6 Part B – Handbook for Small and Medium-sized Enterprises (SMEs)

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)
CSIRT	Computer Security Incident Response Team
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
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)
PSD	Payment Service Directive
SME(s)	Small and Medium Sized Enterprise (s)
VDAI	Valstybinė duomenų apsaugos inspekcija (Lithuanian DPA)
WP29	Article 29 Working Party

6.1 Introduction

6.1.1 Background

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 data protection law. The Regulation covers only personal data, meaning any information relating to an identified or identifiable natural person.

The GDPR was introduced to update the former Data Protection Directive 95/46/EC to 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 in a more uniform way the free movement of personal data within the European Economic Area.[21]

Becoming the economy more and more digital and data driven, 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.[22] 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 benefit not only the newly established businesses, that often start digital, but also widen the business opportunities of the more traditional ones (e.g. with e-commerce).[23] Likewise, stronger data protection rules can boost business by increasing the confidence of consumers in the digital environment.[24]

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.[25] SMEs are not exempted from applying this new legal framework. Regardless their business sectors and their digitalisation level, the processing of personal data is unavoidable for the vast majority of the SMEs. 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 a CCTV system at the premises of an SME entails the processing of personal data, too.

The enforcement actions undertaken by several Data Protection Authorities (DPA) (or supervisory authorities) 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 costed 15.000 Euro to a Belgian company. Another SME continuously filming its employees at their workstation was fined 20.000 Euro by the French DPA (CNIL).[26] A small shipping company had to pay 5.000 Euro for missing a data processing agreement with one of the business partners.[27]

SMEs admittedly face several challenges when complying with the GDPR. Among them: the shortage of resources, in terms of time and money, to devote to data protection; the lack of internal expertise in data protection; misinformation about GDPR requirements; understanding what changes to implement to comply with GDPR; the scarcity of practical guidance and clarity on how to put into practice certain GDPR provisions.[28]

---

[21] 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

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

[23] 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> 0

[24] 'Data protection - Better rules for small business' <https://ec.europa.eu/justice/smedataprotect/index_en.htm>

[25] 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)

[26] ibid

[27] '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/> accessed 13 May 2020

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

Conscious of that, the STAR II consortium conceived this Handbook as a tool to support the SMEs in complying with the GDPR.

6.1.2 Methodology

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

That is why this handbook unpacks the GDPR provisions entailing a risk-based approach.

As noted by the European data protection regulators, a risk-based approach, while has been further articulated in the GDPR, is not a new addition to the EU data protection framework. Rather, it is an extension of the existing principles imbedded in the text of the Data Protection Directive, in particular, in the articles on the security (Article 17), the DPA prior checking obligations (Article 20) and the more stringent requirements for the processing of special categories of data (Article 8).[29] The notion of a risk-based approach in the GDPR is used in an attempt to update and modernise the EU data protection framework. The use of this notion allows to move from a legal compliance-based approach associated with provisions of the Data Protection Directive to 'a strong harm-based approach' focusing on 'responsible data use based on risk management'.[30]

This specific methodology has been chosen as a result of findings extracted during interviews conducted with 18 DPAs, 22 SME association representatives, 52-60 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.[31]

Additionally, the handbook aims at integrating other three recommendations, which were most frequently suggested by the respondents within the scope of the interviews conducted in 2019.[32] In particular, respondents suggested that the handbook could be:

1. A generic SME handbook focused predominantly on a compilation of examples and templates.
   That is why in each section of the handbook concrete examples and additional sources where SMEs can find templates and further guidance are provided.
2. 'Selling' the GDPR handbook.
   That is why the handbook suggests SMEs how to 'sell' their compliance with the GDPR, to transform it in a competitive advantage, and addresses also certifications and code of conducts.
3. Myth-busting handbook.
   That is why the handbook makes the GDPR understandable also for data protection newbies, at the same time proving that not necessarily the new rules introduced by the Regulation are as burdensome as they may appear to be.

Albeit from the interviews it resulted that a sector-specific handbook may have been beneficial, the consortium decided to follow a holistic approach and to create a handbook that could be useful for as many SMEs as possible, regardless their business area. Indeed, creating a sector specific handbook would have meant disregarding a large portion of SMEs. Still, to at least partially address the suggestion to provide a sector specific handbook, the authors will provide a wide range of examples to cover several business sectors.

Within the scope of STARII project, the NAIH (Hungarian Data Protection Authority) launched a hotline dedicated to SME enquiries. NAIH welcomed questions from SMEs based or functioning across the European Union (EU) about the interpretation and application of the GDPR provisions.

---

[29] Article 29 Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (2014) 2.
[30] ibid 3.
[31] 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).
[32] ibid.

In addition to that, the handbook covers other three topics that were found of particular concern for the SMEs that addressed to the hotline operated between 15 March 2019 and 31 March 2020 by the partner NAIH in order to assist SMEs with questions and uncertainties concerning compliance with the GDPR. These are: how to deal with consent of data subjects and the other legal basis; how to manage the data of employees; how to grant data subjects their rights.

6.1.3 Structure

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 developed by various DPAs across Europe and other bodies (as the European Data Protection Board (EDPB), which is the former Article 29 Working Party (WP29)). The text refers to national and European case law and DPA decisions when available and relevant for the interpretation of GDPR provisions.

At the end, a glossary explains data protection related terminology.

6.1.4 Added value of the handbook

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 manual 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 various templates and guidance on specific GDPR provisions provided by different DPAs and bodies across Europe, making their consultation easier.

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.

6.1.5 Target audience

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

6.2 DPAs guidance on GDPR compliance for SMEs

To enhance compliance with the revised EU data protection framework, DPAs independently and in the set-up of the EDPB 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 last review this included the DPAs from Belgium (APD-

GBA),[33] France (CNIL),[34] Ireland (DPC),[35] Lithuania (VDAI),[36] Slovenia (IP),[37] Spain (AEPD),[38] Sweden (Datainspektionen)[39] and the UK (ICO).[40] Some of these DPAs further distinguish guidance for micro-businesses.[41]

The guidance provided through the DPA websites and takes the form of either a downloadable document, a section of the DPA website or indeed a separate dedicated website. The approach taken in the SME specific guidance is usually holistic in terms of the issues covered, often presented in the same order as an SME might logically need to commence addressing data protection within their organisation. The issues typically include, in various presentation styles: key concepts of the GDPR (e.g. what is (not) personal data and the difference between personal data and special categories or the so called sensitive data), principles (e.g. accuracy, data minimisation, limited retention); data security obligations concerning technical and organisational set up of the processing; obligations concerning data subject rights; and the appointment of a Data Protection Officer (DPO), among others. These issues were often usefully identified to SMEs by the asking of positive questions or activity-based steps rather than approaching the issue in terms of the GDPR obligations.

Apart from guidance documents for SMEs, DPAs across the EU have reported that they engaged in numerous awareness raising activities.[42]

Templates, tools and guidance issued by any DPAs can be beneficial for any SMEs in the EU, regardless the place of establishment.

6.3 The concept of a risk-based approach in the EU data protection framework

6.3.1 The GDPR provisions embedding the risk-based approach

The articulation of the risk-based approach has led to the principal novelties of the EU data protection framework.[43]

---

[33] The Belgian Data Protection Authority operates in a number of languages. *L'Autorité de protection des données* (APD) is the French abbreviation simply translates as Data Protection Authority in English. CPVP, 'RGPD Vade-Mecum Pour Les PME (January)' (2018) <https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/PME_FR_0.pdf>.

[34] *La Commission Nationale de l'Informatique et des Libertés* (CNIL) meaning the National Commission of Information Technology and Freedoms. See, Bpifrance, '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>.

[35] *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>.

[36] *Valstybinė duomenų apsaugos inspekcija (VDAI)* meaning State Data Protection Inspectorate. 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>.

[37] Informacijski pooblaščenec (IP) meaning the Information Commissioner. See, 'Varstvo Osebnih Podatkov' (*Upravljavec*, 2018) <https://upravljavec.si> accessed 3 October 2019.

[38] Agencia Española de Protección de Datos (AEPD) meaning Spanish Data Protection Agency. See, 'Facilita RGPD' (*AEPD*) <https://www.aepd.es/herramientas/facilita.html> accessed 3 October 2019.

[39] Meaning Data Inspection Board. See, 'GDPR - Nya Dataskyddsregler' (*Verksamt*, 2018) <https://www.verksamt.se/driva/gdpr-dataskyddsregler> accessed 3 October 2019.

[40] Information Commissioner's Office (ICO). See, 'Micro, Small and Medium Organisations' (*ICO*) <https://ico.org.uk/for-organisations/in-your-sector/business/> accessed 3 October 2019.

[41] '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/> accessed 4 October 2019.

[42] See, 'Contribution of the EDPB to the evaluation of the GDPR under Article 97', Adopted on 18 February 2020, 35-46.

[43] 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.

The risk-based approach in data protection builds upon the idea that the sole respect of data protection principles[44] is not sufficient to protect fundamental rights and freedoms of individuals. To adapt to the transforming and more and more complex data processing realities, compliance with data protection needs to be combined the risk analysis and risk management.[45]

By providing more substance to the previously established data protection principles, the risk-based approach aims to bring compliance from theory to practice.

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

- Article 24 on responsibility of the controller;
- Article 25 on data protection by design and by default;
- Article 30 on the obligation for documentation (records of processing activities);
- Article 32 on 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 subjects' rights are respected**. From the pragmatic compliance point of view, some suggest that the risk-based approach requires '**adjusting some of the data protection obligations to the risks presented by a data processing activity**'.[46]

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

6.3.2 The notion of risk

The notion of 'risk' is quite a new entry in the legal domain. Indeed, up until now, it has been used more frequently in the areas concerning technology, economics, natural sciences and politics. That is why its understanding in law (and specifically in data protection law) is still evolving.[47] Defining risks is a real challenge. Risks can be 'subjective'[48] and 'objective'[49], as well as voluntarily undertaken,[50] societally imposed,[51] discrete and pervasive[52]. Any of such risks can be evaluated from different perspectives (e.g., technological, economics, psychological).[53] Furthermore, the perception of risk is variable, being affected for example by different attitudes, the manner in which information is given and portrayed, and the familiarity of the person with an activity or hazard.[54] Other elements that can play a role when people are evaluating risk are:

1) The degree an individual feels in control;
2) The nature of consequences and the distribution of the impact;
3) Whether an individual is exposed to an activity voluntarily;

[44] 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.
[45] 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
[46] Christopher Kuner, Lee Bygrave and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP; 2020), 26
[47] ibid 6.
[48] Subjective risk assessment entails non-expert perceptions by the public.
[49] Objective risk is assessed scientifically by experts and is probabilistic.
[50] For example, by taking some drugs, such as contraception.
[51] For example, a nuclear power plant.
[52] The latter includes risks that are bound to happen, such as an earthquake.
[53] Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy, and Practice* (Oxford University Press 1999) 139.
[54] Paul Slovic, 'Perception of Risk' (1987) 236 Science 280–285.

4) The perceived benefits of an activity.[55]

Nevertheless, when the legal analysis and the interpretation of the notion of 'risk' in the GDPR are concerned, these insights are, at practical level, of little use.

For a more concrete understanding of the notion of 'a risk' in the GDPR, one should turn to guidance and opinions issued by the data protection regulators, namely the national DPAs. Regulators issue opinions independently and in the set-up of the EDPB, which replaced the Article 29 Working Party.[56] The WP 29 suggests that '**a "risk" is a scenario describing an event and its consequences, estimated in terms of severity and likelihood**.'[57]

While in general 'risk' is understood as a future threat, in data protection law, it relates more specifically to **threats concerning the rights and freedoms of individuals** whose personal data are being processed (i.e. data subjects). The WP29 made it clear on several occasions, that such threats are not limited to the right to protection of personal data or privacy. In particular, in the statement concerning risk based approach and the Opinion concerning data protection impact assessments, the WP29 argued that while 'the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy… [it] may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.'[58]

An example about how personal data processing operations can pose threats to the rights and freedoms of individuals, different from privacy and data protection, is given by health-related data. If health related data are not accurate or up to date, this can create a risk for the health of the data subject.

This means that, for each processing operation, the relevant rights and freedoms of individuals must be considered. The consideration of potential threats must be carried out on individual basis, taking into account the context of the processing.

Despite this definition provided by the WP29 reiterates the conventional understanding of risk in the literature, it raises uncertainty as there is no single method to follow to evaluate risk.[59] An action that should be taken by both controllers and processors is defined by the regulators as "risk management", which is perceived 'as the coordinated activities to direct and control an organization with regard to risk'.[60]

6.3.3 Conceptualising a risk-based approach

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

- taking into account;
- 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 processing;
- purposes of processing; and
- risks of varying likelihood and severity for rights and freedoms of natural persons posed

[55] ibid.
[56] Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279 <https://www.sciencedirect.com/science/article/pii/S0267364917302698> accessed 11 April 2018.
[57] 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.
[58] ibid.
[59] Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279 <https://www.sciencedirect.com/science/article/pii/S0267364917302698>.
[60] 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.

by the processing.[61]

In practice, this entails that the GDPR grants SMEs enough margin to customise technical and organisational solutions to their specific needs.[62] Also, the state of the art depends greatly on applications and sectors.[63]

6.3.4 Types of risks

As mentioned in Section 6.3.2, evaluating risks to rights and freedoms is often a challenging activity. While different methods can be invoked for compliance purposes with the GDPR, it is necessary to distinguish at least the following three types of risks situations.

1) low risk situations: where the risk to the rights and freedoms of natural persons deriving from the processing operations is minimal because, for example, the actual realisation of the risk would lead to negligible consequences for the data subjects, like mere disappointment or annoyance.

2) risky situations: where the processing operations could affect the rights and freedoms of natural persons, leading to material, non-material or physical damages (e.g. discrimination, identity theft, fraud, damage to reputation etc. (Recital 75 GDPR)). In case of risky situations, personal data are processed and requires controllers (and processors) to take appropriate organisational and technical measures.;

3) high risk situations:, where the actual realisation of the risk would lead for example to significantly detrimental or irreversible damages for the data subjects In these cases, additional measures, such conducting a data protection impact assessment or consulting a data protection authority prior to launching a processing operation, or communicating the existence of a data breach to the data subject.

The risk level therefore triggers the applicability of different GDPR provisions and influences the adoption of technical and organisational measures to ensure data security (Article 32 GDPR) and data protection by design and by default (Article 25 GDPR).

6.3.5 How can a risk-based approach benefit SMEs?

The EDPB provides the following conceptualization of a risk-based approach:[64]

> 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).

This definition clarifies that 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.

As suggested by the European regulators on several occasions, 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).

Considering the compliance with the GDPR through the lens of a risk-based approach is particularly useful for SMEs because of its flexibility:

---

[61] Add Reference

[62] 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

[63] 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

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

- on the one hand, SMEs enjoy a certain freedom in determining 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.
- on the other hand, the risk-based approach allows for SMEs to frame data protection requirements in a flexible manner. It does not prescribe or demand a particular measure, but 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, the measures to be adopted to comply with the GDPR by an SME that does not engage in high risky data processing operations will be much more limited than those ones to be adopted by an SME whose business activities are based on high risky data processing operations.

6.3.6 Attribution of roles

An SME can play different roles with regards to data processing operations. Most likely, it would be data controller (or controller), data processor (or processor), or data recipient (or recipient).

Article 4 GDPR provides the following definitions:

> 'controller' i.e. the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
>
> 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
>
> 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Determining whether an entity is a data controller or a data processor (or a recipient) for the purposes of EU data protection law of utmost importance for SMEs, as their obligations under the GDPR change. If it true that also data processors have to comply with certain legal obligations under the GDPR,[65], the data **controllers bear an ultimate responsibility for the processing of personal and for complying with the key data protection requirements and principles,** which include: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality (security), and accountability.

The notions of controllers and processors need to be interpreted in a **functional sense** rather than in a legalistic way. Since these notions are intended to allocate responsibilities, they must stem from actual reality. Even if an SME is formally considered a data processor or a data controller or a recipient in a contract, this will not be sufficient to allocate the responsibility of the

[65] For example, data processors must be able to demonstrate compliance, keeping record 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) <https://www.whitecase.com/publications/article/chapter-11-obligations-processors-unlocking-eu-general-data-protection> accessed 19 April 2019

processing operations.[66] Hence, whereas an entity has the capacity to determine means and purposes of data processing, regardless its denomination, it will be deemed as data controller.

Furthermore, the **role** of the SME is **suitable to change depending on the processing operations**. It may be possible that an SME acts for certain datasets as data processors and for other datasets as data controller.

For example, SME1 provides services of promotional advertisement 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 data processor and SME2 is data controller. Nevertheless, if SME1 decides to use SME2 clients' database for another purpose (e.g. promoting the products of a third SME), then SME1 will be treated as data controller for this type of data processing.

For example, the owner of a building concludes a contract with an SME providing security services, so that the latter installs some cameras in various parts of the building and monitor the camera on behalf of the owner. The owner of the building is considered to be the data controller, while the SME the data processor, in so far as its personnel just looks at the screens and eventually calls the police in case of anomalies. For any processing operation(s) that the SME performs without just following the instructions of the owner, the SME will be considered data controller (e.g. if the SME decides to store the recordings without having been requested by the owner of the building). 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** between the processor and the controller (or between joint-controllers, or processors and sub-processors), or another legal act under Union or Member State law, detailing reciprocal obligations and rights, other than subject matter, nature, purpose, duration of the processing, types of personal data and category of data subjects (Articles 28(3) and (9) GDPR).

Useful resources

'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

DPA decisions concerning 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. [67]

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

[67] '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/> accessed 22 April 2020

6.3.7 Accountability

(a) Background

'Accountability' is one of the principles relating to the processing of personal data (Article 5(2) GDPR), that 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.

Notwithstanding Article 5(2) mentions only the data controller, data processors are expected to be accountable, too. They have to comply with obligations related to accountability and assist the data controller in some of the compliance requirements.[68]

Hence, the concept of accountability is relevant for different types of SMEs and enterprises across various sectors, regardless 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".[69] An example of such a mechanism could be an obligation to demonstrate that the processing of personal data is in compliance with the EU Data Protection Framework.

In the field of data protection and privacy, "accountability is [considered to be] a form of enhanced responsibility"[70] or "a proactive demonstration of an organization's capacity to comply" with the GDPR.[71] Accountability can boost transparency and confidence for both regulators and data subjects, and ensure greater transparency of corporate practices".[72]

The actual recognition of the principle of accountability within the GDPR marks a shift from a primarily reactive approach to a proactive compliance and practice.[73] Whereas (mere) compliance entails that an SME meets certain rules, the accountability principle goes further: SMEs have to demonstrate their commitment to respect personal data.[74] For example, a risk assessment cannot be reduced to a mere 'tick boxes' exercise.[75] Nor the evaluation of the 'appropriateness' of the technical and organisational measure can.

(b) What does an SME need to do to be accountable?

To be accountable, an SME must adopt policies and implement appropriate measures to ensure, and be able to demonstrate, compliance with the data protection framework.

More specifically, according to Article 24 of the GDPR, when an SME acting as data controller is responsible for implementing appropriate technical and organisational measures 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 processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

---

[68] 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.

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

[70] 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

[71] 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)

[72] ibid

[73] Add reference

[74] 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

[75] 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

Even when an SME acts as 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 (Article 28(1) GDPR).

With these premises, it is easy to understand how keeping exhaustive and up to date written documentation plays a key role in relation to accountability.

(c) What are the other examples of accountability measures?

There are several accountability measures foreseen in the GDPR. For example:

- Adopting and implementing data protection policies at the organisational level of an SME;
- Following a 'data protection by design and default' approach (Article 25 GDPR). Albeit it is mandatory just for data controllers, it could represent an effective accountability measure also for data processors and designers of e.g. Apps and Internet of Things Devices;
- Concluding written agreements between (joint) controllers, data controllers and data processors, and processors and sub-processors, specifying reciprocal roles and responsibilities, is now a legal obligation that reflects the accountability principle;
- Maintaining documentation of the processing activities (Article 30 GDPR) and implementing appropriate security measures (Article 32 GDPR) are other examples of obligations binding both data controllers and processors;
- Recording and, where necessary, reporting personal data breaches to DPAs and data subjects (Articles 33 and 34 GDPR);
- Carrying out data a protection impact assessment (DPIA) (Article 35). DPIA is mandatory for only data controllers, and in so far as the processing operations are likely to result in a high risk for the rights and freedoms of natural persons. Yet, data controllers can decide to perform DPIA even for medium risk processing operations. And data processors can, voluntarily, perform a DPIA, too. Carrying out a DPIA even when not legally required can be useful for an SME to better understand (and document) the processing operations, the respect of organisational standards and demonstrate commitment to data protection.
- 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.[76]

It should be noted that these (accountability) measures need to be continuously revised and updated in order to reflect the reality of the processing operations. Hence, accountability requires a continuous effort from the controller's and processor's side.

(d) What are the advantages of accountability for an SME?

The principle of accountability may benefit businesses for several reasons.

It is a leverage for the implementation of good governance and best practices in SMEs. Accountability is an incentive for businesses to keep their data house in order[77] 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.

Additional 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

[76] 'Accountability tools' <https://edpb.europa.eu/our-work-tools/accountability-tools_en> accessed 13 May 2020

[77] 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

Personal 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

6.3.8 Data protection by design and data protection by default

(a) Background

Data Protection by Design and Data Protection by Default (DPbD and DPbDf) left the realm of 'buzzwords' and entered the one of legal obligations, for data controllers, once the GDPR was adopted in 2016. The importance of these principles has grown in proportion to the deadline for the GDPR implementation and the fears over looming fines.

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.[78]

Short of pseudonymisatiom, the GDPR does not provide examples of the technical and organisation 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 principle but can adopt customised solutions.

(b) 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 in order 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 expression of a lifecycle thinking applied to the processing activity.[79]

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

- the nature (i.e. the inherent characteristics of the processing operations), scope (scale and range (e.g. if they concern sensitive data) of the processing operations), context (circumstances of the processing) and purposes/aims of the processing[80]
- 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
- as well as the risks of vary likelihood and severity to the rights and freedoms of natural person deriving from the processing operations.

In particular, the controller must:

---

[78] 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.

[79] 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

[80] 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

- 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 (see Article 5) and integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects (see Chapter III). Another example of the 'by design' approach is the performance of DPIA[81];
- 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 EDPB clarified that the technical or organisational measures referred in Article 25 can be anything, from the use of advanced technical solutions to the basic training of personnel, for example on how to handle customer data. Yet, some DPAs (e.g. DPC) expects the use of encryption whenever possible where personal data is at rest or in transit.[82]
There is no requirement to the sophistication of a measure, as long as it is appropriate for implementing the data protection principles effectively.[83]
That is why there are no specific measures that ensure automatically compliance: the controller will have to define them on the basis of the concrete processing operations.

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.[84]

Other than support the data controllers in their duty to demonstrate compliance, offering PETs to clients may give a competitive advantage to SMEs aimed at attracting data protection aware clients.
Furthermore, the development of new PETs may represent a business opportunity for SMEs. Indeed, pursuant to Recital 78 GDPR, '*when developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations*'

[81] 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
[82] Add reference
[83] 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
[84] 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

ENISA is currently working on establishing a PETs repository and a tool to assess the maturity of the technologies.[85]

(c) How to measure effectiveness of data protection by design measures?

In its opinion the EDPB notes that 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; data controllers must demonstrate they have implemented dedicated measures to protect data protection principles, and that they have integrated specific safeguards that are necessary to secure the rights and freedoms of data subjects.[86]

It is therefore not enough to implement generic measures solely to document DPbDD-compliance; each implemented measure must have an actual effect.

While Article 25 does not oblige controllers to implement any prescribed technical and organizational measures or safeguards, the measures and safeguards chosen by controllers 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.

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

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 desired outcome matters (e.g. to have a competitive advantage comparing with other SMEs providing similar services and avoiding being sanctioned)
- How the progresses will be measured: KPIs may include metrics. Metrics maybe 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 number of complaints 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
- 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 progresses towards the outcome will be reviewed[87]

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

---

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

[86] 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

[87] 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

(d) What does data protection by default entail?

Pursuant to Article 25(2) GDPR, the controller shall 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. .[88] 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 also in an organisational sense, for example when allocating data access to staff having different roles.[89]

(e) 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)

For example, if a bookshop wants to start to selling books 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)

For example, in case a sports centre is required by law to ask clients to provide a medical authorisation for the enrolment, it has to destroy the certificates once the membership expires (unless differently required by law)

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

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

- Establish access control policies to personal data are perhaps one of the most illustrative examples on how to implement data protection by default in practice (which affects the accessibility to data).

Following this principle, an SME must limit 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 in fact accessible to those who need it when necessary (for example, in critical situations).

Access controls must be observed for the whole data flow during the processing. Personal data should not be made accessible, without the individual's intervention, to an indefinite number of natural persons.

Additional 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)

[88] 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

[89] ibid.

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

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.[90]

6.3.9 Documentation

(a) Background

Documentation may be regarded as continuation of the accountability obligation stemming from Article 24. The WP29 highlights that the 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 – both key components of the principle of accountability contained in the GDPR.

For many micro, small and medium-sized organisations, where data processing does not represent the core business, maintaining a record of processing activities is unlikely to constitute particularly heavy burden. Conversely, it could be a tool to strengthen the good governance of the SME.

(b) What does documentation require?

According to Article 30, 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.

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.

European data protection regulators explain that documentation of processing activities must be kept in writing.[91] The controller (and the processor) can chose whether to keep such records in paper or in an electronic form. It is assumed that organisations will, however, benefit more from maintaining their documentation electronically, as such documentation they can easily added to, have entries removed and amended as necessary. Paper documentation is regarded appropriate for SMEs and micro enterprises. It should be added that SMEs (entities having less than 250 employees as specified in Article 30 GDPR) are exempted from this obligation unless:

- The processing is likely to result in a risk to the rights and freedoms of data subjects;
- The processing is not occasional (meaning that it is not regularly/frequently undertaken); or
- The processing includes special categories of data or personal data relating to criminal convictions and offences.

In practice, only some SMEs can avail of this exemption, as most of them will usually process special categories of data at least as part of their employees files. Also, the exemption does not

[90] 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

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

apply to SMEs when processing personal data in the context of activities that are going to involve continuous processing of personal data.

It must be noted that, even for SMEs falling within the exemption, it would be convenient to maintain a record of the occasional processing activities, as it will be much easier for them to cooperate with DPAs when requested and to demonstrate compliance with other GDPR requirements.[92]

There are multiple templates and specialist software packages facilitating documentation available on the market. Examples of free templates are provided by some data protection regulators on their official websites.

For example, the ICO and the CNIL have such templates available on their websites.[93]

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 processing carried out on behalf of the controller
- 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, a description of the security measures (e.g. …) implemented in respect of the processed data.

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

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. In the event that an organisation fulfils the role

[92] 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

[93] When downloading a template consider whether your SME acts as a controller or as a processor within the particular processing operation(s) that you are going to document. See ICO templates here https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/ and CNIL templates here https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement;

of both the controller and processor for a particular activity at the same time, the records may be split up to correspond to those respective roles.[94]

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

Other than keeping 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 due diligence and compliance with the GDPR. Some are expressly required by the GDPR, others are best practices.

For example:

- 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 on the basis of Article 25 in the various phases of the processing operations;
- Keeping track of the DPIA process in all its phases (see section below on DPIA);
- Keep track of data breaches, including the reasons leading to breach, its effects and the remedial action taken (Article 33(5) GDPR) (see below on data breaches)

Additional 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

6.3.10 Appointment of the DPO

(a) Is appointment of a DPO mandatory for SMEs?

The appointment of a Data Protection Officer (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

Normally, this situation does not regard SMEs, but it may be possible that an SME is entrusted, under the legal regime applicable to it, with the performance of services of public interest (e.g. public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing etc.). In this case, it shall appoint a DPO.

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

[94] 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

Core activities of an SME refer to the main business pursued by the business. 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). Still, the fact that processing activities are ancillary does not exempt them to be recorded on the basis of Article 30.

Activities that may constitute a 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 (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.

Large-scale activities encompass processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards); processing of real time geo-location data for statistical purposes by a processor specialised in providing these services. Large scale is not defined by the legislation though different DPAs have given some guidance relevant to different activities (See also Glossary).

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

Examples: SME is involved in health-related sector (e.g. laboratories that provide blood analysis), criminal law firms; SME providing dating app services etc. will have to appoint a DPO.

For SMEs who provide services into other organisations, the voluntary appointment of an internal or outsourced DPO can provide commercial and strategic advantage by communicating a commitment to data protection and promoting higher levels of trust. Furthermore, it may be convenient to centralise data protection related matters in one person or office.

(b) 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;
- 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 legal proceeding).

To ensure the independence of the function, at 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.

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 on a voluntary basis.

(c) 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 (Art. 39(1) GDPR)

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 in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

In this sense, the DPO can e.g. 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.[95] Again, the DPO cannot be considered personally responsible for non-compliance of the data controller or processor with data protection requirements.[96]

- to **provide advice** where requested **as regards the data protection impact assessment and monitor its performance** pursuant to Article 35 GDPR;

The 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) are in compliance with data protection requirements.[97]
Nevertheless, 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 assessor and 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.

For example, when notifying the breach to a DPA, Article33(3)(b) GDPR requires the controller to provide the name and contact details of its DPO as contact point. It is questioned the possibility for a DPO to represent the SME in front of the DPA or in a court in case of proceedings, as this would be incompatible with the independence required from this function[98]

- **Handle data subjects' requests and complaints** (Art. 38(4) GDPR)

The data protection officer may fulfil other tasks and duties, providing that they do not result in a conflict of interests (Article 38(6) GDPR).

For example, the 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. [99] The DPO can also provide advice on the data sharing agreements to be concluded between controllers and processors, (joint) controllers or processor

---

[95] 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>
[96] ibid.
[97] ibid. 25
[98] 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
[99] 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

and sub-processors. The DPO can help the SME to adhere to a code of conduct or to obtain a certification.[100]

(d) Can I share my DPO with other organisations?

Appointing a joint DPO may be a practical solution for a group of SMEs.

It is a possibility 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.

(e) What should SMEs consider before appointing a DPO?

- Not all the SMEs have to appoint a DPO, but it still may be useful to have an expert in data protection working within the enterprise and dealing with stakeholders. It arguably may result in a competitive advantage.
- When the SME is entrusted, under the legal regime applicable to it, with the performance of services of public interest, albeit it is not mandatory, it is recommended that the SME designates a DPO.[101]
- To be able to demonstrate compliance (accountability) with the regulation, it may be useful to document why the enterprise chose to appoint or not to appoint a DPO, and why his/her level of expertise was deemed appropriate.
- To be able to demonstrate compliance (accountability) with the regulation, when a SME decides to pursue an activity in contrast with the advice of the DPO, it should document the reasoning.

Additional 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.[102]

6.3.11 Data Protection Impact Assessment

(a) 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).

[100] ibid. see Tasks 10, 11.

[101] 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

[102] '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

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 project. Impact assessments help decision-makers find the best and most beneficial solutions for the development and deployment of initiatives.[103] To be practical, impact assessments must be scalable, flexible and applicable inter alia for large organisations, consortia or for small and medium-sized enterprises.

Accordingly, also the DPIA process has to begin *before* the starting of the processing operations. The DPIA has been conceived as a tool to shape the envisaged processing operations, in order 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. [104] Yet, the protection of personal data and the compliance with the GDPR must be ensured (Art. 35(7)(d) GDPR).

(b) 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 provide assistance, the data controller bears the final responsibility of the DPIA process. Still, even SMEs acting as data processors may choose to perform a DPIA. This could their enhance 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.

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.

(c) When is a DPIA mandatory?

Not all processing operations require a DPIA. Article 35 GDPR establishes that a DPIA has to be performed where a type of processing is "**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**".

Article 35 refers to rights and freedoms of 'natural persons', not just of data subjects, that are the individuals whose personal data are processed. It is indeed possible that a processing operation presents a risk to natural persons whose personal data are not processed. For example, in the case of self-driving vehicles, a pedestrian may not be a data subject, but 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;

---

[103] 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]

[104] 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

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.[105]

The GDPR leaves data controllers some amount of discretion in determining whether the envisaged processing operations fall within the pre-defined high-risk criteria[106]. The GDPR just gives just few examples of processing operations that, by their own 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;
(b) the processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences;
(c) the systematic monitoring of a publicly accessible area on a large scale.

Other examples of processing operations 'likely to result in a high risk for the rights and freedoms of natural persons' are included in the lists of data processing operations that require a data protection impact assessment compiled by national DPAs (Article 35(4) GDPR).

In principle, also codes of conducts may provide guidance whether a DPIA is required or desirable.

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 a software, or offering data shredding and sanitizing services or cloud based storage).[107]

(d) What are the elements and characteristics of the processing operations that may generate a high risks to rights and freedoms of individuals?

There are certain elements that contribute to qualify the processing operations as 'likely to result in a high risk' for natural persons.

According to the WP29, 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, 5) data processed on a large scale, 6) matching or combining datasets; 7) data concerning vulnerable data subjects, 8) the use of innovative or new technological or organisational solutions, 9) situations where the processing in itself "prevents data subjects from exercising a right or using a service or a contract." These elements are not cumulative in the sense that and it suffices for one of them to be present to create a high risk for data subjects.[108]

Other risk indicators are: processing that can lead to a material, non- material or physical damage for the data subject (Recital 75); data transfers outside the European Economic Area without an adequacy decision or appropriate safeguards in place;; processing operation(s) concerning personal

[105] 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.
[106] 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

[107] 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
[108] ibid 11.

data that have not been obtained by the data subjects and for which providing information to the data subjects would entail a disproportionate effort.[109]

However, the WP 29 warns that these elements that could be used to determine the threshold for distinguishing risk into 1) a risk and 2) a high risk when determining the need for a data protection impact assessment are not applicable when considering whether a controller has an obligation to notify a data breach to individuals.

(e) What situations could require a DPIA?

Examples of processing operations that could trigger a DPIA:

- If the SME is implementing a new tool to monitor access to office combining use of fingerprints and facial recognition.
- If the SME is a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks
- If the SME is providing CCTV surveillance shopping centre or using a large number of cameras in their own premises;
- If the SME is processing data of vulnerable people (e.g. employees, children, minorities etc.)
- If the SME is performing creditworthiness assessment on the basis of automated decision making without any possibility of human intervention.
- If the SME is monitoring social media data to create profiles of clients or of employees.
- If the SME is developing an eHealth app
- If an SME is considering implementing an automatic staff appraisal for assigning bonuses to its employees to increase salaries;
- if an SME is going to rank clients for providing them insurance services;
- if an SME provides private investigation services and handles data concerning criminal convictions and offences

(f) When DPIA is not required?

The GDPR expressly foreseen 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;
- 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.
- 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.

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

[109] See ICO on 'Data protection impact assessments' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/> accessed 14 May 2020

(g) 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". [110]

In practice, this means that the DPIA needs to be periodically revised.

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. Therefore, it should be noted that the **revision of a DPIA is** not only **useful for continuous improvement**, but also critical to maintain the level of data protection in a changing environment over time. A new DPIA may also become necessary because the **organisational or societal context for the processing activity has changed**, for example because new rules on data protection or data protection impact assessment have been adopted in the jurisdiction where the data controller is operating; or because 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.

(h) How to conduct a DPIA?

The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing practices. National Data Protection Authorities may provide different 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 five phases including the eleven steps.[111] The Steps marked by * are not literally required by Article 35 and 36 GDPR but they emerge for pragmatic reason or by the interpretation of other GDPR provisions.

Phase I Preparation of the Assessment	Step 1	*Screening* (*threshold analysis*).
	Step 2*	*Scoping*
	Step 3*	*Planning and preparation*
Phase II Assessment	Step 4	*Description*
	Step 5	*Appraisal of impacts*
Phase III Recommendations	Step 6	*Recommendations*
Phase IV Ongoing Steps	Step 7	*Stakeholders involvement*
	Step 8*	*Documentation*

[110] 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

[111] As interpreted from Dariusz Kloza et al., 'Towards a method for data protection impact assessment: Making sense of GDPR requirements' (2019) *d.pia.lab Policy Brief* <https://cris.vub.be/files/48091346/dpialab_pb2019_1_final.pdf> accessed 14 May 2020

	Step 9*	*Quality Control*
Phase V Prospective Steps	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 occur in all the other steps. The last two steps are prospective, in the sense that they are triggered only if certain conditions are met.

i) Phase I: Preparation of the assessment process

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. On the basis of that, it should be possible to determine if the DPIA process is required (i.e. the processing operations are likely to result in a high risk for the rights and freedoms of natural persons) or not (because the processing operations are not likely to result in a high risk, or an exemption applies). If the latter, then it is best practice for the SME to document the decision by issuing a statement of non-significant impact explaining why the DPIA was not performed.

*** Step 2: *Scoping***
In this step, the data controller determines:

(a) what aspects of the fundamental right to personal data protection (for example, the exercise of data subjects' rights, the conditions of consent etc.) 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) (Article 35(9) GDPR); the DPO (Article 39(c) GDPR; and the data processor (Article 28(f) GDPR);

(c) which techniques will be used for assessing the impacts. The GDPR mentions only the necessity and proportionality assessment and the risk appraisal, but 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 in relation 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, an environmental impact assessment (EIA) may be warranted or required by law. Similarly, if an initiative affects human health, a health impact assessment may be required by law or an ethics impact assessment may be desirable.

*** Step 3: *Planning and preparation***
In this step, the data controller specifies:

(a) the objectives/goals of the assessment process;

(b) the criteria for the risk acceptance 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 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 (Article 35(11) GDPR), others are possible. For example, the data controller may establish periodic reviews of the DPIA process.

ii) Phase II: Assessment

Step 4: *Description*
In this step, by widening the preliminary description, the envisaged processing operation(s) are described both contextually and technically. Nature, scope, context and purposes of the processing operations are clarified, as well as any legitimate interest pursued by the data controller (Article 35(7)(a) GDPR).

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 (Article 35(7)(b)-(c) GDPR) are assessed. It is best practice to include the risks identified and their appraisal into a register.

iii) Phase III: Recommendations

Step 6: *Recommendations*
In this step, mitigation measures to address the risks identified in the previous step and to demonstrate compliance with the law (Article 35(7)(d) GDPR) are suggested. 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.[112]

iv) Phase IV: On-going steps

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 (Art.39(c) GDPR, of the data (Art. 28(f) GDPR) and, where appropriate, of the data subjects and of their representatives (Article 35(9) GDPR). 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. [113] 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***
Keeping intelligible records, in writing or another permanent format, of all activities undertaken with the assessment process, is the easiest way to demonstrate accountability. It is best practice to keep track also of the advices 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 (Art.39(c) GDPR). 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.

---

[112] 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

[113] 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

v) Phase V: *Perspective* steps (triggered only in certain situations)

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 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 on the basis of Article 58 GDPR (e.g. start an investigation, issue warnings).

Step 11: *Revisiting*
Revisiting of (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 (Article 35(11)).

Additional resources:

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

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

6.3.12 Security requirements

(a) Background

Article 32 GDPR requires controllers and processors 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.

(b) How the security obligation is related to other provisions?

This obligation also requires 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 take a decision with sufficient evidence demonstrating that the processor is suitable, it can then enter into a binding arrangement. It should be added that 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 own staff or a trusted third party. When outsourcing the processing of personal data (e.g. for the provision of technical assistance or cloud services), the controller must conclude a contract, another legal act or binding arrangement with the other entity already setting out clear and precise data protection obligations and the nature of processing in a detailed data processing agreement.

(c) What organizational security measures can an SME take?

Carrying out an information risk assessment is one example of an organisational measure, but controllers and processors will need to take other measures as well. Each organisation should aim to build a culture of security awareness within your organisation.

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. This includes the system administrator accounts is an example of an appropriate organisational measure.

(d) What technical security measures can a 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, you should look at factors such as:

- the quality of doors and locks, and the protection of your premises by such means as alarms, security lighting or CCTV;
- how you control access to your premises, and how visitors are supervised;
- how you dispose of any paper and electronic waste; and
- how you keep IT equipment, particularly mobile devices, secure.
- 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. It may therefore be sensible to assume that your systems are vulnerable and take steps to protect them.

When considering cybersecurity, you should look at factors such as:

- system security – the security of your network and information systems, especially those which process personal data;
- data security – the security of the data you hold within your 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 of your website and any other online service or application that you use; and
- device security – including policies on Bring-your-own-Device (BYOD) if you offer it.

(e) What level of security is required?

The GDPR does not define the security measures that an SME should have in place. It requires controllers and processors to have a level of security that is 'appropriate' to the risks presented by your processing. Also in this case, the size of the business does not matter, depending the 'appropriateness' on the risk presented by the processing.

Both controllers and processors need to consider this in relation to 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 own circumstances, the processing they are engaged, and the risks it presents to their organization as well as the rights and freedoms of data subjects.

So, before deciding what measures are appropriate, you need to assess your information risk. You should review the personal data you hold and the way you use it in order 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. You should also take account of factors such as:

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

Additional 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/

6.3.13 Personal data breach notification

(a) 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 (Article 4(12) GDPR). If the GDPR is breached in a different way (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.[114] 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.[115]

Controllers are required to notify "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." An obligation to notify personal data breach notifications to DPAs and individuals accompanies a number of other provisions, such as data protection by design, security measures, data protection impact assessments and certification that also imbed *the risk-based approach.*

According to the explanation provided by European data protection regulators, an obligation to notify personal data breach is both an accountability obligation and an obligation requiring

[114] 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

[115] ibid. para 29

'additional measures when specific risks are identified'.[116] While being an accountability obligation a data breach notification is part of controllers' obligations, which 'can and should be varied according to the type of processing and the privacy risks for data subjects.'[117] An 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.

(b) Under what conditions is a notification to the DPA required?

The GDPR requires that, when the data breach is likely to result in a risk to the rights and freedoms of natural persons, '[i]n the case of a personal data breach, 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'. (Article 33(1) GDPR). At 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 contact point with the DPA
- A description of the likely consequences of the data breach
- 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 about the personal data breach, which may include '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'. Consequently, this means that the controller must have an internal procedure allowing to confirm breach of security concerning personal data. The GDPR does not specify practical aspects of such procedure. At the same time, it is widely recognised that for any entity handling information, including processing personal data, to run in a smooth way it must have an appropriate governance or organizational structure in place where roles and responsibilities of individuals involved would be specified in internal policy and strategy documents. Such documents can be developed based on standards, guidelines and models provided by external sources yet it is essential that they 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 are 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) Directive (EU) 2015/2366).

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.

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

The following documents in place that 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,

[116] 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

[117] ibid 3.

responsibilities, and authority and how program outputs such as incident communication and reporting will be managed.

2) **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** are documents containing technical step-by-step actions that the CSIR Team will take to manage specific incidents. Standard Operating Procedures (SOPs) help minimize incident management errors and ensure a consistent and repeatable incident management capability. SOPs traditionally also include the forms and checklists that will be used by CSIR Team members in the execution of the CSIR Team.'[118]

(d) Under what conditions is a notification to affected individuals required?

The WP29 analysis does however establish clear threshold criteria when to notify individuals. The WP 29 points out that the high risk threshold for communicating a breach to individuals is higher than for notifying DPAs so that individuals are protected from 'unnecessary notification fatigue' and do not receive notification about all breaches. [119] In view of this, the WP29 suggests considering the following elements of the breach to determine if it 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.[120] 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, cyberespionage (concerning national security or economic interests), or acts aiming to publicly humiliate someone without an intention of attaining financial gains.[121]
- **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.'[122] 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 an identity theft.[123]
- **Ease of identification of individuals**: when evaluating risks associated with a data breach, it is also important to consider for controllers whether 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).

---

[118] Kevvie Fowler, *Data Breach Preparation and Response: Breaches Are Certain, Impact Is Not* (2016) Kindle edition 50.
[119] ibid.
[120] ibid 7.
[121] 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.
[122] Article 29 Data Protection Working Party, 'Guidelines on Personal Data Breach Notification under Regulation 2016/679' (n 207) 24.
[123] ibid.

- **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, example, if the breach concerns personal data about vulnerable individuals. According to the European regulators, 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.)It should be added that 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.'[124] For example, 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.[125]

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 are able to identify the more serious beaches 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.[126] 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.[127]

Additional sources:

[124] ibid 25.
[125] 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.
[126] Article 29 Data Protection Working Party, 'Guidelines on Personal Data Breach Notification under Regulation 2016/679' (n 207) 31–33.
[127] Irish Data Protection Commission, 'A Practical Guide to Personal Data Breach Notifications under the GDPR' (2019).

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

6.4 Codes of conduct

6.4.1 Background

Opting in for a code of conduct could be beneficial for an SME as it could facilitate its compliance with the GDPR requirements. More specifically, codes of conduct foreseen in Article 40 of the GDPR are meant to include best practice to follow 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), their monitoring can be done a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.[128]

(a) What are the advantages of codes of conduct?

While the GDPR makes it clear that the use of codes of conduct should be encouraged by national data authorities, the EDPB and the Commission, the advantages need further clarification. As the code of conduct should facilitate compliance of an SME operating in the specific setting, it should allow reducing compliance costs and a risk of fines.

(b) How to evaluate a code of conduct?

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'.[129] In practice, this means, for a DPA to approve a code of conduct applicable in its territory, or for 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 the manner in which the consent of the holders of parental responsibility over children is to be obtained;
- the measures and procedures referred to in Articles 24 and 25 and the measures to ensure 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 with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

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

Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(c) How to select the appropriate code of conduct?

When selecting a code of conduct under the GDPR, an SME should pay a 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. Approved codes of conduct should be published and available in the public register of approved codes of conduct.

Additional sources:

Article 29 Working Party, Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing (13 July 2010) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp174_en.pdf

Article 29 Working Party, Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing (22 September 2015) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640601

6.5 Certification

6.5.1 Background

Article 42 and Article 43 GDPR provide for the Member States, the DPAs, the European Data Protection Board and the Commission 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.

(a) 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 work as enhancers for the trust of clients and data subjects, offering them more transparency about the data protection policies of data processors and controllers and reducing the asymmetries of information.[130]

Secondly, certifications can reward privacy-aware technologies developed or employed by SMEs. Building upon these two aspects, certifications can offer a competitive advantage for the SMEs choosing to apply for them.[131]

Furthermore, in case of data transfers (in the sense of transmissions of personal data outside the European Union), they can assume the role of appropriate safeguards, becoming the lawful basis pursuant to which the exporter controller or processor transfer personal data to the certified importer controller or processor.[132]

Certifications do not prove compliance with the GDPR themselves, but can be used by controllers and processors as a support to demonstrate compliance with the GDPR concerning: the implementation and demonstration of appropriate technical and organisational measures; the existence of sufficient guarantees for the relations processor to controller and sub-processor to processor.[133]

---

[130] 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>
[131] Ibid.
[132] Ibid.
[133] 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

(b) How to choose between different certifications?

Albeit at the moment of writing there is no EU data protection seal (yet), still there are national and internationally recognised certification schemes that an SME can consider applying to.

Certifications are different: some of them are fully related to data protection; whereas others are partially related to data protection; and still others are related to aspects of data protection (e.g. cybersecurity). Furthermore, 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 multiple SMEs-friendly models that have a dedicated offer to the SMEs. 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.[134]

Not all of them are within the scope of Article 42 and 43 GDPR, meaning that, albeit data protection related, they are not specifically tailored upon GDPR requirements.[135]

The criteria to evaluate if a certification is within the scope of Art. 42 GDPR are:

1. the fact that the certification concerns personal data and privacy in a broad sense;

2. the voluntary nature of the certification;

3. the performance of third-party (which can be an accredited certification body - accredited by a National Accreditation Authority- or a supervisory authority) conformity assessment. This entails self-certification schemes are excluded from the scope of Article 42 GDPR;

4. the fact that the certification concerns the processing operation. The EDPB clarified that, when assessing a processing operation, three core components must be considered, i.e. 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).[136]

For those within the scope of Articles 42 and 43, it is possible to distinguish between: Comprehensive GDPR schemes, that cover the full breadth of the GDPR; and Single-issue schemes, that focus on a particular GDPR sub-topics (e.g. data protection by design, children consent etc.).[137]

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 certification 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 art evolves.[138] In fact, the GDPR itself provides for a maximum duration of 3 years.

Additional sources:

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

[134] 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
[135] Ibid.
[136] ibid
[137] ibid
[138] 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

6.6 Addressing the questions raised by SMEs in NAIH hotline

This part of the Handbook addresses those questions that have been mostly raised by SMEs in the NAIH hotline.

6.6.1 SMEs and legal basis for data processing

(a) Background

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

Personal data may be lawfully processed if they meet one of the following criteria:

- the processing is based on the consent of the data subject.
- a contractual relationship requires the processing of personal data;
- the processing is necessary for compliance with a legal obligation of the controller;
- vital interests of data subjects or of another person require the processing of their data;
- the processing is needed for the performance of a task in the public interest;
- legitimate interests of controllers or third parties are the reason for processing, but only as long as they are not overridden by the interests or the fundamental rights of the data subjects.

(b) How to choose among different legal basis?

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

i) Consent

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.).

To be valid, 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 practical level, consent is **freely given** in so far as it can be withdrawal anytime by the data subjects, without any detriment. Examples of detriments are disadvantage, deception, intimidation, coercion or significant negative consequences.[139] However, consent can be valid even in circumstances where not consenting/withdrawing the consent have minor negative consequences on the data subjects. For example, if an SME is a shop offering clients a card for getting extra discounts, the SME could process the personal data of the clients on the basis of their consent. Not enjoying extra discounts is not seen as a detrimental effect.[140]

Furthermore, 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.

Informed consent means that data subjects have to understand what they are agreeing to. Therefore, data subjects need to be given information concerning: the identity of the controller and the purposes of the processing; the (type of) data will be collected and used; the existence of the right to withdraw consent.[141]

---

[139] 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

[140] 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

[141] 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

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. For example, if an SME would like to collect customers e-mail addresses for sending them marketing but would also like to share customer's details with other partner companies, it has to ask consent separately for the two purposes.

Unambiguous means that it must be obvious that the data subject has consented to the particular processing. That is why 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.[142] A mere 'no objection' to the processing cannot count as affirmative action, neither.

When information society services (i.e. contracts and other services that are concluded or transmitted on-line) are offered directly to a **child**, and consent is used as legal basis, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Otherwise, it is the holder of parental responsibility over the child that has to consent. The threshold can be lowered at 13 years old by national law.

With these premises, it is possible to understand that 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. That is why SME should not refrain from using other grounds for processing.

ii) Contractual relationship

In certain cases, processing personal data is necessary to perform a contract to which the data subject is party.

For example, if an SME has an online shop, it will have to process the information concerning the address of the customers to perform the delivery of the products. In this case, the legal basis of the processing is the performance of the purchasing contract between the shop and the customer. Even pre-contractual arrangements are covered.

iii) Compliance with a legal obligation

In certain cases, processing personal data is necessary for the data controller to comply with a legal obligation.

For example, SMEs may need to process personal data of their employees for social security and tax purposes. Or SMEs may need to share data of their customer to tax authorities.

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.

iv) 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.

For example, in an emergency situation, an SME can undoubtedly share the personal data of its employees to medical personnel.

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

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 basis.

---

[142] ibid. para 8

vi) Legitimate interests pursued by the data controller

An SME acting as data controller (or a third party) can have a legitimate interest in processing personal data. Still, when using this legal basis, the SME has always to balance its legitimate interest with the rights and freedoms of data subjects.

An interest, to be legitimate, must be: lawful, meaning in accordance with applicable EU and national law; 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.[143] As general criterion, legitimate interest can be invoked 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 processing for that purpose may take place (Recital 47).

For example, an SME has an online shop and asks the customers to share their e-mail address to give updates about the order on the basis of consent. If the SME decides to use the e-mail address also to send marketing materials, it can invoke the legitimate interest. The GDPR establishes that processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest (Recital 47),[144] but it is not automatically the case. There have been situations where DPAs imposed fines.

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 (Recital 47).

Additional 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

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

6.6.2 SMEs and employees' data

(a) Background

Many activities performed routinely in the employment context entail the processing of personal data of workers. For example, processing application forms and work references, payroll and tax information-tax and social benefits information, sickness records, annual leave records, unpaid leave/special leave records, annual appraisal/assessment records, records relating to promoting, transfer, training, disciplinary matters, records relating to accident at work, etc. Some information concerning employees may also belong to the special categories of personal data listed in Article 9 (e.g. trade union membership, health related information). Even monitoring of emails and calls and recording of workspaces, although for security purposes, involve the processing of personal data of employees.[145]

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

---

[143] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controllerunder 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> accessed 14 May 2020

[144] In this respect, see nevertheless 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/

[145] 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

Processing personal data in employment context falls within the specific processing situations where special national rules may have been adopted (See Article 88 GDPR).

Recital 155 specifies that "*Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship*".

Hence, this section provides just an overview of the general principles that have to be taken into consideration by the SME in the employment context. For more targeted guidance it is necessary to refer to national implementing rules of the GDPR.

(b) What is the best legal basis 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 processing of personal data in the employment context is questionable. Indeed, the GDPR requires that, to be valid, the consent must be freely given. Considering the economic imbalance between employer and employees, this requisite can be affected.[146] 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.[147]

More appropriate legal basis can be:

- the performance of a contract to which the employee is party (Article 6(1)(b). For example, when meeting obligations under the employment contract, such as paying the employee, the employer is required to process some personal data of the employee[148].
- the compliance with a legal obligation to which the employer is subject (Article 6(1)(c). For example, when the employer has to communicate personal data of the employee for social security, welfare or tax purposes;
- 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. For example, a recruiter of an SME can browse a publicly available database (as LinkedIn or similar) and contact a person to offer a job interview; the employer may also communicate to a client the contact details of one of the employees.

(c) 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.[149]

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

---

[146] 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

[147] 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

[148] 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

[149] ibid.

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).[150]

In certain situation, 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), and this constitute a lawful basis for the processing operations.

In other cases, the employers may still have a legitimate interest in monitoring employees (e.g. increase security purposes; safety purposes; proving 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 (especially client data) or workplace.[151] That is why the employer has to be careful in motivating the necessity and the proportionality of the monitoring.

There are many differences at national level concerning the possibility to monitor employees. A common trait is that policies and rules concerning legitimate monitoring must be clear and readily accessible, ideally elaborated by the employer together with representatives of the employees. Furthermore, privacy friendly solutions, should be preferred to monitoring of employees. For example, an employer should opt for the introduction of filters to websites accessible from workplace rather than monitoring all the web activities of the employees.

6.6.3 SMEs and data subjects' rights

(a) Background

Data subjects' rights are not a novelty in data protection legal landscape. With the GDPR, they have been extended and better defined in their scope. Most of data subject right mirrors a corresponding duty of the data controller. That is why it is important that SMEs are familiar with data subjects' rights and the corresponding obligations arising from them.

Normally, to comply with data subjects' queries is a duty that relies on SMEs acting as data controllers, whereas SMEs acting as data processors have to assist their data controllers in granting data subjects their rights (Article 28(3)(e) GDPR). The data controller shall reply to data subject queries 'without undue delay' and in any case within 30 days (Article 12 (3) GDPR), but this time limit can be adjusted taking into account the complexity and number of the requests, and extended by two further months where necessary, providing that the data subject is prevented within the 30 days and the delay is duly motivated. If a DPO is appointed within the SME, normally s/he will be in charge of deal with the data subjects' requests.

If data processing does not belong to the core business of the SME, it is unlikely that replying to data subjects request will be burdensome. Furthermore, if good policies to deal with data subjects requests were in place before the adoption of the GDPR, the adaptation will be minimal.

In so far as the requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b), refuse to act on the request, but it will bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

The GDPR explicitly enables controllers to require data subjects to provide proof of identity before giving effect to their rights. This helps to limit the risk that third parties gain unlawful access to personal data.

[150] ibid.
[151] ibid.

(b) What are the data subjects' rights?

i) 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.) and contact details of parties involved (e.g. data controllers and, if present, DPO and recipients), together with the possibility to claim data subjects' rights. Article 12, 13 and 14 GDPR contain a list of the information to be provided to data subjects. They also give a good guidance to SMEs concerning the points to address 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.

ii) 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. The data subject has the right to receive information also about the purposes of the processing, the personal data protection concerned etc. (see list in Article 15).

iii) Right to rectification (Article 16 GDPR)

To enable data subject to correct the information the data controller has on them.

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

iv) 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 SME. SME have to act without undue delay and delete the personal data when: personal data are no longer necessary regarding the purposes for which they processed; the data subject withdraws the consent or objects the processing and there is no other legal ground for the processing; personal data have been unlawfully processed (e.g. without a legal basis); Union or Member State law require the controller to do so; personal data have been collected concerning the offer of information society services to children.[152]

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 of national legal obligation requiring the processing; establishment, exercise or defence of legal claims.

v) Right to restriction of processing (Article 18 GDPR)

The data subject can ask the SME 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; decision is pending on the legitimate interests of the data controller prevailing over the interests of the data subject.

The methods in which a controller can restrict personal data processing can include, for example, temporary movement of the selected data to another processing system, making the data unavailable to users or the removal of personal data on a temporary basis. The controller must notify the data subject before the restriction on processing is lifted.[153]

---

[152] 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
[153] ibid. 223

vi) 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.[154]

At 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 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.

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.

vii) Right to object (Article 21 GDPR)

When the processing is carried out by the SME on the basis of a public interest or a legitimate interest; when the processing is performed by the SME 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 data subject can object the processing. The right to object can be exercised by automated means (e.g. blocking cookies on a webpage).

viii) 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

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 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).[155]

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

Additional 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/

[154] ibid. 228

[155] 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

Glossary

Data controller (or just controller): It is the natural or legal person which, alone or jointly with others (joint controllers), determines the purposes and means of the processing of personal data.

Data processor (or processor): means a natural or legal person which processes personal data on behalf of the controller.

Personal data: any information related to an identied or identifiable natural person.

Data subject: identified or identiable natural person to whom personal data refer. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Public authority or body: it is not defined in the GDPR, nor does the Regulation refer to national laws for the purpose of determining its meaning. Thus, the term should be given an autonomous EU- wide meaning. It encompasses those 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. (see e.g. Case C- 279/ 12, Fish Legal and Shirley, para. 42 and case law cited therein).

Core activities: they are the key operations necessary to achieve the controller's or processor's goals. If the processing of data forms an inextricable part of the controller's or processor's activity, then it can be considered a core activity (e.g. if an SME carries out the surveillance of a number of private shopping centres and public spaces, surveillance is the core activity of the company, but it is at the same time inextricably linked to the processing of personal data).

Regular: meaning that it constantly or periodically taking place (i.e. ongoing or occurring at particular intervals for a particular period , or it is recurring or repeated at fixed times)

Systematic: meaning that it is occurring according to a system; pre-arranged, organised or methodical; taking place as part of a general plan for data collection; carried out as part of a strategy.

Monitoring: it happens 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 in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes* (Recital 24 GDPR)

Large scale: there is a number of factors to consider in order to determining whether the processing is carried out on a large scale: 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.

Exeptions to large scale: 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).

Special categories of data: they are those personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms and for this reason they deserve specific protection. They are those data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (when processed for the purpose of uniquely identifying a natural person), data concerning health or data concerning a natural person's sex life or sexual orientation. They are listed in Article 9 GDPR.

Sensitive data: in the GDPR 'sensitive data' are related to the special categories of personal data (Recital 10 GDPR). More broadly, they encompass also data related to criminal convictions and offences of on the basis of Article 10. In a wider sense, sensitive data include also personal data

related to vulnerable people (e.g. children, elderly, patients, employees, asylum seekers etc.) or data of highly personal nature (e.g. geolocation data, financial details etc.).

Exception to special categories of data: The processing of **photographs** should not systematically be considered to be processing of special categories of personal data! They are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person

Nature of the processing operations: it relates to the inherent characteristics or type of the processing operations (e.g. data matching, collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction etc.)

Scope of the processing operations: it refers to the scale (large or not) and range of the processing operations (i.e. if they concern sensitive data).

Context of the processing operations: it refers to the circumstances of the processing operations, for example is implementing new technologies or organisational solutions, or is performing a processing in one of the specific situations of Chapter IX GDPR (e.g. processing and freedom of information etc.)

Purposes of the processing operations: it refers to the aims pursued by the controller, for example if the data controller is pursuing a private or public interest.

Supervisory Authority or Data Protection Authority: independent authority established in a Member State.