SupporT small And medium enterprises on the data protection Reform II

(Draft) Handbook on European data protection law for Small and Medium-sized Enterprises

DRAFT

LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES VRIJE UNIVERSITEIT BRUSSEL

TRILATERAL RESEARCH

Acknowledgements

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

STAR II project ran in the partnership of the National Authority for Data Protection and Freedom of Information (NAIH), the Research Group on Law, Science, Technology & Society (LSTS) of the Vrije Universiteit Brussel (VUB), and Trilateral Research Limited (TRI IE) between 2018 and 2020.

The main goal of the project was enhancing compliance with the General Data Protection Regulation by assisting Data Protection Authorities (DPAs) and Small and Medium-sized Enterprises (SMEs) in their reciprocal obligations.

The handbook is the outcome of the work of the diverse and well balanced STAR II consortium, encompassing: the interdisciplinary research group Law Science Technology and Society (LSTS) of the Vrije Universiteit Brussel, with extensive theoretical experience in privacy and data protection; Trilateral Research Ltd, multidisciplinary research services consultancy with extensive publications in the field of privacy policy research and experience in tracking the impacts and changes arising from the GDPR across several domains; the Hungarian Data Protection Authority, active in awareness raising activities for SMEs.

DRAFT

Contents

DRAFT

DRAFT

List of abbreviations

AEPD	**Agencia Española Protección de Datos (Spanish DPA)**
APD-GBA	Autorité de protection des données - Gegevensbeschermingsautoriteit (Belgian DPA)
CNIL	Commission nationale de l'informatique et des libertés (French DPA)
CSIR(T)	Computer Security Incident Response (Team)
CSV	Comma Separated Values
DPA	Data Protection 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
EEA	European Economic Area
EU	European Union
GDPR	General Data Protection Regulation
NGO	Non-Governmental Organisation
NIS	Network and Information Security
ICO	Information Commissioner's Office (United Kingdom DPA)
IP	Informacijski pooblaščenec (Slovenian DPA)
JSON	JavaScript Object Notation
PSD	Payment Service Directive
RDF	Resource Description Framework
SME(s)	Small and Medium-Sized Enterprise(s)
SOP(s)	Standard Operating Procedure(s)
VDAI	Valstybinė duomenų apsaugos inspekcija (Lithuanian DPA)
WP29	Article 29 Working Party
XML	Extensible Markup Language

DRAFT

I. INTRODUCTION

Background

The European Data Protection reform

The Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, or General Data Protection Regulation (GDPR), is the cornerstone of European personal data protection law.

The GDPR was introduced to update the former Data Protection Directive 95/46/EC with two main goals. The first, fundamental rights-oriented, that is to increase the protection of the rights and freedoms of natural persons when their personal data are processed. The second, business-oriented, that is to regulate more uniformly the free movement of personal data within the European Economic Area.[1]

With the economy becoming more and more digital and data-driven, to unleash the potential of the (digital) single market, the old patchwork of national data protection rules needed to be replaced with more consistent provisions to ensure more legal certainty for companies doing business in Europe.[2] The digital transformation is an opportunity for companies -including Small and Medium-sized Enterprises (SMEs)- for scaling up and reducing costs. The digital economy can bring benefits to not only the newly established enterprises, that often start digital, but also widen the business opportunities of the more traditional ones (e.g. with e-commerce).[3] Likewise, stronger data protection rules could, in principle, boost business by increasing the confidence of consumers in the digital environment; consolidating pre-existing trust among business partners; creating new business opportunities for those organisations providing technical solutions in privacy innovation.[4]

Since May 2018, all the companies that process personal data, either established in the European Union (EU) or processing personal data of individuals based in the EU, have to abide by this Regulation.[5]

SMEs are not exempted from applying this new legal framework. Regardless of their business sectors and their digitalisation level, the processing of personal data is unavoidable for the vast majority of them. For example, to pay the employees, an SME needs to process personal data. Similarly, to get in touch via mail or via telephone with (potential) clients, an SME needs to process personal data. The installation of a CCTV system at the premises of an SME entails the processing of personal data, too.

The enforcement actions undertook by several Data Protection Authorities (DPAs) (or Supervisory Authorities (SAs)) across Europe against SMEs leave no doubt about the applicability of the Regulation to them. Not complying with information obligations stemming from the GDPR when using cookies cost 15.000 Euro to a Belgian company. Another SME continuously filming its employees at their

[1] Proposal for a European Parliament and Council Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final

[2] Andrea Jelinek, 'Foreword to the GDPR Consolidated text', ISBN 978-92-9242-275-2

[3] Angel Gurría, 'Remarks to the Launch of "Digital for SMEs" Initiative' (OECD conference, Paris, 29 November 2019) https://www.oecd.org/industry/launch-of-digital-for-smes-initiative-paris-november-2019.htm

[4] See 'Data protection - Better rules for small business' https://ec.europa.eu/justice/smedataprotect/index_en.htm. and European Digital SME alliance Position Paper on 'General Data Protection Regulation (GDPR) Two-Year Review: Clear guidance for SMEs and stronger European-minded Data Protection Authorities (DPAs) (10 June 2020) https://www.digitalsme.eu/digital/uploads/Position-Paper-GDPR-Review-2020.pdf. However, the Position Paper pointed out how tangible evidence about the increase of customer trust is still lacking.

[5] Leanne Cochrane, Lina Jasmontaite-Zaniewicz and David Barnard-Wills, 'Data Protection Authorities and their awareness-raising duties under the GDPR: The case for engaging umbrella organisations to disseminate guidance for Small and Medium-size Enterprises' (forthcoming)

workstation was fined 20.000 Euro by the French DPA.[6] A small shipping company had to pay 5.000 Euro for missing a data processing agreement with one of the business partners.[7]

Yet, compliance with the Regulation is still problematic for most SMEs, which represent the vast majority of all businesses in the EU. Albeit the European legislators acknowledged that SMEs deserve special attention and support from DPAs, small entrepreneurs still have to cope with several challenges, including misinformation about the GDPR requirements; scarcity of practical, easy to understand and targeted guidance about data protection law; uncertainty about the interpretation of certain provisions of the law; lack of internal data protection expertise and resources to invest thereto.[8] On top of that, a lack of legal certainty, due to the national specificities of GDPR implementation and the limited rulings coming from the highest courts.[9]

In this context, the STAR II consortium has undertaken research activities to examine, on the one hand, DPAs' awareness-raising efforts concerning the GDPR compliance for SMEs; on the other hand, the SMEs' experience with the GDPR. The STAR II consortium has conceived this handbook as a tool that makes the GDPR simple for SMEs and to help them comply with their legal obligations.

Structure and method

The handbook summarises the main requirements that SMEs have to abide by to lawfully process personal data under the GDPR.

Preliminarily, the handbook provides an overview of the main actors of the European data protection landscape, clarifying how they may support, directly or indirectly, SMEs in complying with their obligations under the GDPR (CHAPTER I WHO IS WHO?).

Then, the handbook guides SMEs in identifying what personal data are; choosing the most appropriate legal basis for the different personal data processing operations; granting data subjects rights; processing the personal data of their employees (Chapter II A GUIDE FOR SMEs TO LAWFULLY PROCESS PERSONAL DATA).

These topics were found of particular concern for the SMEs that addressed the hotline operated between 15 March 2019 and 31 March 2020 by the partner NAIH to assist SMEs with questions and uncertainties concerning compliance with the GDPR.

Then, the handbook unpacks the GDPR provisions entailing a risk-based approach (Chapter III SMEs and THE RISK-BASED APPROACH IN THE EU DATA PROTECTION FRAMEWORK).

Indeed, a core message coming through from the STAR II data[10] is that SMEs face a methodological challenge with the risk-based approach in the GDPR, i.e. they understand it conceptually but less so how it applies to their specific context.

---

[6] ibid

[7] 'Hessian DPA Fines Shipping Company For Missing Data Processing Agreement' (23 January 2019) https://www.jdsupra.com/legalnews/hessian-dpa-fines-shipping-company-for-76851/

[8] STAR II Deliverable D2.2 Report on the SME experience of the GDPR (2019), 31-34

[9] European Digital SME alliance Position Paper on 'General Data Protection Regulation (GDPR) Two-Year Review: Clear guidance for SMEs and stronger European-minded Data Protection Authorities (DPAs) (10 June 2020) https://www.digitalsme.eu/digital/uploads/Position-Paper-GDPR-Review-2020.pdf

[10] I.e. the findings extracted during interviews conducted with 18 DPAs, 22 SME association representatives, over 50 respondents to the online survey, and 11 face to face interviews with SME representatives that were conducted within the scope the STAR II research in 2019. Cf. STARII, Deliverable D2.1 Report on DPA efforts to raise awareness among SMEs on the GDPR (Version 1.1; 2019); STARII, Deliverable D2.2 Report on the SME experience of the GDPR (2019).

Then, the handbook refers to certifications and codes of conduct as tools that may help controllers and processors demonstrate compliance with the GDPR and best practice. (Chapter IV ENHANCING PERSONAL DATA PROTECTION).

Additionally, following the suggestions of the DPAs and SME associations that were interviewed by STAR II consortium in 2019,[11] the handbook:

- includes examples and provides references to templates and guidance developed by various DPAs across Europe and other bodies, like the European Data Protection Board (EDPB); in each section, the handbook firstly introduces the background of a provision and then provides references to good practices, includes examples, references to templates and guidance;
- suggests SMEs how to 'sell' their compliance with the GDPR, to transform it into a competitive advantage;
- targets a wide range of SMEs, regardless of their business sector;
- aims to boost some misconceptions about the GDPR

Finally, the text refers to available national DPAs' decisions concerning SMEs to clarify how certain GDPR's provisions were interpreted in practice.

Added-value of the handbook

This handbook is the result of several complementary expertise. Contributors include public officials from the Hungarian Data Protection Authority (NAIH), academics from the interdisciplinary research group Law Science Technology and Society (LSTS) of the Vrije Universiteit Brussel, practitioners from Trilateral Research Ltd (TRI), a multidisciplinary research services consultancy with extensive publications in the field of privacy policy research. The handbook builds upon the concrete questions that have been raised by SMEs both during the interviews conducted by STARII consortium and during the year of operation of the hotline at NAIH. The handbook provides a reference point for SMEs seeking to better understand the risk-based approach of the GDPR and to effectively put it into practice. Furthermore, the text condenses in a unique document references to templates and guidance on specific GDPR provisions developed by different DPAs and bodies across Europe, making their consultation easier.

Target audience

The handbook targets especially SMEs owners and their employees dealing with data protection matters, including Data Protection Officers (DPOs), and associations of SMEs providing advice to their member on GDPR issues.

Due to its practical nature and its reference to templates and guidance issued by DPAs and other bodies across Europe, it may be of interest also for bigger companies.

[11] ibid.

I. WHO IS WHO? AN OVERVIEW OF THE MAIN ACTORS OF THE EUROPEAN DATA PROTECTION SCENE

Several European and national bodies deal with data protection. Each of them has different tasks and powers. For this reason, they may be useful for SMEs in different ways.

The Supervisory Authorities or Data Protection Authorities

The Supervisory Authorities (SA) or Data Protection Authorities (DPAs) are the independent public authorities responsible for monitoring the application of the GDPR in the Member States. Each Member State may provide for one supervisory authority (for example, countries as France, Spain, Hungary, and Italy have only one supervisory authority) or more (for example, in Germany there is one supervisory per each *lander*).

DPAs may be (in)famous among SMEs for their powers to handle complaints lodged by data subjects. issue fines and take other enforcement actions against companies for non-compliance with the GDPR.

Nevertheless, DPAs have also other fundamental tasks, such as engage in awareness-raising activities to help companies -and specifically SMEs- to understand their obligations arising from the GDPR.

Accordingly, DPAs have been issuing guidance on various aspects concerning the GDPR. Some of such guidance documents have been addressed to SMEs specifically. Based on the information provided by the STAR II DPA interviews as well as desktop research of all EU DPA websites, it appears that slightly less than one-third of EU DPAs currently provide GDPR guidance that is specifically tailored for SMEs; upon the last review, this included the DPAs from Belgium (APD-GBA),[12] France (CNIL),[13] Ireland (DPC),[14] Lithuania (VDAI),[15] Slovenia (IP),[16] Spain (AEPD),[17] Sweden (*Datainspektionen*)[18] and the UK (ICO).[19] Some of these DPAs further distinguish guidance for micro-businesses.[20]

TIP
In principle, templates and tools issued by any DPAs across the European Union can be used by any SMEs, regardless of the place of establishment, providing that (when necessary) they are adjusted to the national laws implementing the GDPR.

[12] *Autorité de protection des données* (APD) or *Gegevensbeschermingsautoriteit* (GBA) See 'RGPD Vade-Mecum Pour Les PME (January)' (2018) <https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/PME_FR_0.pdf>.

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

[14] *An Coimisiúm um Chosaint Sonraí/* The Data Protection Commission (DPC). See 'Guidance Note: GDPR Guidance for SMEs (July)' (Data Protection Commission 2019) https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190708 Guidance for SMEs.pdf>

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

[16] *Informacijski pooblaščenec (IP)* See, 'Varstvo Osebnih Podatkov' (*Upravljavec*, 2018) https://upravljavec.si

[17] *Agencia Española de Protección de Datos (AEPD)*. See 'Facilita RGPD' (*AEPD*) https://www.aepd.es/herramientas/facilita.html

[18] *Datainspektionen*. See, 'GDPR - Nya Dataskyddsregler' (*Verksamt*, 2018) https://www.verksamt.se/driva/gdpr-dataskyddsregler> accessed 3 October 2019.

[19] *Information Commissioner's Office* (ICO). See, 'Micro, Small and Medium Organisations' (*ICO*) https://ico.org.uk/for-organisations/in-your-sector/business/

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

A list of EU Data Protection Authorities, and their website, is available here **https://edpb.europa.eu/about-edpb/board/members_en**

The European Data Protection Board

The European Data Protection Board (EDPB) is an independent European body that contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between DPAs. The EDPB is composed of the heads of the DPAs in the EU and the European Data Protection Supervisor (EDPS) or their representatives. With the entry into force of the GDPR, it replaced the Article 29 Working Party (WP29), the independent European working party that used to deal with issues relating to the protection of privacy and personal data until 25 May 2018. WP29 Opinions, albeit not directly related to the GDPR, are still useful to understand key concepts of European data protection laws.

As the former WP29, the EDPB regularly issues opinions and general guidance (not legally binding) to clarify certain aspects of European data protection laws. Albeit the EBPB does not provide individual consultancy services, the general guidance provided by this body can be useful for SMEs.[21] For example, the EDPB adopted guidelines on consent, on data protection by design and by default, on the processing of personal data through video devices, and many more.[22] The EDPB is also empowered by the GDPR to take legally binding decisions towards national DPAs to ensure a consistent application of the Regulation across the European Union.[23]

The European Union Agency for Cybersecurity

The European Union Agency for Cybersecurity (ENISA) supports the European Institutions, the Member States, and the business community in addressing, responding to, and especially in preventing network and information security problems. The agency has issued several guidance documents targeted specifically to SMEs, including a Cloud Security Guide for SMEs, a Handbook on Security of Personal Data Processing specific for SMEs, and Guidelines for SMEs on the security of personal data processing.[24]

The European Data Protection Supervisor

The European Data Protection Supervisor (EDPS) acts as the DPA for the European Union institutions, bodies, and agencies.[25] As the EDPB, the EDPS issues opinions and general guidance (not legally binding), about certain aspects of European data protection laws, too. Albeit formally addressed to European Institutions, bodies, and agencies, these opinions and guidance may be useful to clarify certain concepts under the GDPR. For example, the EDPS issued a Preliminary Opinion on Privacy by Design.

DRAFT

[21] 'About EDPB' https://edpb.europa.eu/about-edpb/about-edpb_en

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

[23] 'About EDPB' https://edpb.europa.eu/about-edpb/about-edpb_en

[24] ENISA Publications https://www.enisa.europa.eu/publications#c5=2010&c5=2020&c5=false&c2=publicationDate&reversed=on&b_start=0

[25] 'Our role as supervisor' https://edps.europa.eu/data-protection/our-role-supervisor_en

II. A GUIDE FOR SMEs TO LAWFULLY PROCESS PERSONAL DATA

What is personal data processing under the GDPR?

Understanding the concept of personal data processing under the GDPR is fundamental for SMEs. Indeed, the GDPR covers only the processing of personal data, meaning that, if the data processed are not personal, the Regulation does not apply.

Example
Even if a company processes only a small amount of personal data in the context of its business activities (e.g. of contractual partners or their contact persons to fulfill contracts of service), it is still subject to the GDPR.
In so far as the processing is carried out data in the context of an SME's business activities, the so-called household exemption (which exempts natural persons in the course of a purely personal or household activity from applying the GDPR) is not triggered.[26]

'Processing' encompasses any operations performed on personal data, either manually or automatically, such as storage, recording, deletion, transfer, consultation, combination, etc.[27]

Examples
A hairdresser who has an agenda containing names, surnames, and phone numbers of his/her clients is performing some processing.

The owner of a bed & breakfast who is saving reservations and contact details of guests on an excel file is performing some processing.

The employer who is communicating the details of a sick employee the competent authority for welfare purposes is performing some processing.

The recruiter who is consulting the CVs of prospective candidates for a job post is performing some processing.

Extracting phone numbers and e-mail addresses from web pages to send direct marketing communications is constitute a form of processing.

Personal data is any information related to an identified or identifiable natural person (the data subject).[28]

The definition is very broad. 'Any information' encompasses both objective information (e.g. ID and social security numbers, results of blood analysis), and subjective ones (e.g. opinions and assessments about a client and/or an employee).[29]

Information is 'related to' a natural person when is about that natural person, or objects, events, or processes that are somehow connected to the natural person.[30]

[26] Art. 2(2)(c) GDPR
[27] Art. 4(2) GDPR
[28] Article 4(1) GDPR
[29] 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
[30] 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 9

Examples

The service register of a car held by a mechanic contains personal data of both the car owner and the mechanics. On the one hand, the information on the car, mileage, dates of service checks, etc. are associated with a plate number and an engine number, which can be linked to the owner. But the information contained in the register can be associated with the mechanic that worked on the car, too.[31]

The call logs of phones located inside a company office contain personal data of different subjects, such as the employees of the company performing the calls; the clients called by the employees; certain third parties (e.g. potential clients of the company, security or cleaning staff using the phone).[32]

Household consumptions or usage of energy are personal data.[33]

In principle, contacting a company (i.e. a non-natural person) with a direct marketing offer is not an activity subject to the GDPR because the protection of the data of non-natural persons, such as companies, does not fall within the scope of the Regulation. [34]
However, where the name of a legal person derives from that of a natural person, or a corporate e-mail is normally used by a certain employee, they are considered personal data and the GDPR is applicable.[35]

Under the GDPR, a person is 'identifiable' when s/he can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier (e.g. internet protocol addresses (IP addresses), cookie identifiers, radio frequency identification (RFID)[36]) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[37]

To determine the 'identifiability' of an individual, account should be taken of all the means reasonably likely to be used to perform the identification, taking into consideration objective factors (e.g. the state of the art of the available technology at the time of the processing and technological developments, and the costs and the amount of time required for identification).[38] Direct identification usually occurs by name. In turn, indirect identification entails a combination of several pieces of information.[39]

Example

In the case of pseudonymisation, personal data such as name, date of birth, sex, address, etc. are replaced by a pseudonym. Pseudonymisation techniques include encryption with a secret key, hash function, tokenisation, etc.[40]

---

[31] 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

[32] 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

[33] Vagelis Papakonstantinou and Dariusz Kloza, '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

[34] Albeit in some Member States (e.g. Italy) the national laws implementing the GDPR extend the applicability of certain provisions of the Regulation to legal persons

[35] 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

[36] Recital 30 GDPR

[37] Article 4(1) GDPR

[38] Recital 26 GDPR

[39] 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 13

[40] 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

Pseudonymised data can no longer be attributed to a specific data subject unless additional information is used,[41] but the data subject remains indirectly identifiable. That is why pseudonymised data are considered personal data and the GDPR applies to them.[42]

When all identifying elements are eliminated, meaning that data are anonymised, the GDPR is not applicable.[43] Several anonymisation techniques exist,[44] but their effectiveness has been criticised. It has been argued that current methods for anonymizing data still leave individuals at risk of being re-identified[45] and that the distinction between anonymized data and personal data is fluid, as the re-identification of an individual largely depends on the context.[46]

SMEs must be particularly careful when they decide to rely on anonymization techniques because, if it turns out that data are not actually anonymized, they may incur in legal responsibility under the GDPR.

TIP
In case of doubts, it is best practice to consider data as personal data, to better protect the individuals to whom the data may refer to and to prevent GDPR infringements.

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

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

Depending on the role, the obligations of an SME under the GDPR change. Even if data processors have to comply with certain rules,[47] the data controllers bear the ultimate responsibility for the processing

[41] 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 94

[42] 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 pag 8

[43] 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 93.

[44] Anonymization techniques are ascribable to two main approaches: the randomisation and the generalisation. The former encompasses those methods (such as noise addition and permutation) which alter the accuracy of the data. The latter includes those practices (such as aggregation and k-anonymity, l-diversity/t closeness) that generalize, or dilute, the attributes of a data subject by modifying their scale (i.e. a region rather than a city, a month rather than a week). For more information, refer to 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

[45] Luc Rocher, Julien M. Hendrickx and Yves-Alexandre de Montjoye, '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

[46] Sophie Stalla-Bourdillon and Alison Knight, '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

[47] For example, data processors must be able to demonstrate compliance, keeping records of processing activities; ensure the security of processing, implementing technical and organisational measures; nominate a DPO in certain situations; notify data breaches to the data controller. See FRA/ECtHR/EDPS, *Handbook on European data protection law* (Publications Office of the European Union, 2018), 101, 102. Comparing with the previous Data Protection Directive, the obligations posed by the GDPR on data processors have increased. See Detlev Gabel and Tim Hickman, '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)

of personal and for complying with the key data protection requirements and principles. For certain processing operations, it may be Union or Member State law to allocate the different roles.

As regards the roles in the processing operations:

1) an SME is a data controller (or controller) when, alone or jointly with others, determines the purposes and means of the processing of personal data. The 'purposes' of processing data involves 'why' the personal data is being processed and the 'means' of the processing involves 'how' the data is processed.[48] If a company can determine e.g. which data shall be processed, for how long, who shall have access to them, the legal basis of the processing, then it will be a controller.[49]

Example
A spa and a beautician are different legal entities sharing the same working spaces.
They enter into a partnership and set up a common fidelity programme for their clients (e.g. for a spa entrance, 5% discount at the beautician; for 40 euro spent at the beautician, 5% discount on spa entrance).
To join the common fidelity programme, clients are requested to give their name, surname, e-mail address.
For the personal data processed within the common fidelity programme, the spa and the beautician will be joint controllers.

2) An SME is a data processor (or processor) when processes personal data on behalf of a controller, following the controller's instructions. A processor must be legally separate from the controller.[50] Upon written authorisation of the controller, a processor may engage a sub-processor.

Example
An employee of a pet shop is tasked with sending offers via mail to the clients. In this case, the processing occurs in-house and both the roles of controller and processor are played by the pet shop.
Conversely, if the pet shop relied on a marketing company for the same activity, then the former would be a controller and the latter a processor.
A data controller can decide either to process data in-house or to outsource this activity to a processor.

3) An SME is a data recipient (or recipient) when personal data are disclosed to it, whether a third party or not.

Examples

<https://www.whitecase.com/publications/article/chapter-11-obligations-processors-unlocking-eu-general-data-protection>

[48] Data Protection Commission, 'Guidance Note: GDPR Guidance for SMEs' (July 2019) <https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190708%20Guidance%20for%20SMEs.pdf>

[49] Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' [WP169] Adopted on 16 February 2010

[50] Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' [WP169] Adopted on 16 February 2010

An SME owner entrusts an employee to perform data processing operations on a dataset. In this case, the employee will be a recipient but not a third party.[51]

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.

The attribution of roles must stem from actual reality.[52] Whereas an entity has the capacity to determine means and purposes of data processing, it is deemed as a data controller, regardless of its formal denomination (e.g. 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 data processor for certain datasets and as a data controller for others.

Examples
SME1 provides advertisements and direct marketing for other companies. SME1 concludes a contract with SME2 pursuant to which SME1 commits to provide advertising to the clients of SME2. In this case, SME1 is the data processor and SME2 is the data controller.
Whereas SME1 decided to use SME2 clients' database for another purpose (e.g. promoting the products of a third SME), SME1 would be treated as the data controller for this type of data processing.

A jeweller concludes a contract with a security company so that the latter installs cameras in various parts of the jewellery and monitors them. In so far as the personnel of the security company just looks at the screens and calls the police in case of anomalies, the security company is a processor and the jewellery a controller.
For any processing operation(s) exceeding the instructions of the jeweller (e.g. if the security company stores recordings without been requested to do so), the security company is considered the data controller.
If the security company just does a mechanical activity (install cameras), it does not even qualify as a processor.

The GDPR requires the conclusion of a **written contract** (data processing agreement) between the processor and the controller (or between joint-controllers, or processors and sub-processors), detailing reciprocal obligations and rights, other than subject matter, nature, purpose, duration of the processing, types of personal data and category of data subjects.[53]

The data processing agreement is to be concluded before the actual data processing takes place.

If a processor engages a sub-processor, the same data protection obligations as set out in the agreement between the controller and the (original) processor apply.[54]

[51] 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 111
[52] Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' [WP169] Adopted on 16 February 2010
[53] Articles 28(3) and (9) GDPR
[54] Article 28(4) GDPR

The contract between joint controllers shall specify the respective roles and relationships of the joint controllers towards the data subject.[55]

TIP
DPAs may adopt standard contractual clauses with regards to data processing agreements between controller and processor and processor and sub-processor.
Before drafting a data processing agreement from scratch, it is worthy to consult the website of the DPA where the SME is established to see if templates of contracts are available in the local language.

Useful sources
'Controllers and processors' by ICO https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

Opinion 1/2010 on the concepts of "controller" and "processor" by the WP29 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

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

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

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

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

'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' by AEPD https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf

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

DPA decisions relevant SMEs
The Hessian DPA fined a small shipping company for missing a data processing agreement with one of the business partners. The fine was 5.000 Euro per missing agreement. [56]

[55] Article 26(2) GDPR
[56] 'Hessian DPA Fines Shipping Company For Missing Data Processing Agreement' (23 January 2019) <https://www.jdsupra.com/legalnews/hessian-dpa-fines-shipping-company-for-76851/>

What are the principles relating to processing of personal data?

The principles at the basis of personal data processing are: [57]

- Lawfulness, fairness and transparency.

Lawfulness means that there must be a legal basis (or ground) for processing personal data (see section *What are the possible legal bases for personal data processing?*).[58] 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 it in ways that have unjustified adverse effects on them.[59] Transparency entails the data subjects must be informed, in clear and plain language, about how their data are being used, and what the risks, the rules and the safeguards and the rights connect to the processing of personal data are.[60]

- Purpose limitation

Purpose limitation entails that any processing of personal data must be done for a well-defined specific purpose, identified before the starting of the processing. Any further processing must be compatible with the original one.[61]

- Data minimisation

Data minimisation entails using only those data which are adequate, relevant and not excessive in relation to the purpose for which they have been collected and/or further processed.[62]

- Accuracy

Accuracy requires that personal data must be checked regularly and kept up to date, and that inaccurate data are promptly erased of rectified.[63]

- Storage limitation

Storage limitation requires the deletion of anonymisation of personal data as soon as they are no longer needed for the purposes for which they were collected.[64]

- Integrity and confidentiality
- Integrity and confidentiality are related to data security. They entail that, to prevent data breaches, appropriate technical and organisational measures must be in place.[65]
  Accountability

[57] Art. 5 GDPR
[58] FRA/ECtHR/EDPS, Handbook on European data protection law (Publications Office of the European Union, 2018) 118 https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf
[59] 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/''
[60] FRA/ECtHR/EDPS, Handbook on European data protection law (Publications Office of the European Union, 2018) 118 https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf
[61] FRA/ECtHR/EDPS, Handbook on European data protection law (Publications Office of the European Union, 2018) 122 https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf
[62] FRA/ECtHR/EDPS, Handbook on European data protection law (Publications Office of the European Union, 2018) 125 https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf
[63] FRA/ECtHR/EDPS, Handbook on European data protection law (Publications Office of the European Union, 2018) 127 https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf
[64] FRA/ECtHR/EDPS, Handbook on European data protection law (Publications Office of the European Union, 2018) 129 https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf
[65] FRA/ECtHR/EDPS, Handbook on European data protection law (Publications Office of the European Union, 2018) 131 https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

DRAFT

Accountability principle will be presented in the section *Article 24 on the responsibility of the data controller and the principle of accountability*.Article 24 on the responsibility of the data controller and the principle of accountability

What are the possible legal bases for personal data processing?

To process personal data lawfully, meaning in accordance with the GDPR, SMEs need a legal basis (or a ground for processing personal data).

Personal data may be lawfully processed if one of the following criteria is satisfied:

- 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 exercising official authority;
- the processing is necessary for the purposes of the legitimate interests of controllers or third parties, in so far as they are not overridden by the interests or the fundamental rights of the data subjects.

How to choose among different legal basis?

The choice of the legal basis depends on the circumstances surrounding the processing operations.

Consent

The consent can be rendered by the data subjects with a statement (written, oral, video, audio, etc.) or affirmative action (a click, typing a digit, etc.). The consent can be obtained electronically as the GDPR does not specify any form. However, the data controller must prove that the data subject had given consent.

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

At a practical level, consent is **freely given** when it can be withdrawn anytime by the data subjects, without any detriment. Examples of detriments are disadvantage, deception, intimidation, coercion or significant negative consequences.[66] Negligible negative consequences on the data subjects do not undermine the consent.

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

Example
A minimarket offers clients a personal card for getting discounts. In this case, the minimarket can process the personal data of the clients on the basis of their consent because not enjoying extra discounts is a minor negative consequence.[67]

[66] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' (4 May 2020) para 46, 47 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 14 May 2020

[67] FRA/ECtHR/EDPS, *Handbook on European data protection law* (Publications Office of the European Union, 2018) 145 https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

A company develops 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 requirement, and geolocation data.
In this case, the consent form shall be separated from the Terms and Conditions. Furthermore, the user shall be able to choose if s/he wants to share all the information requested or only some of them, as not all of them are necessary for the functioning of the app.

Informed consent means that data subjects have to understand what they are agreeing to. Therefore, data subjects 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;
- existence of the right to withdraw consent.[68]

TIP
A lengthy consent form full of legalese and technical terms does not count as informed consent.
When presenting a consent form, the data controller has to put him/herself in the shoes of the data subject and use clear and plain language.

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. It is the so-called granularity of the consent.

Example
A sports centre would like to collect customers' e-mail addresses for sending them a monthly newsletter concerning new courses and training activities.
Furthermore, the sports centre would also like to share customer's details with other partner companies (e.g. a company specialised in fitness clothing and a company specialised in supplements)
In this case, the sports centre has to ask consent separately for the two purposes, i.e. sending the newsletter and share the e-mail 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.[69]

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

Example
A catering service requires clients to create an online account to make orders and organise the delivery.
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', 'I agree to receive marketing communication'.
If the boxes are already ticked by default, the consent is not valid.

[68] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' (4 May 2020) para 64, 65 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 14 May 2020
[69] ibid. para 8

When information society services (i.e. contracts and other services that are concluded or transmitted on-line) are offered directly to a **child**,[70] and consent is used as a legal basis, the holder of parental responsibility over the child that has to consent.

TIP
Using consent as legal basis for processing personal data is not always possible, nor desirable. Conversely, demonstrating that the consent was freely given, informed, specific and unambiguous can be challenging. When possible, SMEs should not refrain from using other legal bases.

Useful sources
'Guidelines 05/2020 on consent under Regulation 2016/679' by EDPB
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

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

Contractual relationship

In certain cases, processing personal data is necessary to perform (or enter into) a contract to which the data subject is a party.

Example
An online shop, to perform the delivery of the products, must process the information concerning the addresses of the customers. In this case, the legal basis of the processing is the performance of the purchasing contract between the shop and the customer.

Compliance with a legal obligation

In certain cases, processing personal data is necessary for the data controller to comply with a legal obligation. The legal obligation may originate from both Union and Member State law. The law itself will determine the purposes of the processing, the specifications to determine the controller, the type of personal data processed, the data subjects concerned, the entities to which data will be disclosed, the purpose limitation.

Example
When an entrepreneur shares the personal data of his/her customers with tax authorities for fiscal purposes, the legal basis for the processing is compliance with a legal obligation.

When an employer communicates to the competent national authority information about his/her 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.

The right to data protection is a fundamental right but it is not absolute. In matters of life and death, the right to personal data protection is overridden by the right to life.

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

Example
In the case of a workplace accident, the employer may share with the emergency doctors the personal information of the employee.

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

In certain cases, processing personal data is necessary for the performance of a task carried out by the data controller in the public interest or exercising 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 has to process personal data, the public interest and the exercise of the official authority count as legal bases.

Example
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 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 of controllers or third parties, in so far as they are not overridden by the interests or the fundamental rights of the data subjects.

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

- whether there is a **legitimate interest** -of the SME itself, or of a third party- behind the processing (**purpose test**)

  To be legitimate, an interest must be:

  - **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.[71]

- whether the **processing** is **necessary for that purpose** (**necessity test**)
- whether the **legitimate interest** is **not overridden by the data subjects' interests, rights or freedoms** (**balancing test**)[72]

As a general criterion, the legitimate interest can be invoked as a legal basis in so far as the data subject can reasonably expect, at the time and in the context of the collection of the personal data, that

[71] 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) 25 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>

[72] 'What is the 'legitimate interests' basis?' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/ and Rigas case (C-13/16, 4 May 2017)

processing for that purpose may take place[73]. 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.[74]

Example
A company offers a restaurant at home service. New clients may enjoy a free meal delivered at home. The offer is valid only once and per household. In this case, the company may compare its database of existing clients with its database of new clients to spot any frauds.

An online shop and requires the customers to share their e-mail addresses to give updates about the orders on the basis of consent.
If the shop decides to use the e-mail address also to send marketing materials, which entails a change in the purposes of the processing, for this new type of processing operations the shop may invoke the legitimate interest.

DPA decisions relevant for SMEs
Even if the GDPR provides that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest,[75] this is not automatically the case.
For example, the Dutch DPA imposed a fine against a tennis association for sharing its members' data with some sponsors.
In this case, the Dutch DPA denied that the mere commercial interest could constitute a legitimate interest,[76] but the decision is very 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

'Direct Marketing Recommendations' by Belgian DPA https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/02/Recommandation_01-2020_marketing_direct1-French.pdf

'Direct Marketing' by ICO https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

'Direct Marketing - What you need to know about direct marketing' by DPC https://www.dataprotection.ie/en/news-media/blogs/direct-marketing-what-you-need-know-about-direct-marketing

'La réutilisation des données publiquement accessibles en ligne à des fins de démarchage commercial' by CNIL https://www.cnil.fr/fr/la-reutilisation-des-donnees-publiquement-accessibles-en-ligne-des-fins-de-demarchage-commercial

[73] Recital 47 GDPR
[74] Recital 47 GDPR
[75] Recital 47 GDPR
[76] In this respect, see 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/

SMEs and employees' data

From a data protection point of view, in employment relationships, the employer has normally the role of the data controller, whereas the employee is the data subject.

Many activities performed routinely in the employment context entail the processing of workers' personal data, some of them belonging to the special categories of personal data as listed in Article 9 GDPR (e.g. trade union membership, health-related information).

Examples
Processing application forms and work references; preparing payroll; sharing with competent authorities tax information and social benefits information; keeping sickness records, annual leave records, unpaid leave/special leave records, annual appraisal/assessment records; maintaining records relating to promoting, transfer, training, disciplinary matters; having a registry related to accidents at work, etc.
Even monitoring of emails and calls and recording of workspaces, although for security purposes, involve the processing of personal data of employees.[77]

The GDPR gives Member States some flexibility as to the rules on personal data processing in the employment context. Member States are entitled to adopt specific rules -including collective and work agreements- concerning e.g. the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, etc.[78]

TIP
Since the GDPR gives some flexibility to the Member States as to the rules governing personal data processing in employment context, SMEs must preferably refer to national implementing rules of the GDPR or to the guidance issued by DPAs.

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

To process the personal data of their employees, SMEs need a legal basis.

In general, the choice to use consent for the processing of personal data in the employment context is questionable. As the GDPR requires that, to be valid, the consent must be freely given, this requirement can be affected due to the economic imbalance between employer and employees.[79] Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment.[80]

The more appropriate legal bases can be:

- the performance of a contract to which the employee is party

Example

[77] Article 29 Working Party, 'Opinion on the processing of personal data in the employment context' (2001) 1 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48sum_en.pdf> accessed 14 May 2020
[78] Article 88 GDPR and Recital 155.
[79] FRA/ECtHR/EDPS, *Handbook on European data protection law* (Publications Office of the European Union, 2018) 330 https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf
[80] Article 29 Working Party, 'Opinion on the processing of personal data in the employment context' (2001) 2 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48sum_en.pdf> accessed 14 May 2020

When meeting obligations under the employment contract, such as paying the employee[81].

- the compliance with a legal obligation to which the employer is subject

Example
When the employer communicates personal data of the employee for social security, welfare, or tax purposes.

When the employer is legally obliged to check the certificate of good conduct of (prospective) employees.

- the legitimate interest of the employer, in so far it is not overridden by the interests or fundamental rights and freedoms of a data subject.

Example
When a recruiter browses a publicly available database (as LinkedIn or similar) and contact a person to offer a job interview.

When a plumber communicates to a client the contact details of one of his/her workers to schedule an appointment.

To which extent can an SME monitor its employees?

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.[82]

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 relation (e.g. video-surveillance, GPS on vehicles used by employees) and even after the end of the working relations (e.g. if an employer control former employees' LinkedIn profile to be sure that s/he is not infringing the non-competition clause).[83]

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 the employees) but this activity is risky from a fundamental rights perspective. Systematic or occasional monitoring can infringe upon the privacy rights of the employees, but also 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.[84] That is why the employer has to be careful in motivating the necessity and the proportionality of the monitoring activity.

Example
An employer envisaging 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.

[81] Article 29 Working Party, 'Opinion 2/2017 on data processing at work'[WP249] (23 June 2017) 7 < https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169> accessed 14 May 2020
[82] ibid.
[83] ibid.
[84] ibid.

However, the employer has first to evaluate whether the data processing is by all means necessary for the purposes designated, and whether its implementation by a GPS device is proportionate to the limitation on the rights of the employees.
Employers must inform their employees of installing 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 would be disproportionate.

TIP
Notwithstanding national differences concerning the possibility for an employer to monitor his/her 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.
- privacy-friendly solutions should be preferred to the monitoring of the employees. For example, an employer should opt for the introduction of filters to websites accessible from the workplace rather than monitoring all the web activities of the employees.

SMEs and data subjects' rights

Background

Data subjects' rights are not a novelty in data protection legal landscape, but with the data protection reform they have been extended and better defined in their scope. As most data subject right mirror duties and obligations of the data controller, SMEs should be familiar with them.

Complying with data subjects' queries is a duty for SMEs acting as data controllers, whereas SMEs acting as data processors have to assist their data controllers in granting data subjects their rights[85].

In principle, the data controller replies to data subject queries 'without undue delay', and within 30 days[86]. 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. phone) or in writing (e.g. e-mail, post, social media).[87]

In so far as data subjects' requests are manifestly unfounded or excessive (e.g. repetitive), the controller may either charge a reasonable fee on the basis of the administrative costs bore, or refuse to act. Still, the controller will bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Before following up a request, the data controller verifies the identity of the person presenting it to prevent third parties to gain unlawful access to personal data.

[85] Article 28(3)(e) GDPR
[86] Article 12 (3) GDPR
[87] '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/

In some cases, requests can 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 his or her request and consent, if a data subject does not have the mental or legal capacity to manage his or her affairs).[88]

TIPS

- If a Data Protection Officer (DPO) is appointed, s/he will deal with the data subjects' requests.
- Having a policy to deal with data access request (specifying roles, internal deadlines, etc.) increases efficiency in dealing with such requests.
- Keeping written records of the (verbal) requests received and of the follow up help a company to demonstrates compliance with the GDPR in case of investigations by a DPA.

Useful sources

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

What are the data subjects' rights?

Right to transparency and information (Articles 12, 13, 14 GDPR)

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

- the main elements of processing operations (e.g. 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);
- possibility to claim data subjects' rights.

TIP

Article 12, 13 and 14 GDPR contain a detailed list of the information to be provided to data subjects and that SMEs shall include in their privacy and data protection notices.
In so far as a privacy/data protection notice is clear and transparent, this increase the trust of data subjects and, most likely, reduce the queries presented by data subjects.

The information must be concise, transparent, intelligible and easily accessible.

Example

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

- a layered approach;
- dashboards;
- just-in-time notices;
- icons;
- mobile and smart device functionalities;[89]
- cartoons, infographics, or flowcharts[90]

[88] Adam Panagiotopoulos, Data subjects' requests made on behalf of others: Practical considerations on data subjects' requests and elected representatives'< https://www.trilateralresearch.com/dpo/data-subjects-requests-made-on-behalf-of-others-practical-considerations-on-data-subjects-requests-and-elected-representatives/Z>

[89] '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/

[90] 'Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (Adopted April 2018) https://iapp.org/media/pdf/resource_center/20180413_Article29WPTransparencyGuidelinespdf.pdf

Useful sources
'Guidelines on transparency under Regulation 2016/679' by Article 29 Working Party https://iapp.org/media/pdf/resource_center/20180413_Article29WPTransparencyGuidelinespdf.pdf

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

'How to write clearly' by European Commission https://op.europa.eu/en/publication-detail/-/publication/725b7eb0-d92e-11e5-8fea-01aa75ed71a1/language-en

Template Privacy Policy https://gdpr.eu/wp-content/uploads/2019/01/Our-Company-Privacy-Policy.pdf

Right to access (Article 15 GDPR)

The right to access entails for the data subject the right to receive from the controller the confirmation if his/her personal data have been processed and, if so, get access to and a copy of the personal data processed.

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

Through the right to access, data subjects can verify the lawfulness of data practices of a data controller.

While the right to information under Articles 13 and 14 is meant ensure that the data subject receives a general and comprehensive picture of the processing, the right of access under Article 15 has the express aim of ensuring that the data subject receives information on the processing of his or her personal data in order establish and control the lawfulness of processing.

When replying to a data access request, the data controller shall provide the data subject the following information:[91]

- confirm whether personal data concerning the data subjects are being processed;
- provide a copy of the personal data undergoing processing (in so far as this does not affect the rights and freedoms of others);

Example
A data access request may regard a registry containing the personal data of the person advancing the request, but also personal data of others (but also trade secrets, intellectual property, etc.). 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 to comply with the request insofar as possible, whilst also ensuring adequate protection for the rights and freedoms of others.[92] For example, by giving access to the registry after deleting the personal data of the other people concerned.

- provide information as to:

[91] See Article 15 GDPR
[92] 'The Right of Access'https://www.dataprotection.ie/en/individuals/know-your-rights/right-access-information

- the purposes of the processing,
- the categories of personal data concerned (e.g. contact details, credit card details);
- the (categories of) recipients;
- the retention period, meaning for how long personal data will be stored, or the criteria to determine it;
- 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 right to lodge a complaint with a supervisory authority;
- the source of personal data, where they are not collected from the data subject;
- the existence of automated decision-making, including profiling, together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- the appropriate safeguards existing in case of a data transfer to third countries or international organisations (e.g. standards data protection clauses, binding corporate rules, a code of conduct, a certification)

TIP
When the data access request is broad, asking the individual to clarify its scope could reduce the time spent searching for and compiling data.

Useful sources
Right to access by ICO https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

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

Right to rectification (Article 16 GDPR)

Data subjects have the right to demand the data controller to correct the information concerning them.

The right to rectification is useful both for the data subjects and for the SMEs, that this way can rely on updated data.

The controller shall communicate any rectification to each recipient to whom they disclosed the personal data unless this proves to be impossible or involves a disproportionate effort.[93]

Right to erasure, i.e. right to be forgotten (Article 17 GDPR)

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

The controller deletes the personal data when:

- they are no longer necessary for the purposes for which they processed;
- they were collected in relation to the offer of information society services to children;
- they were unlawfully processed (e.g. without a legal basis);

[93] Article 19 GDPR

- the data subject withdraws the consent or objects the processing and there is no other legal ground for the processing;
- Union or Member State law requires the controller to do so.[94]

There are exceptions to the right to erasure, too. Among them: 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; establishment, exercise, or defence of legal claims, etc.

The controller shall communicate any rectification to each recipient to whom they disclosed the personal data unless this proves to be impossible or involves a disproportionate effort.[95]

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. The ability to restore erased data shall be finally terminated by all technically feasible means, too.

TIP
To increase efficiency, in order to grant the right to erasure in practice, a controller may implement a right to erasure request form on his/her website.

Useful sources
Right to erasure request form https://gdpr.eu/wp-content/uploads/2019/01/RIGHT-TO-ERASURE-REQUEST-FORM.pdf

Right to restriction of processing (Article 18 GDPR)

The data subject can ask the data controller to temporality limit the processing of his/her personal data if:

- the accuracy of the personal data is contested;
- the processing is unlawful and the data subject requests the restriction instead of the erasure;
- the data must be kept for the exercise or defence of legal claims;
- 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 rectification to each recipient to whom they disclosed the personal data unless this proves to be impossible or involves a disproportionate effort.[96] Furthermore, the controller must notify the data subject before the restriction on processing is lifted.[97]

Examples
Methods to grant the restriction of processing include:
- moving temporarily the selected data to another processing system;
- making the data unavailable to users;
- removing personal data temporarily.

[94] FRA/ECtHR/EDPS, *Handbook on European data protection law* (Publications Office of the European Union, 2018) 223 https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf
[95] Article 19 GDPR
[96] Article 19 GDPR
[97] ibid. 223

Right to data portability (Article 20 GDPR)

Under the GDPR, data subjects enjoy the right to data portability in situations where the personal data that they have provided to a controller are 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.[98]

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 develop interoperable formats that enable data portability for the data subject. Formats have to be machine-readable, structured, and commonly used, but the GDPR does not impose particular recommendations on the specific format to be used to achieve data portability.

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

Data portability can benefit SMEs to the extent that, if they are offering better services than a competitor, it is easier for the consumers to switch.

Example
Structured, commonly used and machine-readable formats appropriate for data portability include CSV, XML, JSON, RDF[99]

Right to object (Article 21 GDPR)

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;
- when the processing is performed by the controller for direct marketing purposes;
- when the processing of personal data is done in the context of information society services;
- when the personal data are processed for scientific, historical or statistical purposes

The right to object can be exercised by automated means, too.

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

Right not to be subject to a decision based solely on automated decision making (or processing), including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her

The 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, for example, data provided directly by the individuals concerned (such as responses to a questionnaire); data observed

[98] ibid. 228

[99] 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/

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).[100]

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 are suitable to have legal effects or to produce significant effects, and therefore a significant impact on the life of individuals, the data subject has the right not to be subject solely to these automated decisions.

Example
A company relies on an automated system to calculate the annual bonus to pay its employees. The payment of a bonus is deemed to produce significant effects on a person. The final decision on the bonus must be scrutinised by a human.

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

Useful sources
European Data Protection Board Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

[100] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (22 August 2018) 8 < https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053> accessed 14 May 2020

SME and the obligation to appoint a Data Protection Officer (DPO)

Is the appointment of a DPO mandatory for SMEs?

The main role of a Data Protection Officer (DPO) is to ensure that her organisation processes the personal data of its staff, customers, providers, or any other in compliance with the applicable data protection rules.[101]

Contrary to popular belief, decisive for the legal obligation to appoint a DPO is not the size of the company but the core processing activities which are defined as those essential to achieving the company's goals.

The appointment of a DPO regards both SMEs acting as data processors and data controllers.

It is mandatory only in certain cases:

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

Public authorities or bodies are legal 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.[102]

Normally, this situation does not regard SMEs.

Example
If an SME deals with public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing, etc. then it shall appoint a DPO.

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

Core activities refer to the main business pursued by the 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, albeit essential or necessary to a business, are considered ancillary (e.g. paying employees or having standard IT support activities).

Monitoring is when natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours, and attitudes.[103] The monitoring is **regular and systematic** when it is ongoing, or occurring at particular intervals of time, and is pre-arranged, organised, or methodical, taking place as part of a general plan for data collection or strategy.

Example
Activities that may constitute regular and systematic monitoring of data subjects include e.g. operating a telecommunications network; providing telecommunications services; email retargeting; data-driven marketing activities; profiling and scoring for purposes of risk assessment

[101] 'Data Protection Officer' https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

[102] See e.g. Case C- 279/ 12, Fish Legal and Shirley, para. 42 and case law cited therein.

[103] Recital 24 GDPR

(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 device.

The factors to consider to determine 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.

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

A medium-size tile manufacturing company subcontracts its occupational health services to an external processor, which has a large number of similar clients. The processor shall designate a DPO provided that the processing is on a large scale. However, the manufacturer is not necessarily under an obligation to designate a DPO.[104]

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 GDPR. They are those personal 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, data concerning a natural person's sex life or sexual orientation

Example
A laboratory that provides blood analysis has to appoint a DPO.

A criminal law firm or a clinic -but not an individual lawyer or health care professional-[105] have to appoint a DPO.

An SME providing dating app services has to appoint a DPO.

Who should be a DPO?

A DPO may either be an **employee of the SME** or an **external expert** but, in both cases, it is fundamental that he or she is **independent**, in the sense that:

- the DPO shall be provided with all the necessary resources to carry on his/her tasks, in terms of money, time, workforce, time to devote to professional development, etc.;
- the DPO shall not receive instructions for the exercise of his/her tasks;
- the DPO shall not be dismissed or penalized for the performance of his/her tasks;

[104] Article 29 Working Party, 'Guidelines on Data Protection Officers ('DPOs')'[WP243] (13 December 2016) https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[105] Personal data should not be considered 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)

- the DPO shall report to the highest level of management; and
- the DPO should not be in any conflicts of interest in respect to other tasks and duties (e.g. determining objects and purposes of the processing, representing the SME in a legal proceeding).

To ensure the independence of the function, at a practical level, when a DPO is an employee of the organisation, it must be made clear if he or she is acting in the DPO function or not.

Examples of incompatible positions

- Chief executive
- Chief operating
- Chief financial
- Chief medical officer
- Head of marketing department
- Head of Human Resources
- Head of IT department

As regards the level of expertise, it must be commensurate with the sensitivity, complexity and amount of data that an organisation process. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support.

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

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

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

- **Inform and advice** the SME on the obligations arising from the GDPR and other EU or national data protection provisions

Still, the DPO shall not be held accountable whether his/her advice is implemented or not in the SME.

- to **monitor compliance** of the SME with the GDPR, other national and EU data protection provisions and with any SME policy about the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

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.[106]

Again, the DPO cannot be considered personally responsible for non-compliance with the data controller or processor with data protection requirements.[107]

- to **provide advice** where requested **as regards the data protection impact assessment (DPIA) and monitor its performance**;

[106] Article 29 Working Party, 'Guidelines on Data Protection Officers ('DPOs')'[WP243] (13 December 2016) 24 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>

[107] ibid.

Example
An SME can ask advice to the DPO as to whether or not to carry out the DPIA process; the method to apply thereof; whether to outsource the DPIA process or not; the risk mitigation measures to apply; whether the DPIA has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) comply with data protection requirements.[108]
The DPO cannot perform the DPIA himself/herself.
This task would be incompatible with the independence requirement, as the DPO entrusted with the performance of the DPIA would combine the functions of an assessor and an auditor of the DPIA process. Nevertheless, the DPO will play a fundamental role in assisting the controller.

- to **cooperate with the supervisory authority** (i.e. DPA);
- to act as the **contact point for the supervisory authority** on issues relating to processing and to consult, where appropriate, with regard to any other matter.

Example

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

It is questioned the possibility for a DPO to represent the SME in front of the DPA or a court in case of proceedings, as this would be incompatible with the independence required from this function[109]

- **Handle data subjects' requests and complaints**
- **Fulfill other tasks and duties**, providing that they do not result in a conflict of interests.

Example
A DPO can be tasked to create and maintain the register of the processing activities, under the responsibility of the controller or processor. Such records should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.[110]

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 certification.[111]

Can an SME share a DPO with other organisations?

Appointing a joint DPO may be a practical solution for a group of SMEs. Such a possibility is foreseen by the GDPR, on condition 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 organisation.

[108] ibid. 25

[109] Judit Garrido-Fontova, '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> accessed 14 May 2020

[110] Douwe Korff and Marie Georges, *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

[111] ibid. see Tasks 10, 11.

What to consider 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 and dealing with stakeholders.
- When the SME is entrusted with the performance of services of public interest, albeit it is not mandatory, it is recommended that the SME designates a DPO.[112]
- The level of expertise requested by a DPO depends on the riskiness of the processing operations.

TIP

Keeping written documentation explaining why an enterprise chose (not) to appoint a DPO, and why his/her level of expertise was deemed appropriate, may support an SME to demonstrate compliance and accountability in case of an investigation by a DPA.

Similarly, when an SME decides to pursue an activity in contrast with the advice of the DPO, it should document the reasoning to demonstrate compliance and accountability in case of an investigation by a DPA.

Even if no legal obligation exists, companies can appoint a DPO on a voluntary basis to help with data protection compliance.[113]

Useful sources

Article 29 Working Party, Guidelines on Data Protection Officers("DPOs")' (adopted on 5 April 2017), in Particular the Annex https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

Douwe Korff and Marie Georges, *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* https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf

DPA decisions concerning SMEs

A German SME active in the telecommunication sector was fined by the Federal German DPA because the company did not comply with the legal requirement under Article 37 GDPR to appoint a data protection officer despite repeated requests. The amount of the fine of 10,000 euros was established taking into account that this is a company from the category of micro-enterprises.[114]

[112] Article 29 Working Party, 'Guidelines on Data Protection Officers ('DPOs')'[WP243] (13 December 2016) 24 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048> 6

[113] http://www.project-star.eu/ , Training materials: Topic 5 – Role of the DPO

[114] '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> accessed 14 May 2020

III. SMEs AND THE RISK-BASED APPROACH IN THE EU DATA PROTECTION FRAMEWORK

The articulation of the risk-based approach has led to the principal novelties of the EU data protection framework.[115]

The risk-based approach in data protection builds upon the idea that the sole respect of data protection principles is not sufficient to protect the fundamental rights and freedoms of individuals. [116] To adapt to the transforming and more and more complex data processing realities, compliance with those principles needs to be combined with risk analysis and risk management.[117] In other words, the risk-based approach is aimed at giving the data protection principles more substance to tailor them to the compound of evolving data processing situations.[118]

Following the risk-based approach, data controllers and processors are expected to engage in a risk management process, i.e. a series of coordinated activities to direct and control their organisation with regard to risk.[119]

The three basic steps of risk management are:

1) Identification of the risks;
2) Evaluation (and prioritisation) of the risks;
3) Plan and control the risks.[120]

What is a risk in the GDPR?

The understanding of 'risk' in law -and specifically in European data protection law- is still evolving.[121] Up until now, 'risk' pertained more to the areas of technology, economics, natural sciences, etc.

In general, risks can be 'subjective'[122] and 'objective'[123], as well as voluntarily undertaken,[124] societally imposed,[125] discrete and pervasive.[126] Any of such risks can be evaluated from different perspectives (e.g. technological, economics, psychological).[127]

The perception of risk is variable, being affected by different attitudes, how information is given and portrayed, the familiarity of the person with an activity or hazard, etc.[128] Other elements that can play

[115] Albeit the risk-based approach itself is not entirely new in data protection law. See Article 29 Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (2014) 2 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf> accessed 22 April 2020.
[116] Principles related to the processing of personal data are listed in Article 5 GDPR and encompass: lawful, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality.
[117] Raphaël Gellert, '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
[118] ibid
[119] 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' (2017) 6.
[120] Paolo Rossi, How to link the qualitative and the quantitative risk assessment'. Paper presented at PMI® Global Congress 2007—EMEA, Budapest, Hungary. Newtown Square, PA: Project Management Institute.
[121] ibid 6.
[122] Subjective risk assessment entails non-expert perceptions by the public.
[123] Objective risk is assessed scientifically by experts and is probabilistic.
[124] For example, by taking some drugs, such as contraception.
[125] For example, a nuclear power plant.
[126] The latter includes risks that are bound to happen, such as an earthquake.
[127] Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy, and Practice* (Oxford University Press 1999) 139.
[128] Paul Slovic, 'Perception of Risk' (1987) 236 Science 280–285.

a role are the degree an individual feels in control; whether an individual is exposed to an activity voluntarily; the perceived benefits of an activity.[129]

The GDPR does not contain a definition of `risk' but the WP 29 suggests that '**a "risk" is a scenario describing an event and its consequences, estimated in terms of severity and likelihood**.'[130] More specifically, in data protection law, risks relate to **threats to the rights and freedoms** of individuals whose personal data are being processed (i.e. data subjects) or natural persons more in general. 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.[131]

The risks to the rights and freedoms of natural persons may result from personal data processing activities which could lead to physical, material, or non-material damage of an individual.[132]

Example
If a clinic does now keep the data of the patients accurate and up to date, this can prejudice the health or the life of the patients.

In the case of self-driving vehicles, the passengers of the vehicle may not be data subjects under the GDPR because their personal data may not be processed. Still, their health or life may be endangered by the processing operations performed by the vehicle.

How to evaluate risks under the GDPR?

Under the GDPR, different risk levels trigger the applicability of different legal obligations.

The Regulation distinguishes at least three types of risk situations for the rights and freedoms of individuals deriving from the processing operations:

1) low-risk situations

2) risky situations

3) high-risk situations.

One company can have multiple processing operations of personal data in place, and they may be on various risk levels.

Example
The risks may result from a personal data processing which could lead to physical, material or non-material damage.
This happens where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in

[129] ibid.
[130] 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' (2017) 6.
[131] ibid.
[132] Recital 75 GDPR

particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.[133]

Typically, the risk level is assessed by combing the likelihood or probability (of the risk to materialise) and the severity (of the consequences due to the materialisation of the risk).[134] 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.[135]

Risk can be assessed qualitatively or quantitatively or combining the two. Quantitative risk assessment requires very precise values, namely the definition of the probability of each single risk factors occurrence (expressed in a scale 0-1), and the quantitative definition of its severity. Qualitative risk assessment, in turn, assumes the impossibility of getting such precise values and uses instead different levels of likelihood and severity, expressed in scale. Short of data security, the risks to the rights and freedoms of natural persons are suitable to be evaluated qualitatively.[136]

Example
As general rule, from a data protection perspective, certain business sectors are presumed to be riskier than others (e.g. health care services; solvency and creditworthiness; creation and use of profiles (profiling); political, trade union or religious activities; telecommunications services; insurances; banking and financial companies; social services activities; advertising; large-scale CCTV (Closed Circuit TV) (Video surveillance of major infrastructures such as railway stations or shopping centres).
Similarly, the processing of certain types of data (e.g. 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 (e.g. 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, ISP); 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).[137]

[133] Recital 75 GDPR
[134] Paolo Rossi, How to link the qualitative and the quantitative risk assessment'. Paper presented at PMI® Global Congress 2007—EMEA, Budapest, Hungary. Newtown Square, PA: Project Management Institute.
[135] Recital 76 GDPR, EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Adopted (13 November 2019) para 27
[136] Paolo Rossi, How to link the qualitative and the quantitative risk assessment'. Paper presented at PMI® Global Congress 2007—EMEA, Budapest, Hungary. Newtown Square, PA: Project Management Institute.
[137] Facilita RGPD' https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd

Examples of likelihood and severity scales (1-5):[138]

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 on personal data, minor economic loss etc.)
S3	Medium - Physical, material or non-material damage to rights and freedoms of data subjects (e.g. restrictions in exercise rights)
S4	High - Significant physical, material or non-material damage to rights and freedoms of data subjects that can be overcome with difficulty by data subjects
S5	Critical - Irreversible physical, material or non-material damage to rights and freedoms of data subjects

Value	Likelihood of occurrence
L1	Remote - it does not seem possible for the selected risk sources to materialize
L2	Unlikely - it seems difficult for the selected risk sources to materialize
L3	Occasional - it seems possible for the selected risk sources to materialize
L4	Likely - it seems highly possible for the selected risk sources to materialize
L5	Frequent - it is almost certain for the selected risk sources to materialize

Example of a risk matrix:

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 4 and 5;
Medium risk – between 5 and 9;
High risk – between 10 and 16;
Critical risk – ≥ 17.

Example of a data protection risk registry:[139]

ID	Risk Description	GDPR provision	Description of possible impact on data subjects	Likelihood	Severity	Magnitude
1	Unauthorised repurposing	Art. 5	Personal data are processed for purposes other than those originally identified	2	4	8
2						
…						

TIP

[138] As interpreted from 'Knowledge base for Privacy Impact Assessment https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

[139] Inspired from the Spanish Data Protection Authority 'Practical Guide for DPIAs', p 23-33.

Keeping a registry of risks related to the processing operations present several advantages. First, it raises awareness in an organisation about potential data protection issues associated with a project, and it allows to identify and mitigate against data protection risks. Consequently, it supports the choice of the most appropriate technical and organisational measures to ensure data security and data protection by design and by; it may facilitate the performance of a data protection impact assessment (DPIA) when required; it may help an organisation to demonstrate compliance with the law in the event of a regulatory investigation or audit.[140]

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

Risk assessment and data protection planning https://tietosuoja.fi/en/risk-assessment-and-data-protection-planning

Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales sujetos al RGPD' by AEPD https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf

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 strictly 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);
- Article 36 on prior consultation.

While the formulation of the risk-based approach to some degree varies 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 entails that the data controllers and processors need to **adjust some of the data protection obligations to the risks presented by a data processing activity**.[141]

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

- taking into account;[142]
- the state of the art (in terms of technical and organisational 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

[140] Risk based approach' https://dataprotection.ie/en/organisations/know-your-obligations/risk-based-approach
[141] Christopher Kuner, Lee Bygrave and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP; 2020), 26
[142] The formulation 'taking into account' entails there is not only one solution possible to comply with the risk based approach, but there are several elements to consider (i.e. the state of the art, the costs of implementation, etc.).

processing.[143]

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).[144]

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 purposes of the processing operations.

Considering the compliance with the GDPR through the lens of a risk-based approach is particularly useful for SMEs for several 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;
- the risk-based approach allows SMEs to frame data protection requirements flexibly. It does not prescribe or demand a particular measure to comply with the law. Instead, it requires to understand 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 are being processed. In practice, this entails that the GDPR grants SMEs enough margin to customise technical and organisational solutions to their specific needs.[145] Also, the state of the art depends greatly on applications and sectors;[146]

Albeit the risk-based approach is easy to spot in the text of the GDPR, its practical application still raises practical and theoretical concerns. 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 purposes of the processing).

A closer look to the GDPR provisions embedding a risk-based approach

Article 24 on the responsibility of the data 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. However, data processors are expected to be accountable, too, as they have to comply with obligations related to accountability and assist the data controller in some of the compliance

[143] Add Reference

[144] EDPB, Guidelines 4/2019on Article 25 Data Protection by Design and by Default, Adopted on 13 November 2019, 9.

[145] Belgian DPA, RGPD vade-mecum pour les PME - Un guide pour préparer les petites et moyennes entreprises (PME) au Règlement général sur la protection des données (January, 2018) 5 < https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/PME_FR_0.pdf> accessed 22 April 2020

[146] For further information concerning the state of the art technical and organisational measures, see ENISA and TeleTrusT - IT Security Association Germany, 'Guideline state of the art – Technical and Organisational measures' (2020) <https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/2020-01-TeleTrusT_Guideline_State_of_the_art_in_IT_security_ENG.pdf> accessed 13 May 2020

requirements.[147] Hence, the principle is relevant for any SMEs, regardless of their role in the processing operations.

Accountability can be defined as both a virtue that entails "a normative concept, as a set of standards for the behaviour of actors or as a desirable state of affairs" and as a mechanism "that involves an obligation to explain and justify conduct".[148] An example of such a mechanism could be an obligation to demonstrate that the processing of personal data complies with the EU Data Protection Framework.

In the field of data protection and privacy, "accountability is [considered to be] a form of enhanced responsibility"[149] or "a proactive demonstration of an organization's capacity to comply" with the GDPR.[150] Accountability can boost transparency and confidence for both regulators and data subjects, and ensure greater transparency of corporate practices.[151]

The actual recognition of the principle of accountability within the GDPR marks a shift from a primarily reactive approach to proactive compliance and practice.[152] Whereas (mere) compliance entails that an SME meets certain rules, the accountability principle goes further: SMEs have to demonstrate their commitment to protecting personal data.[153] For example, a risk assessment, or the evaluation of the 'appropriateness' of technical and organisational measures, cannot be reduced to mere 'tick boxes' exercises.[154]

What does an SME need to do to be accountable?

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

When taking such measures, the controller has to consider the nature, scope, context, and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.[155]

Even an SME acting as a data processor has to provide sufficient guarantees to implement appropriate technical and organisational measures in a way that the processing will meet the requirements of the GDPR end ensure the protection of the rights of data subjects.[156]

TIP

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

[148] Mark Bovens, 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism', (2010) WEP 946 — 967

[149] Colin Bennett, 'The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats' in Daniel Guagnin et al. (eds.), *Managing Privacy through Accountability* (Springer 2012) 46

[150] Joseph Alhadeff, Brendan van Alsenoy and Jos Dumortier, 'The accountability principle in data protection regulation: origin, development and future directions', in Daniel Guagnin et al. (eds.), *Managing Privacy through Accountability* (Springer 2012)

[151] ibid

[152] Add reference

[153] Paul De Hert, 'Accountability and System Responsibility: New Concepts in Data Protection
Law and Human Rights Law' in Daniel Guagnin et al. (eds.), *Managing Privacy through Accountability* (Springer 2012)199, 202

[154] Dariusz Kloza 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> accessed 13 May 2020

[155] Article 24

[156] Article 28(1) GDPR

Keeping written documentation about the technical and organisational measures in place, explaining why the measures were chosen, is an effective way to demonstrate accountability and compliance with the law.

What are the other examples of accountability measures?

Several provisions in the GDPR operationalise accountability. For example:

- Adopting and implementing data protection policies at the organisational level of an SME;
- Following a 'data protection by design and default' approach[157];
- Concluding written agreements between (joint) controllers, data controllers and data processors, and processors and sub-processors, specifying reciprocal roles and responsibilities;
- Maintaining documentation of the processing activities;[158]
- Implementing appropriate security measures;[159]
- Maintain procedures to respond to requests for access to personal data;
- Publish privacy policies on the internet;
- Have a data protection incident response plan in place;[160]
- Recording and, where necessary, reporting personal data breaches to DPAs and data subjects;[161]
- Carrying out data a protection impact assessment (DPIA);[162]
- Adhering to codes of conduct, which focus on the proper application of the GDPR in different processing sectors and different kinds of enterprises;
- Adhering to certification mechanisms, seals, and marks, which promote different organisations' compliance with GDPR requirements.[163]

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 the controller's and processor's side.

What are the advantages of accountability for an SME?

The principle of accountability is a leverage for the implementation of good governance and best practices in SMEs and can increase efficiency.

Accountability is an incentive for businesses to keep their data house in order[164] and to be more aware of the data processing operations occurring within their organisation, to make the most of them. Accountability fosters the implementation of innovative technical and organisational measures, including data protection policies, within an SME.

Finally, accountability can increase the trust between SMEs and their clients, creating a competitive advantage.

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

[157] Article 25 GDPR
[158] Article 30 GDPR
[159] Article 32 GDPR
[160] http://www.project-star.eu/, Training materials: Topic 4 – Responsibilities of data controllers and processors
[161] Articles 33 and 34 GDPR
[162] Article 35 GDPR
[163] 'Accountability tools' <https://edpb.europa.eu/our-work-tools/accountability-tools_en> accessed 13 May 2020
[164] Commissioner 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

Data (WP 168, 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 (WP 173, 13 July 2010) https://www.dataprotection.ro/servlet/ViewDocument?id=720

Article 25 on data protection by design and data protection by default

Background

With the entry into force of the GDPR, Data Protection by Design and Data Protection by Default (DPbD and DPbDf) principles became legal obligations for data controllers. The importance of these principles has grown in proportion to the deadline for the GDPR implementation and the fears over looming fines.

DPA decisions concerning SMEs
The Baden-Württemberg DPA issued a fine of 20.000 Euro 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 involving 333.000 users.[165]

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 shielding the meaning of these principles.[166]

Short of pseudonymisatiom, the GDPR does not provide examples of the technical and organisational measures complying with this 'by design' and 'by default' approach.

The choice depends on the fact that the GDPR aims to be a technology-neutral instrument suitable to adapt itself to the evolution of technology.

This approach is an advantage for SMEs, that are not bound to adopt predefined measures to comply with data protection by design and by default principles but can adopt customised solutions.

What does data protection by design entail?

The principle of data protection by design requires the data controller to implement both organisational 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 initiating it as well as at its later stages (e.g. including tenders, outsourcing, development, support, maintenance, testing, storage, deletion, etc.). It is an expression of a lifecycle thinking applied to the processing activity.[167]

The data controller has to do so by taking into account:

[165] See press release (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/> accessed 13 May 2020

[166] Michael Veale, Reuben Binns and Jef Ausloos, 'When data protection by design and data subject rights clash' (2018) International Data Privacy Law, ipy002, https://doi.org/10.1093/idpl/ipy002.

[167] European Data Protection Supervisor, 'Opinion 5/2018 Preliminary Opinion on privacy by design' (31 May 2018) para 10 <https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf> accessed 13 May 2020

- 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 (circumstances of the processing) and the purposes/aims of the processing;[168]
- the state of the art of the existing technical and organisational measures, which is very variable;
- their cost of implementation, including either money, time, and human resources;
- the risks of vary 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 organisational measures and necessary safeguards into the processing. An example of measure (the only one mentioned in the GDPR) is the pseudonymisation;
- implement data protection principles[169] and integrate the necessary safeguards into the processing to meet the requirements of this Regulation and protect the rights of data subjects.[170] Another example of the 'by design' approach is the performance of DPIA[171];
- in an effective manner;
- at the time of the determination of the means for processing, at the time of the processing itself with a view also the phase following the conclusion of it (lifecycle thinking).

The technical or organisational 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.). Yet, some DPAs (e.g. DPC) expects as a minimum the implementation of encryption as a technical solution, whenever possible, where personal data is at rest or in transit.[172]
There is no requirement for the sophistication of a measure, as long as it is appropriate for implementing the data protection principles effectively.[173] This means that there are no specific measures that ensure, automatically, 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, either traditional data security technologies (e.g. anonymisation, encryption cryptography, both for personal data at rest or in transit) and other tools aimed more in general at strengthening data protection: for example, antitracking tools for web browsing; dashboards and other users' 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 data controller or to customise the terms and conditions of privacy policies.[174]

---

[168] European Data Protection Board 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (13 November 2019) para 27 < https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en> accessed 13 May 2020
[169] See Article 5 GDPR
[170] See Chapter III GDPR
[171] European Data Protection Supervisor, 'Opinion 5/2018 Preliminary Opinion on privacy by design' (31 May 2018) para 10 <https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf> accessed 13 May 2020
[172] Add reference
[173] European Data Protection Board 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (13 November 2019) para 9 < https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en> accessed 13 May 2020
[174] See e.g. Steve Kenny, '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 Yun Shen and Siani Pearson 'Privacy Enhancing Technologies: A Review' <https://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf> all accessed 13 May 2020

The use of PETs may give a competitive advantage to SMEs, including those acting as data processors, aimed at attracting data protection aware clients.
Furthermore, the development of new PETs may represent a business opportunity for SMEs. Even if DPbD is a legal obligation only for data controllers, producers of the products, services, and applications based on the processing of personal data should be encouraged to take into account the right to data protection when developing and designing such products, services, and applications, to make sure that controllers and processors can fulfill their data protection obligations.[175]

ENISA is currently working on establishing a PETs repository and a tool to assess the maturity of the technologies.[176]

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

The appropriateness of the measures is strictly related to their effectiveness. **Effectiveness** means that controllers **must be able to demonstrate** that the measures chosen are suitable to achieve the goals of data protection by design, having regard to the actual processing operations.

It is therefore not enough to implement generic measures solely to document DPbD compliance but each implemented measure must have an actual effect. [177] The measures should be designed to be robust and be able to be scaled up in accordance with any increase in risk of non-compliance with the 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 the SMEs with the data protection ones.

Example

To establish smart (Specific, Measurable, Attainable, Relevant, Time-bound) 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 subject more privacy and demonstrate compliance with the GDPR)
- Why the desired outcome matters (e.g. to have a competitive advantage comparing with other SMEs providing similar services, and avoiding being sanctioned)
- How the progress will 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 that.
- How the SME can influence the outcomes (e.g. adopting PETs or recruiting additional staff)
- To indicate the responsible persons for the realisation of the outcomes

[175] Recital 78 GDPR

[176] 'ENISA PET maturity assessment repository' <https://www.enisa.europa.eu/publications/enisa2019s-pets-maturity-assessment-repository> accessed 13 May 2020

[177] European Data Protection Board 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (13 November 2019) para 14 ss < https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en> accessed 13 May 2020

- To indicate explicit targets to achieve the outcome (as e.g. the reduction of complaints of data subjects of X%)
- To indicate how often the progress towards the outcome will be reviewed[178]

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

What does data protection by default entail?

Data controllers shall also implement appropriate technical and organisational measures for ensuring that, by default, only those personal data which are necessary for each specific purpose of the processing are 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.[179] 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 their processing, the period of their storage, etc.

Data protection by default can be nuanced in an organisational sense, too.[180]

What are the examples of measures implementing data protection by default?

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

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

Example

If a bookshop is considering selling books also online, both in paper and in e-book formats, it should provide for different web forms to place the orders: whereas in the former case knowing an address of the client is necessary for the delivery, in the second it is superfluous.

- Adopt clear policies concerning data deletion (affecting the period of storage)

Example

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

- Avoid pre-ticked boxes that nudge the clients to accept the provision of extra services (affect the extent of processing)

[178] Mohammed Badawya 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> accessed 13 May 2020

[179] European Data Protection Board 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (13 November 2019) para 39 ss < https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en> accessed 13 May 2020

[180] ibid.

Example
When setting up cookies on its website, a company avoids pre-ticking the boxes for not necessary cookies.

To implement organisational measures aimed at data protection by default, an SMEs can:

- Establish access control policies to personal data (which affects the accessibility to data).

  This means limiting the number of employees who can have access to personal data based on an assessment of necessity, and also make sure that personal data is accessible to those who need it when necessary. Access controls must be observed for the whole data flow during the processing.

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

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

Useful sources
ENISA PET maturity assessment repository https://www.enisa.europa.eu/publications/enisa2019s-pets-maturity-assessment-repository

EDPS Opinion 5/2018 Preliminary Opinion on privacy by design (31 May 2018)

EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Adopted (13 November 2019)

Article 30 on the record of processing activities and other documentation

Background

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

For many micro, small, and medium-sized organisations, where data processing does not represent the core business, maintaining a record of processing activities may not be necessarily a burdensome activity. Conversely, it could be a tool to strengthen the good governance of the SME.

What does documentation require?

Both data controllers and data 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 data 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. …) with whom the data may be shared, specifying if they are outside the European Economic Area (EEA) or international organisation;
- In case of international data transfers, the identification of the country outside the European Economic Area or to the international organisation to whom personal data are transferred;
- where possible, the applicable data retention periods; and
- where possible, a description of the security measures (e.g. …) implemented in respect of the processed data.

For the SMEs acting as data processors, the information must include:

- the name and contact details of the processor/representative/ DPO /controller on which behalf the processor is acting;
- Categories of the 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 to the international organisation to whom personal data are transferred
- where possible, a description of the security measures implemented in respect of the processed data.

TIP

Albeit not expressly required, it is best practice to include in the register also the legal basis under which data are processed or transferred to countries outside the EEA, attaching also the written data-sharing agreements between the (joint) controller(s), the data controller and the processor, the processor and the sub-processor.

The GDPR does not explicitly require data controllers to maintain a detailed records of all data transfers. Yet, under the principle of accountability, the data controller shall be able to demonstrate the lawfulness of data processing. This obligation can be best met by recording all the details of the personal data transfers.

When discussing the documentation obligation, alternative terms are being used, including but not limited to, 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.[181] The controller (and the processor) chooses whether to keep such records in paper or electronic form.

TIP

Maintaining documentation electronically has the advantage that it can easily be added to, have entries removed, and amended as necessary. Paper documentation is however regarded appropriate for SMEs and micro-enterprises.

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

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 (meaning that it is 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, only a few SMEs can avail, entirely, of this exemption.

Example
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 and most employees' files include also special categories of personal data.

An insurance company occasionally carries out an internal staff engagement survey. Since the company doesn't do this particular processing activity very often, it does not need not document it as part of its record of processing activities. However, if the company occasionally does profiling on its customer database, for insurance-risk classification, the company must still document it because profiling is a risky processing operation. [182]

A tattoo shop keeps a record of the processing activities concerning the health-related data of its client.

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.[183]

TIP
Even for SMEs falling within the exemption, it would be convenient to maintain a record of the occasional processing activities performed. This way, it would be much easier for them to cooperate with DPAs if an investigation is started and to demonstrate compliance with other GDPR requirements.[184]

Data processors and data controllers can put in place a single set of shared records that they can quickly make available to the DPA upon request. If an organisation fulfills the role of both controller and processor for a particular activity at the same time, the records may be split up to correspond to those respective roles.[185]

What are the other types of documentation required by the GDPR or desirable?

Other than keeping a record of the processing activities, there are other types of documentation, that should be kept in writing because useful to support the data processors and the data controllers in their duty to demonstrate their accountability and compliance with the GDPR.

[182] 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

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

[184] Belgian DPA, 'Recommandation n° 06/2017 du 14 juin 2017' <https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/recommandation_06_2017.pdf> accessed 13 May 2020

[185] Belgian DPA, 'Recommandation n° 06/2017 du 14 juin 2017' <https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/recommandation_06_2017.pdf> accessed 13 May 2020

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, data controllers and data processors, and processors and sub-processors, specifying reciprocal roles and responsibilities
- Keeping track of the DPO advices (mail, written opinions, etc.);
- Keeping track of the decision on the (not) appointment of a DPO;
- Keeping track of the technical and organisational 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 breach, its effects, and the remedial action to be 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;
- Keeping track of the legal bases and the review of them.

Useful sources
EDPS, Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies (16 July 2019) https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en

Templates of Register of Processing activities are available
- on ICO website https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

- on CNIL website https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

- on page 158 and following of Douwe Korff and Marie Georges, *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*
https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf

TIP
When downloading a template an SME has to consider whether it acts as a controller or as a processor within the particular processing operation(s) to be documented

Article 32 on the security of processing

Background

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

- the pseudonymisation 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 organisational measures for ensuring the security of the processing.

How the security obligation is 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 such a processor where they have faith in their ability to comply with the obligations under GDPR.

During this process, the controller may take into account whether the processor provides adequate documentation proving compliance with data protection principles that could be found in privacy policies, records management policies, information security policies, external audit reports, certifications, and similar documentation. The controller in particular should take into account the processor's expert knowledge (e.g. technical expertise when dealing with data breaches and security measures), reliability, and its resources. A site visit may also be necessary. After carrying out the due diligence process, the controller should be able to decide with sufficient evidence demonstrating that the processor is suitable, it can then enter into a binding arrangement.

This due diligence process is not a one-time effort. The controller will have an ongoing obligation to check whether the processor is compliant and meeting their obligations either by auditing using their 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 already setting out clear and precise data protection obligations and the nature of the processing in a detailed data processing agreement.

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

What organizational security measures can an SME take?

- Carrying out an information risk assessment, focusing on the risks arising from an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.[186]
- Build a culture of security awareness within the organisation, by participating e.g. to training;
- Have an information security policy foreseeing the role of each user and the required permission levels (access control) appropriate to the role which minimises access to only that data necessary for that tole (e.g. system administrator accounts).

What technical security measures can an SME take?

Technical 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 IT security.

When considering physical security, elements to be considered are:

- the quality of doors and locks, and the protection of the business premises by such means as alarms, security lighting or CCTV;
- the access control to business premises, as well as the supervision of visitors;

[186] Article 32(2) GDPR

- 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 always 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 is held securely through the use of suitable levels of encryption);
- online security – e.g. the security 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 the security measures that an SME should have in place. Data controllers and processors are just required to have a level of security that is 'appropriate'. Both controllers and processors need to consider the appropriateness in relation to the risks for the rights and freedoms of natural persons, the state of the art 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 that there is no 'one size fits all' solution to information security. It means that what's 'appropriate' for each controller and processor will depend on their circumstances, the processing they are engaged, and the risks it presents to their organization as well as 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 will be expected to be implemented and documented.

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

Other factors to consider are:

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

Useful sources

European Union Agency For Network and Information Security, *Handbook on Security of Personal Data Processing* (December 2017) 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

DRAFT

Article 33 and 34 on personal data breach notification

Background

A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.[187] If the GDPR is breached differently (e.g. no adequate legal basis for a processing operation, inadequate information to data subjects), this does not fall under the obligations related to personal data breach. A breach of information security which does not compromise personal data does not fall within the scope of this obligation either.[188] That is why not all security incidents are personal data breaches, but every personal data breach entails a security incident. Among the causes of data breaches, are negligence, accident or technical failure, and intentional acts by internal or external actors.[189]

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 to the competent supervisory authority. When the risk to the rights and freedoms is high, the personal data breach shall be communicated to the data subject, too.

The obligation to notify personal data breaches to DPAs and individuals accompanies several other provisions, such as data protection by design, security measures, data protection impact assessments, and certification that also imbed the risk-based approach.

An obligation to notify personal data breach is both an accountability obligation and an obligation requiring 'additional measures when specific risks are identified'.[190] While being an accountability obligation, a data breach notification is also part of controllers' obligations, which 'can and should be varied according to the type of processing and the privacy risks for data subjects.'[191] Identification of risk of 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.

Under what conditions a notification to the DPA is required?

The GDPR requires that, when 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'.[192]

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;

[187] Article 4(12) GDPR.

[188] European Data Protection Supervisor, 'Guidelines on Data Breach notifications for the European Union Institutions and Bodies' (21 November2018) para 25 <https://edps.europa.eu/sites/edp/files/publication/18-12-05_guidelines_data_breach_en_0.pdf> accessed 14 May 2020

[189] ibid. para 29

[190] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks'(30 May 2014) 3–4. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf> accessed 14 May 2020

[191] ibid 3.

[192] Article 33(1) GDPR

- The measures the controller will implement to address the breach, eventually to mitigate its adverse effects.

If not all information is available, it can be provided to the 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 to confirm the breach of security concerning personal data.

The GDPR does not specify the practical aspects of such procedure.

At the same time, any entity handling information, including processing personal data, to run smoothly, must have appropriate governance or organizational structure 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. Having this contextual awareness as well as awareness of data breach risk is incremental 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 (PSD 2)).

In an ideal scenario, an information incident response policy should precede the occurrence of an incident so that it could be used should a data breach take place.

The GDPR requires that all the data breaches, regardless if notified to the DPA or communicated to the data subjects, are documented, including the effects and remedial actions taken.

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

The following documents in place would assist in case of a (personal) data breach:

> '1) **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 the 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 minimise 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 CSIR Team members in the execution of the CSIR Team.'[193]

Under what conditions a notification to affected individuals is required?

Individuals have to be notified when the breach is likely to result in a high-risks for their rights and freedoms. The threshold for the notification to individuals is higher than for the notifications to DPAs

[193] Kevvie Fowler, *Data Breach Preparation and Response: Breaches Are Certain, Impact Is Not* (2016) Kindle edition 50.

so that individuals are protected from 'unnecessary notification fatigue' and do not receive notification about all breaches.[194]

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

- **The type of breach**: the WP 29 deems that the level of risk presented by data breaches depends if the breach concerns the principle of confidentiality, the principle of integrity and the principle of availability.[195] While to some extent this may be true, the guidance fails to recognise that 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 an intention of attaining financial gains.[196]
- **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 is breached, the greater the impact may be anticipated, 'a small amount of highly sensitive personal data can have a high impact on an individual.'[197] It is also recognised that while data breaches concerning health data, identity documents, and credit card details entail risks, the possibility to combine this data creates higher risk than a single piece of information, as it subsequently could facilitate identity theft.[198]
- **Ease of identification of individuals**: when evaluating risks associated with a data breach, it is also important to consider for controllers whether the identification of individuals who were subject to a breach is going to be easy. In this regard, the controllers should be asking if the compromised data can be matched with other data sets and what kind of security measures were implemented (e.g., what is the level of hashing, encryption, or pseudonymization).
- **The severity of consequences for individuals**: the WP29 argues that controllers by taking into account the nature of the personal data involved in a breach (e.g., access to special categories of data, financial data) can anticipate the potential damage to individuals.
- **Special characteristics of the individual**: the controller when considering 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 not able to knowingly and thoughtfully oppose or consent 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 case the processing of personal data is not performed.
- **Special characteristics of the data 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.'[199]

Example

[194] ibid.
[195] ibid 7.
[196] Josephine Wolff, *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.
[197] Article 29 Data Protection Working Party, 'Guidelines on Personal Data Breach Notification under Regulation 2016/679' (n 207) 24.
[198] ibid.
[199] ibid 25.

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

- **The number of affected individuals**: finally, the controller needs to weigh the amount of personal data that was compromised. In general, it is argued that large scale data breaches will have a more severe impact, however, as pointed out already, a personal data breach involving special categories of personal data of one person can have a severe impact as well.[200]

As GDPR is maturing, different DPAs are expressing different thresholds for the reporting of breaches. Where originally there was a fear of over-reporting, the DPC in Ireland has requested a breach be reported when there is any risk identified to the data subject. This allows the Commission to identify trends and to have confidence that controllers are identifying the minor breaches and thus can identify the more serious breaches should they arise.

On the other hand, the test proposed by the WP29 to evaluate the risk that is likely to result from a breach is more finely defined and articulated. The test requires that each element is evaluated by the controller and that the decisions concerning notifications to DPAs and individuals are documented (i.e., to notify or not). The WP29 in its opinion regrettably avoids demonstrating how this test could play out in practice. Instead, it introduces an analysis suggesting that the following personal data breaches scenario are of high risk to rights and freedoms of individuals: exfiltration of data entered to the website (i.e., a data breach situation in case of British Airways breach in September 2018), ransomware attack encrypting data, an unauthorised access to customer data breach, cyberattack against a hospital medical records database, sending an email with personal data to the wrong list of recipients, sending a direct marketing email revealing other recipients.[201] In this regard guidance provided by national data protection authorities may be of great interest. The Irish Data Protection Commission, for example, in its guidelines provides for more specific scenarios explaining when notifications concerning personal data breaches should be made by the controller.[202]

Useful sources

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

Article 29 Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679' (6 February 2018) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

EDPS, 'Guidelines on personal data breach notification for the European Union Institutions and Bodies' (21 November 2018) https://edps.europa.eu/sites/edp/files/publication/18-12-05_guidelines_data_breach_en_0.pdf

[200] 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.

[201] Article 29 Data Protection Working Party, 'Guidelines on Personal Data Breach Notification under Regulation 2016/679' (n 207) 31–33.

[202] Irish Data Protection Commission, 'A Practical Guide to Personal Data Breach Notifications under the GDPR' (2019).

Article 35 and 36 on Data Protection Impact Assessment (DPIA) and prior consultation

Background

The 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, and are aimed to anticipate 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.[203] To be practical, impact assessments must be scalable, flexible, and applicable inter alia for large organisations, consortia, 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.

Accordingly, also the DPIA process has to begin *before* the starting of the personal data processing operations, and ideally already at their design phase. In no instances, DPIA can be used to retrospectively justify certain types of decisions (e.g. buying a drone, install 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, to minimise the negative consequences that the processing operations could have on the fundamental rights and freedoms of data subjects and natural persons.

DPIA, as other type impact assessments, constitute 'best-efforts obligation'. Being impossible to reduce negative consequences in absolute terms, SMEs have to react to them to the best of their possibilities, depending upon the state-of-the-art and their available resources.[204] Yet, the protection of personal data and compliance with the GDPR must be ensured.[205]

Who has to perform a DPIA?

DPIA is mandatory just for SME acting as data controllers, and only for certain processing operations. Albeit the data processor and the DPO shall assist, the data controller bears the final responsibility of the DPIA process.

TIP

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

[203] 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> [accessed 14 May 2020] and social impact assessments (SIA) were developed in the 1980s. SIAs aim at ensuring that developments or planned interventions maximise the benefits and minimise 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 <http://www.nmfs.noaa.gov/sfa/social_impact_guide.htm> [accessed 14 May 2020]

[204] Dariusz Kloza 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> accessed 13 May 2020

[205] Art. 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 is developing a piece of hardware or software, or offering data shredding and sanitizing services or cloud-based storage).[206]

As to the 'assessors', i.e. the persons or companies who will perform the assessment in practice, the data controller can choose to outsource the DPIA or to perform it 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 are not processed.

Example
In the case of self-driving vehicles, a pedestrian may not be a data subject but she is 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, there are data subjects rights as listed in the GDPR (right to access, right to erasure, rights to data portability, etc.); respect for private and family life, home and communications; freedom of thought, 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; right to asylum, right to access to documents; freedom to choose an occupation; right to education; right to property; equality between men and women; right of elderly; and many more.[207]

The GDPR leaves data controllers some amount of discretion in determining whether the envisaged processing operations fall within the pre-defined high-risk criteria[208].
However, certain elements contribute to qualifying the processing operations as 'likely to result in a high risk' for natural persons.

Example
There are is an inherent high-risk in processing operations entailing:
1) evaluation or scoring, including profiling and predicting,
2) automated-decision making with legal or similar significant effect,
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),

[206] European Data Protection Board, 'Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' [WP248] 8 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236> accessed 14 May 2020

[207] For other examples of fundamental right, 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 national Constitutional Charters of Member States.

[208] Dariusz Kloza 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> 3 accessed 13 May 2020

8) the use of innovative or new technological or organisational solutions (e.g. artificial intelligence, wearable devices),
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 his/her profile).
The data 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 data controller has to evaluate whether to notify a data breach to an individual.[209]

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 which is 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;

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

A company relying on automated systems for recruiting shall perform a DPIA

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

Example
A private clinic shall perform a DPIA.

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

Example
A security company providing CCTV surveillance in a shopping centre, or in a station shall perform a DPIA.

A DPIA is mandatory also when the processing operations are included in the lists of data processing operations requiring a DPIA compiled by the national DPA.[210]

TIP
The lists of processing operations requiring a DPIA are national and may be found on the website of the national DPA.

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

Examples
Situations that may trigger a DPIA:

- a jeweller planning to implement a tool to monitor access to the safe combining use of fingerprints and facial recognition;

[209] European Data Protection Board, 'Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' [WP248] 6 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236> accessed 14 May 2020
[210] Article 35(4) GDPR

- a biotechnology company offering genetic tests directly to consumers to assess and predict the disease/health risks;
- a company monitoring social media data to create profiles of clients or employees.
- eHealth apps developer
- a company implementing an automatic staff appraisal for assigning bonuses to its employees to increase salaries;
- an insurance company ranking clients for providing them insurance services;
- a private investigation service and handling data concerning criminal convictions and offences.

When DPIA is not required?

The GDPR expressly foresees situations where the DPIA process is not required.

- When the data processing operations are included in the list of data processing operations non requiring a DPIA compiled by the DPA(s) to which jurisdiction(s) the data controller is subject; (see useful sources to know where to retrieve them

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

- When the personal data are processed in order to comply with a legal obligation or in the public interest, on the basis of EU law or the Member State's law, and 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 this will be relevant for SMEs).
- When processing operations concern personal data from patients or clients by an individual physician, other health care professional or lawyer, because they are not considered to be on a large scale.

The mere fact that the conditions triggering the obligation to carry out DPIA have not been met does not diminish controllers' general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects. The requirement to have appropriate technical and organisation measures to mitigate the likelihood and severity of risks are part of general controller obligations, data protection by design and by default, data security. These are all horizontal requirements and exist regardless of whether the requirement to document them in a DPIA applies or not.

In case of doubt whether to conduct the DPIA or not, it is best practice to conduct the process.

When a new (revised) DPIA is required?

The risk-based approach entails that data 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". [211] 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 maintain the level of data protection in a changing environment over time.

[211] European Data Protection Board, 'Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' [WP248] 6 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236> accessed 14 May 2020

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

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 if a monitoring activity is no longer systematic. In that case, the review of the risk analysis made can show that the performance of a DPIA is no longer required.

How to conduct a DPIA?

The GDPR provides data controllers with a lot of flexibility to determine the precise structure and form of the DPIA. DPAs provided several methods and templates for carrying out the DPIA.

A proposed method for carrying out a DPIA, as interpreted from the GDPR and enriched with best practices, can be articulated into eleven steps.[212]

Step 1	*Screening* (*threshold analysis*).
Step 2	*Scoping*
Step 3	*Planning and preparation*
Step 4	*Description*
Step 5	*Appraisal of impacts*
Step 6	*Recommendations*
Step 7	*Stakeholders involvement*
Step 8	*Documentation*
Step 9	*Quality Control*
Step 10	*Prior consultation with a supervisory authority (DPA)*
Step 11	*Revisiting*

The first six steps are consecutive. Steps 7, 8, and 9 are on-going, in the sense that stakeholders' consultation, documentation, and quality control have to be reflected in all the steps. The last two steps are triggered only if certain conditions are met.

Step 1: Screening (threshold analysis)

In this step, the data 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*

[212] Dariusz Kloza et al. (2020) Data protection impact assessment in the European Union: developing a template for a report from the assessment process. *d.pia.lab Policy Brief No. 1/2020*. VUB: Brussels **(draft, forthcoming)**

In this step, the data 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 be, at least: the data subjects and their representatives (e.g. NGOs)[213]; the DPO[214]; and the data processor[215];

(c) which techniques will be used for assessing the impacts. The GDPR mentions only the necessity and proportionality assessment of the processing operations and the risk appraisal for the rights and freedoms of natural persons. However, they can be combined with others. 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 data 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, health impact assessment may be required by law or ethics impact assessment may be desirable.

Step 3: *Planning and preparation*
In this step, the data 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 necessary resources 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 of the DPIA process 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. data controller, data processors, assessors); natural disasters; utility failures, etc.

(g) the criteria triggering the revision of the process. Other than the change in the level of risk,[216] others are possible. For example, the data 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 data controller.[217]

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.

[213] Article 35(9) GDPR
[214] Article 39(c) GDPR
[215] Article 28(f) GDPR
[216] Article 35(11) GDPR
[217] Article 35(7)(a) GDPR

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 minimisation, accuracy, storage limitation, and integrity and confidentiality.

For the risk assessment, a typical method requires, first, a risk to be identified, i.e. to find, recognise and describe a risk. Second, the risk is analysed, i.e. its nature is comprehended in order to determine the level of risk, e.g. by multiplying the likelihood (probability) of its occurrence by the severity of its consequences. Third, the risk is evaluated, i.e. the results of risk analysis are compared with risk criteria (cf. *Step 3b)* in order to determine whether the risk and its level is acceptable, if any mitigation measure is to be recommended and if any risk needs to be treated with priority.

Step 6: *Recommendations*
In this step, mitigation measures to address the risks identified in the previous step and to demonstrate compliance with the law are suggested.

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 to comply with data minimisation; to reduce the data retention period).

Risk can be mitigated by manipulating either its likelihood (probability) – by e.g. limiting the exposure to a risk – or severity, or both. Risks can be avoided, mitigated, transferred (to another entity, e.g. outsource, insurance etc. or in time) or accepted; however, only in the first case a fundamental right will not be infringed. Residual risk is a risk that remains if there is no measure available to mitigate it and triggers a prior consultation with a DPA (cf. Step 10).

The mitigation measures can be both technical and organisational. They encompass the definition of policies and procedures for the protection of data; the allocation of defined roles and responsibilities as to the processing of personal data; the establishment access control policies to personal data; the creation of a data breach response plan; the setting up of a business continuity plan; the creation of logging and monitoring of data access; the use data deletion and disposal tool; etc.[218]

TIP
To demonstrate compliance, it is best practice to include the risks identified, their appraisal, their mitigation measures into a register.
Furthermore, the register may be forwarded to the competent DPA in case of prior consultation.

Step 7: *Stakeholders involvement*
To ensure the completeness and inclusiveness of the decision-making process, stakeholders must be involved in all the DPIA process. The data controller shall seek the views of the DPO of the data processor and, where appropriate, of the data subjects and of their representatives. Appropriateness does not mean optional: exceptions can be made only in so far as no new insight could be gathered from stakeholders, or stakeholder consultation would entail a disproportionate effort.[219] Nevertheless, other stakeholders may be identified (e.g. information security officer, if present). The views of the stakeholders are sought and taken into consideration, but stakeholders cannot decide about the DPIA. Any final decisions rely on the data controller.

Step 8: *Documentation*

[218] European Union Agency For Network and Information Security, *Handbook on Security of Personal Data Processing* (December 2017) Annex A <https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing> accessed 14 May 2020
[219] Kloza et al., 'Towards a method for data protection impact assessment: Making sense of GDPR requirements' (2019) *d.pia.lab Policy Brief*, 6 <https://cris.vub.be/files/48091346/dpialab_pb2019_1_final.pdf> accessed 14 May 2020

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

Step 9: *Quality Control*

The DPO is expressly tasked with monitoring the performance of the assessment process.[220] In addition to that, to be sure that the DPIA process adheres to a given standard of performance, an SME can use a progress monitoring tool.

Step 10: *Prior consultation with a supervisory authority (or DPA)*

Whereas the residual risk related to the processing operations remains high despite the adoption of mitigation measures, but the data controller decides 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 provides a just 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).

TIPS

DPAs provide prior consultation forms on their websites.

Step 11: *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.

Useful sources

European Union Agency For Network and Information Security, 'Handbook on Security of Personal Data Processing' (December 2017) 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

To consult the national lists of data processing operations (not) requiring a data protection impact assessment, it is possible either to visit the websites of the national data protection authorities or use the EDPB tool available here https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en

Templates for DPIA

From CNIL website https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf

From AEPD website https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-un-modelo-de-informe-para-ayudar-las-empresas

From ICO website https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

Dariusz Kloza, Alessandra Calvi, Simone Casiraghi, Sergi Vazquez Maymir, Nikolaos Ioannidis and Niels van Dijk (2020) Data protection impact assessment in the European Union: developing a template for a report from the assessment process. *d.pia.lab Policy Brief No. 1/2020*. VUB: Brussels **(draft)**

Software for DPIA

[220] Article 39(c) GDPR

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

IV. ENHANCING PERSONAL DATA PROTECTION

Codes of conduct (Article 40 GDPR)

Background

The Member States, the DPAs, the EDPB, and the Commission are expected to encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of SMEs. Codes of conduct are aimed at improving standards by following best practices concerning the processing of personal data in a specific sector or business, for both controllers and processors.

While codes of conduct are voluntary sets of rules that are developed by an organisation representing a sector or category of data controllers or processors (e.g. an association, a chamber of commerce), compliance monitoring against a code of conduct will be carried out by a body which has an appropriate level of expertise about the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.[221]

Codes of conduct must go beyond principles foreseen in the GDPR.

They 'must materially specify or enhance the application of data protection law to a certain sector or processing activity'.[222] In practice, this means, for a DPA to approve a code of conduct applicable in its territory, or for the EDBP 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 codes must specify the application of the GDPR to:

- fair and transparent processing;
- the legitimate interests pursued by controllers in specific contexts;
- the collection of personal data;
- the pseudonymisation of personal data;
- the information provided to the public and to data subjects;
- the exercise 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 for children 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 organisations; or
- 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?

Opting in for a code of conduct could be beneficial for an SME as it could facilitate its compliance with the GDPR requirements. It may be a cost-effective way of reducing non-compliance and therefore risk of fines.

[221] For the latest developments concerning such bodies, see updates on the EDPB website.
[222] DPC 'Codes of conduct' <https://www.dataprotection.ie/en/organisations/codes-conduct> accessed 14 May 2020

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.

Additionally, an SME should check whether the code of conduct has been approved by a DPA, or where appropriate by the EDPB or the 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 Commission.

Useful sources
Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 - version adopted after public consultation https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf

Certification (Articles 42 and 43 GDPR)

Background

The Member States, the DPAs, the DPB, and the Commission are expected to encourage the establishment of data protection certification mechanisms and data protection seals and marks for the purpose to demonstrate compliance with the GDPR of processing operations by controllers and processors.

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

1. the fact that the certification concerns the processing operation.
   More in details, when assessing a processing operation, the components to consider are the personal data (material scope of the GDPR); the technical systems -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 fact that the certification concerns personal data and privacy in a broad sense;
3. the voluntary nature of the certification;
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 EDPB. This entails self-certification schemes are excluded from the scope of Article 42 GDPR; [223]

What are the advantages of certifications for SMEs?

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

First, certifications can enhance trust for data subjects and clients, both in business-to-consumer and in business-to-business relations, offering them more transparency about the way personal data is processed by controllers and processors.[224]

[223] ibid

[224] European Commission 'Data protection certification mechanisms Study on Articles 42 and 43 of the Regulation (EU) 2016/679 : final report – Study' 4, 5 <https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en>

Secondly, certifications can reward privacy-aware technologies developed or employed by SMEs.[225] Building upon these two aspects, certifications can offer a competitive advantage for the SMEs choosing to apply for them.[226]

Furthermore, in case of data transfers (in the sense of transmissions of personal data outside the European Union), a certification can be used as a way of demonstrating that appropriate safeguards are in place for a controller or processor not subject to GDPR. in this sense, the existence of certification can be a legal basis for data transfers[227]

Certifications do not prove compliance with the GDPR themselves, but can be used by controllers and processors as a way of demonstrating the implementation of appropriate technical and organisational measures; the existence of sufficient guarantees for the relations processor-controller and sub-processor-processor.[228]

How to choose between different certifications?

At the moment of writing, there are no EU data protection seal (yet), nor approved national GDPR certification schemes. 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 upon GDPR requirements.[229]

Existing national and international certifications are different. Some of them are fully related to data protection, whereas others are partially related to data protection. 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 (thought for specific business activities, as cloud computing). Even for the multisector ones, there are multiple SMEs-friendly models. Some apply a pricing policy tailored to the size of the applicant, while others apply a free of charge or a discount policy to all the certification candidates.[230]

When approved national GDPR and European certification schemes will be approved, they will be distinguished between comprehensive GDPR schemes, covering the full breadth of the GDPR; and single-issue schemes, focusing on a particular GDPR sub-topics (e.g. data protection by design, children consent, etc.).[231]

For SMEs, certifications covering all facets of GDPR may be easier and more cost-effective than single issues schemes, but it has to be kept in mind that all certifications have limited duration in time. Certification have to be subject to revision when the legal framework of the jurisdiction they refer to is amended; national terms and provisions are interpreted by judgments; or the technical state of the

[225] 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. Kamara (https://iapp.org/news/a/four-gdpr-certification-myths-dispelled/)

[226] Ibid.

[227] Ibid.

[228] 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> accessed 14 May 2020

[229] Ibid.

[230] European Commission Data protection certification mechanisms Study on Articles 42 and 43 of the Regulation (EU) 2016/679 : final report – Study https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en

[231] ibid

art evolves.[232] In fact, the GDPR itself -for GDPR related schemes- provides for a maximum duration of 3 years.

Useful sources
Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf

For an exhaustive list of existing certifications, please refer to European Commission Data protection certification mechanisms Study on Articles 42 and 43 of the Regulation (EU) 2016/679 : final report – Study 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

DRAFT

[232] 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> accessed 14 May 2020

V. Bibliography

To be added

DRAFT