionate.

## SUGGESTION

Whilst there are national differences concerning whether an employer can monitor their employees, the common traits are that:

- policies and rules concerning legitimate monitoring must be clear and readily accessible, ideally elaborated by the employer together with the representatives of the employees; and
- privacy-friendly organizational solutions have to be preferred to the monitoring of the employees. For example, an employer may opt for the introduction of filters upon websites accessible from the workplace rather than monitoring all the web activities of the employees. Consider what other options are available to achieve the same goal.

# Annex I – National laws

The General Data Protection Regulation replaced the Data Protection Directive on 25 May 2018. While it harmonized data protection rules and became 'directly applicable' across the EU/EEA, some differences remain among national laws specifying data protection rules. For this reason, when adhering to data protection rules, national laws implementing the GDPR must be consulted. Below is an overview of such laws, prepared by VUB-LSTS.[258]

| Member State | National law implementing the GDPR | Unofficial English Translation |
|---|---|---|
| Austria | Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) StF: BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.) | Federal Act concerning the Protection of Personal Data |



258 The online version of this list can be found at https://lsts.research.vub.be/en/specifying-the-gdpr/.

| Member State | National law implementing the GDPR | Unofficial English Translation |
|---|---|---|
| Belgium | Wet betreffende de bescherming van natuurlijke personen met betrekking van persoonsgegevens (Kaderwet), 30 juli 2018 - Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (Loi cadre), 30 juillet 2018<br>68616 BELGISCH STAATSBLAD—05.09.2018—MONITEUR BELGE [C−2018/40581]<br><br>Wet van 3 december 2017 tot oprichting van de Gegevensbeschermings-autoriteit - Loi du 3 décembre 2017 portant création de l'Autorité de protection des données.<br>BELGISCH STAATSBLAD—10.01.2018—MONITEUR BELGE 989 [C−2017/31916] | Act on the protection of natural persons with regard to the processing of personal data |
| Bulgaria | Закон за защита на личните данни<br>В сила от 01.01.2002 г.<br>*Обн. ДВ. бр.1 от 4 Януари 2002г*, изм. ДВ. бр.93 от 26 Ноември 2019г | Personal Data Protection Act |

| Member State | National law implementing the GDPR | Unofficial English Translation |
|---|---|---|
| Croatia | Zakon o Provedbi Opće Uredbe o Zaštiti Podataka.<br>Izdanje: NN 42/2018<br>Broj dokumenta u izdanju: 805<br>ELI: /eli/ sluzbeni/2018/42/805 | Implementation Act<br>Not available |
| Cyprus | Αριθμός 125(I) του 2018<br>ΝΟΜΟΣ ΠΟΥ ΠΡΟΝΟΕΙ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΦΥΣΙΚΩΝ ΠΡΟΣΩΠΩΝ ΕΝΑΝΤΙ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΚΑΙ ΓΙΑ ΤΗΝ ΕΛΕΥΘΕΡΗ ΚΥΚΛΟΦΟΡΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΑΥΤΩΝ<br>ΕΠΙΣΗΜΗ ΕΦΗΜΕΡΙΔΑΤΗΣ ΚΥΠΡΙΑΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣΠΑΡΑΡΤΗΜΑ ΠΡΩΤΟ ΝΟΜΟΘΕΣΙΑ<br>-ΜΕΡΟΣ I<br>Αριθμός 4670, Τρίτη,31 Ιουλίου 2018, 827 | Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data |
| Czech Republic | Zákon č. 110/2019 Sb.<br>Zákon ze dne 12. března 2019 o zpracování osobních údajů<br>Částka 47/2019 | Act of 12 March 2019 on personal data processing |

| Member State | National law implementing the GDPR | Unofficial English Translation |
|---|---|---|
| Denmark | LOV nr 502 af 23/05/2018 Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven) Ressortministeriets journalnummer Justitsmin., j.nr. 2017-7910-0004 | Data Protection Act |
| Estonia | Isikuandmete kaitse seadus Avaldamismärge: RT I, 04.01.2019, 11 | Personal Data Protection Act |
| Finland | Tietosuojalaki 1050/2018 Hallinnonala: Oikeusministeriö Voimaantulo: 01.01.2019 | Data Protection Act (1050/2018) |
| France | Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 JORF n°0288 du 13 décembre 2018 | Act N°78-17 of 6 January 1978 on Information Technology, Data Files And Civil Liberties |

| Member State | National law implementing the GDPR | Unofficial English Translation |
|---|---|---|
| Germany | Zweites Gesetz zur Anpassung des Datenschutz-rechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU-2. DSAnpUG-EU)<br>1626 Bundesgesetzblatt Jahrgang 2019 Teil I Nr. 41, ausgegeben zu Bonn am 25. November 2019 | Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 |
| Greece | ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4624<br>Τεύχος Α' 137/29.08.2019<br>Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις | Hellenic Data Protection Authority (HDPA), measures for implementing 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 transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions |

| Member State | National law implementing the GDPR | Unofficial English Translation |
|---|---|---|
| Hungary | 2011. évi CXII. Törvény az információs önrendelkezési jogról és az információszabadságró | Act CXII of 2011 on the right to informational self-determination and on the freedom of information |
| Iceland | Lög um persónuvernd og vinnslu persónuupplýsinga 2018 nr. 90 27. Júní Lagasafn. Íslensk lög 1. október 2020. Útgáfa 150c. | Act no. 90/2018 on Data Protection and the Processing of Personal Data |
| Ireland | Number 7 of 2018 Data Protection Act 2018 | n/a |
| Italy | Codice in materia di protezione dei dati personali (d.lgs. 196/2003) modificato dal Decreto Legislativo 10 agosto 2018, n. 101, Dispozioni per l'adequamento della normativa nazionale alle dispozioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) G.U. 4 settembre 2018 n. 20 | PERSONAL DATA PROTECTION CODE Containing provisions to adapt the national legislation to 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 |

| Member State | National law implementing the GDPR | Unofficial English Translation |
|---|---|---|
| Latvia | Fizisko personu datu apstrādes likums (Publicēts: Latvijas Vēstnesis, 132, 04.07.2018. OP numurs: 2018/132.1) | Personal Data Processing Law |
| Liechtenstein | Datenschutzgesetz (DSG) vom 4. Oktober 2018 LGBl-Nr 2018.272 LR-Nr 235.1 | Data Protection Act of October 4, 2018 |
| Lithuania | ASMENS DUOMENŲ TEISINĖS APSAUGOS ĮSTATYMO NR. I-1374 PAKEITIMO ĮSTATYMAS 2018 m. birželio 30 d. Nr. XIII-1426 | Law of Republic of Lithuania on Legal Protection of Personal Data (integrated Law Amending Personal Data Protection Law no. I-1374) |

| Member State | National law implementing the GDPR | Unofficial English Translation |
|---|---|---|
| Luxembourg | Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en oeuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État MÉMORIAL A - N° 686 du 16 août 2018 | The Act of 1 August 2018 on the organisation of the National Data Protection Commission, implementing 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), amending the Labour Code and the amended Act of 25 March 2015 stipulating the rules of remuneration and the terms and conditions for the promotion of State civil servants |
| Malta | Chapter 586<br>Data Protection Act<br>ACT XX of 2018 | n/a |

| Member State | National law implementing the GDPR | Unofficial English Translation |
|---|---|---|
| Netherlands | Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)<br>Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming) | General Data Protection Regulation Implementation Act |
| Norway | Lov om behandling av personopplysninger (personopplysningsloven) LOV-2018-06-15-38 | Not available |

| Member State | National law implementing the GDPR | Unofficial English Translation |
|---|---|---|
| Poland | Ustawa z 10 maja 2018 o ochronie danych osobowych<br>Dziennik Ustaw 2019 r. Poz. 1781 | The Act of 10 May 2018 on the Protection of Personal Data |
| Portugal | Lei n.º 58/2019, de 8 de agosto que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (RGPD)<br>Diário da República, 1.ª série. No. 151 pag. 3 | Not available |

| Member State | National law implementing the GDPR | Unofficial English Translation |
|---|---|---|
| Romania | LEGE nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) MONITORUL OFICIAL nr. 651 din 26 iulie 2018 | Law No. 190/2018 on implementing measures to 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) |
| Slovakia | Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov | Act no. 18/2018 on personal data protection and amending and supplementing certain Acts |
| Slovenia | Zakon o varstvu osebnih podatkov (ZVOP-1) Uradni list RS, št. 94/07 - uradno prečiščeno besedilo Predlog novega Zakona o varstvu osebnih podatkov (ZVOP-2) – EVA: 2019-2030-0045 | Personal Data Protection Act |

| Member State | National law implementing the GDPR | Unofficial English Translation |
|---|---|---|
| Spain | Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales<br>BOE-A-2018-16673 | Not available |
| Sweden | Lag med kompletterande bestämmelser till EU:s dataskyddsförordning<br>SFS 2018:218 | Act containing supplementary provisions to the EU General Data Protection Regulation (SFS 2018:218) |
| United Kingdom (transition) | Data Protection Act 2018<br>Ch. 12 | n/a |

# About the editors

**Lina Jasmontaitė-Zaniewicz** is a doctoral candidate at the Vrije Universiteit Brussel. Her PhD research concerns primarily the data breach notification obligations foreseen in the General Data Protection Regulation. Lina is a Certified Information Privacy Professional (CIPP/E, IAPP). She has served as an advisor for European projects on regulatory and ethical questions concerning the use of personal data. After obtaining an LLM in Law and Technology (cum laude) at Tilburg University, she completed the traineeship program at the European Data Protection Supervisor. She worked as a legal intern in a Brussels-based European privacy and data security practice in 2013. She worked as a legal researcher at the Leuven University (CiTiP) in 2014-2016.

**Alessandra Calvi** is a doctoral candidate at the Vrije Universiteit Brussel (VUB). Alessandra holds an LLM in International and European law – Data law (summa cum laude) awarded by the Institute of European Studies of the VUB. After obtaining a law degree from the Università Cattolica del Sacro Cuore of Milan (2015), she completed a law clerkship at the Tribunal of Pavia, in the Labour law section in 2016-2017). She also completed traineeships in a criminal law firm and at the European Data Protection Supervisor. Her research interests include the interrelationships between law and technology, in particular between data protection and the circular economy.

**Renáta Nagy** has been working at the Hungarian DPA (NAIH) since 2017. She has been responsible for the administrative management of the STAR II project, as well as for liaising between Hungarian SMEs and SME associations. She coordinated the operationalization of the SME hotline set up at NAIH's premises, also being actively involved in replying to the enquiries received. She has delivered presentations about the SME hotline and the most common enquiries received during the awareness-raising and informational events for SMEs organized by NAIH in partnership with the Chambers of Commerce and Industry.

**David Barnard-Wills** has over a decade's experience in research on privacy and data protection. He has designed and delivered GDPR training for multiple clients, and his research work has explored the way in which data protection authorities work together; how data protection can best be communicated to different audiences; cyber security; and practical ways to undertake privacy-by-design. He is a Senior Research Manager in the Policy, Ethics and Emerging Technologies team at Trilateral Research. David holds a PhD in Politics from the University of Nottingham and has previously been a Research Fellow at the University of Birmingham, Cranfield University, and the UK's Parliamentary Office of Science and Technology.