DATA PROTECTION FOR SMEs*

Fereniki Panagopoulou
Assistant Professor, Panteion University
Sentinel's Ethical & Data privacy Advisory Committee

I. INTRODUCTION

This contribution attempts to provide a concise introduction to data protection in Small and Medium-sized Enterprises/Micro Enterprises (SMEs/MEs). It aims to provide an appropriate legal and ethical background so that the reader can more easily address the specific issues that arise in this context and showcase the most significant legal developments concerning SMEs' compliance with the General Data Protection Regulation (GDPR).

The publication is supported by the EU Funded project SENTINEL "Bridging the security, privacy, and data protection gap for smaller enterprises in Europe" (Grant Agreement Number 101021659) within the framework of the Horizon 2020 Work Programme for Research and Innovation 2018-2020.

II. THE CONCEPT OF PERSONAL DATA

Personal data is any information relating to a specific natural person that can lead to his or her identification[1]. Personal data may relate, for example, to information on belonging to a group, being prosecuted for an offence, having a certain sexual preference, having a certain political, philosophical, or religious belief, and so on. Personal data refer only to living natural persons

* This publication reflects only the author's view. The European Commission is not responsible for any use that maybe made of the information the publication contains.

[1] Cf. Article 4 par. 1 (4) of the General Data Protection Regulation 679/2016 (GDPR). See also a detailed definition by K. Christodoulou, *Personal Data Law, General Data Protection Regulation,* 2020, p. 23 et seq.; and F. Mitletton, "The Concept of Personal Data", in: L. Kotsalis (ed.), *Personal Data, Analysis-Comments-Application,* 2016, pp. 5 et seq. (8).

and not to deceased persons[2]. The deceased are not protected by the data protection legislation, but this does not mean that they are not subject to medical confidentiality[3]. The fact that a person is no longer alive simply means that the processing of their data is not covered by the provisions of the data protection legislation. In principle, legal persons do not have personal data. By way of exception, legal persons may be subject to data protection legislation when the name of a commercial company refers to the name of the main partner and when an institution, or even a commercial enterprise, is commonly identified with the person who runs it[4]. Therefore, SMEs do not generally have personal data, but they do process the personal data of their employees and customers.

Statistics that do not lead to the identification of a specific natural person do not constitute personal data[5]. For example, a statistical survey does not constitute personal data, but if the statistic can lead to identification, then it does.

Personal data are, in principle, distinct from value judgements[6], even though, in certain cases, value judgments may also constitute personal data. A typical example would be the assessment of service or creditworthiness, which constitutes both a value judgment and personal data[7].

Personal data can be divided into simple and sensitive (special categories), with most of them being simple. Sensitive data concern, exclusively, racial, or ethnic origin (e.g. that a person is an ethnic Roma), political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data for the purpose of unambiguous identification of a person (e.g. fingerprints, iris), health, sexual life, or sexual orientation[8]. Anything that is not sensitive is considered simple. The reason we are interested in this distinction is because when we come across sensitive personal data, they need to enjoy enhanced protection[9].

---

[2] See Article 4 par. 1 GDPR in conjunction with Article 35 of the Greek Civil Code, Opinion 4/2007 of the Article 29 Working Party on the meaning of the term "personal data", 20.06.2007, pp. 27-28; and, inter alia, Decisions 100/2001 and 32/2006 of the Hellenic Data Protection Authority.

[3] For example, the issue of the provision of data on the deceased is regulated by Articles 13 par. 6, 5 par. 3 and 14 par. 9 of the Greek Code of Medical Ethics (Law 3418/2005).

[4] See F. Mitletton, “The Concept of Personal Data”, op. cit., p. 10.

[5] Cf. Recital 26 GDPR.

[6] See K. Christodoulou, *Personal Data Law,* op. cit., p. 24 et seq.

[7] Ibidem, p. 25.

[8] See Article 9 par. 1 GDPR.

[9] See Article 9 par. 2 GDPR.

III. FUNDAMENTAL PRINCIPLES OF DATA PROCESSING

The processing of personal data must be based on one of the lawful bases for processing set out in *Articles 5 and 6 GDPR*. These principles are summarized in the principle of lawfulness (personal data must be obtained in a lawful and fair manner); transparency (the data subject must know whether and which personal data are being held about him or her); data minimization (personal data must be adequate, relevant and no more than is necessary for the purpose justifying their processing; for example, in the case of school certificates it is not necessary that they indicate the student's religion or in the case of identity cards it is not necessary that they indicate the cardholder's religion); time limitation (personal data cannot be kept longer than necessary); accuracy (personal data must be accurate and regularly updated); and integrity (taking appropriate technical and organizational security measures in order to avoid unauthorized access, changes, leaks of personal data and accidental loss, destruction, damage).

SMEs are bound by these principles, and they need to incorporate them in their day-to-day business. For instance, all SMEs need to be clear on the lawful basis of their data processing (principle of lawfulness) and they must provide related information notices to their employees and customers (principle of transparency). Also, they need to have a defined retention time for their personal data records (principle of time limitation), and so on.

IV. INNOVATIONS OF THE GENERAL DATA PROTECTION REGULATION

1. STRENGTHENING CITIZENS' RIGHTS

The most important added value of the Regulation lies in the enhancement of citizens' rights[10]. Therefore, the obligations of data controllers and, consequently, SMEs are also strengthened. A key feature is the strengthening of citizens' rights. In this context, the GDPR recognizes new rights, affirms but also updates and renews existing rights for citizens and embraces new mechanisms for the protection of these rights[11] by strengthening the obligations of data controllers (SMEs)[12], establishing a new body, namely the data protection officer[13], and imposing severe sanctions in cases of violations[14].

[10] See in detail F. Panagopoulou-Koutnatzi, *The new rights for citizens under the General Data Protection Regulation: a first assessment and constitutional evaluation,* Journal of Administrative Law 2017, p. 81 et seq.

[11] Cf. in detail G. Dellis, *For an effective public protection of personal data: the "wonderful new world" of Regulation (EU) 679/2016,* Journal of Administrative Law 2017, pp. 2 et seq. (7).

[12] See in detail G. Yannopoulos, *General Data Protection Regulation, The new obligations and the responsibility of the Data Controller,* Journal of Administrative Law 2017, p. 199 et seq. (200).

[13] See in detail A. Varveris, *Technical and organisational issues – the "mandatory" appointment of a Data Protection Officer,* Journal of Administrative Law 2017, p. 206 et seq (211).

A. RIGHT TO INFORMATION (PRINCIPLE OF TRANSPARENCY)

The general list of data subjects' rights is based on the general principle of transparency in the processing of personal data or, more correctly, on a transparent information policy that aims to facilitate the exercise of rights by the data subject, but also to provide consent[15]. This principle is referred to, firstly, in *Article 5 par. 1(a) of the GDPR* and specified in *recital 39*, according to which any information and communication relating to the processing of the personal data in question must be easily accessible and comprehensible, in clear and plain language, free from misinterpretation[16].

B. RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN)

The Regulation positively introduces in *Article 17* a pre-existing right to erasure, the so-called right to be forgotten[17]. Thus, this right is a corollary of the more general freedom to develop one's personality: it is the right of the individual to be able to erase information that he or she does not wish to exist on the internet, and which is not useful for informing the public. In essence, it is a right to shape the digital presentation that is created by consulting relevant search engines[18]. The right hitherto established consists of the deletion of results from search engines. Accordingly, an individual right of deletion has also been recognized for online newspaper archives[19].

C. RIGHT TO PORTABILITY

The relevant right consists, in accordance with *Article 20 of the GDPR*, of the possibility for

---

[14] In particular, the fines may amount to EUR 20 million or 4% of the total worldwide annual turnover of the previous financial year, whichever is higher (Article 83 par. 5 of the GDPR).

[15] See D. Heckmann/A. Paschkee, "Art. 12", in: E. Ehmann/M. Selmayr (eds.), *Datenschutz-Grundverordnung Kommentar,* 2017, margin number 5.

[16] See Ibidem, margin number 17.

[17] See F. Panagopoulou-Koutnatzi, *The right to oblivion in the age of unbearable memory: Reflections on the Proposal for the Data Protection Regulation,* Journal of Administrative Law 2012, pp. 264 et seq.; Idem, *The evolution of the right to oblivion (on the oblivion of oblivion?),* Journal of Administrative Law 2016, pp. 714 et seq. For the right to oblivion, see also I. Igglezakis, *The right to digital oblivion and its limitations,* 2014.

[18] See H. Kranenborg, *Google and the Right to be Forgotten,* European Data Protection Law Review 2015, p. 70 et seq. (74).

[19] See Tribunal Supremo, No 345/2015, 13.10.2015 (Supreme Court of Spain). See analysis of the decision from S. Schweda, *Right to Be Forgotten, Also Applies to Online News Archive, Supreme Court Rules,* European Data Protection Law Review 2015, p. 301 et seq.; and Hanseatisches Oberlandesgericht Hamburg, 7U 29/12, 07.07.2015.

the data subject to obtain personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, and machine-readable interoperable format and to transmit them to another controller, where the processing of personal data is carried out by automated means. Data controllers (SMEs) should be encouraged to develop interoperable formats that allow data portability.

D. RIGHT TO HUMAN INTERVENTION

Under *paragraph 71 of the Preamble and Article 22 of the GDPR*, the data subject should have the right not to be subject to a decision which evaluates personal aspects relating to him or her and which produces legal effects concerning that person or significantly affects him or her in a similar way, taken solely on the basis of automated processing, such as the automatic refusal of an online credit application or e-recruitment practices without human intervention.

E. STRENGTHENING CHILD PROTECTION

An important achievement of the Regulation in the field of rights is the strengthening of the protection of children in the new environment of technological risk. The added value of the Regulation in the area of child protection consists in the requirement in *Article 8* to obtain the consent of the holder of parental responsibility for the processing of personal data of children up to the age of sixteen. The Regulation leaves to Member States the possibility to provide by law for a lower age, but not lower than thirteen years. The Greek legislator has chosen the age of fifteen[20]. What is noteworthy is the recognition of the responsibility for obtaining consent from the parental authority to the controller, who must make reasonable efforts to verify that consent is given or approved by the person having parental responsibility for the child, taking into account the available technology.

The idea of protecting childhood is also reflected in the case law of the ECtHR (*Marper v. United Kingdom*)[21]. According to the Court, the retention of data of persons who have been acquitted could be particularly harmful in the case of minors, given their particular situation and the importance of their development and integration into society. The Court held that particular attention should be paid to the protection of minors from any harm that might result from the retention by the authorities of their personal data after they have been acquitted of a criminal offence.

[20] See Art. 21 par. 1 of Law 4624/2019.

[21] ECtHR, *S. and Marper v. UK* (30562/2004, 30566/2004), 04.12.2008.

SMEs need to be aware of the rights of the data subjects and to have policies that enable them to fulfill these rights following the GDPR provisions.

2. ENHANCED OBLIGATIONS ON THE PART OF THE CONTROLLER

The enhancement of citizens' rights is achieved by imposing enhanced obligations on data controllers (SMEs). The enhanced liability of the controller is an innovation of the Regulation, as *Article 23(2)(a)* of the Regulation exempts him or her if he or she proves that he or she is not liable (Article 23 Law 2472/1997), while the Regulation requires the controller to implement appropriate technical and organizational measures (TOMs) to ensure and be able to demonstrate that the processing is carried out in accordance with the Regulation [Article 24 par. 1].

The obligations of the controller are summarized below:

a. Appropriate technical and organizational measures: The controller (SMEs) must implement appropriate technical and organizational measures to ensure and be able to demonstrate that processing is carried out in accordance with the Regulation.

b. The controller (SMEs) must, by design and by default, establish an appropriate structure (privacy by design) and procedures to meet the requirements of the Regulation.

c. Obligation to inform the supervisory authority and the data subject: The controllers (SMEs) must inform the supervisory authority and the data subject without delay once they have been informed of the data breach. Any complaint of a breach shall also constitute notification of the breach.

d. Preparation of an impact assessment: The controller (SMEs) must prepare an impact assessment for the processing of data presenting a high risk and relating to the assessment of personal aspects, large-scale data, or public area monitoring.

e. Establish a security policy and codes of conduct: The controller (SMEs) must establish data security policies and codes of conduct.

f. Keeping activity records: The controller (SMEs) and processor shall keep a written or electronic record of their processing activities where the undertaking or organization employs more than 250 persons, the processing poses risks to data, is not occasional or involves special categories of data. That record shall be made available to the supervisory authority at its request for the exercise of its powers.

g. Appointment of a data protection officer. In the case of large-scale data processing, the controller is required to appoint a Data Protection Officer (DPO).

It is important to note that the application of the data protection regulation and the

obligations this provides for controllers do not ultimately depend on the size of a company but on the type and nature of its activities. Activities that present high risks for the rights and freedoms of individuals, whether they are carried out by an SME or by a large company, trigger the application of more stringent rules. Nevertheless, some of the obligations of the GDPR may not apply to all SMEs. For instance, as stated above, companies with less than 250 employees are not under obligation to keep records of their processing activities, unless the processing of personal data is a regular activity, poses a threat to the individuals' rights and freedoms, or concerns sensitive data or criminal records. Likewise, SMEs will only have to appoint a Data Protection Officer if they undertake large-scale processing of personal data, and this poses specific threats to the individuals' rights and freedoms (such as monitoring of individuals or processing of sensitive data or criminal records).

3. ACCOUNTABILITY PRINCIPLE

A key innovation of the Regulation, as defined in *Article 5(2) of the GDPR*, is the adoption of the accountability principle. This means that the controllers (i.e. the person who determines for what purpose the data are processed) must demonstrate that they have taken the necessary technical and organizational measures to protect the data. Under the former regime of the Directive and Law No. 2472/1997, the conduct of scientific research with sensitive data required authorization from the Hellenic DPA. Under the current regime, this authorization has been replaced by an obligation on the part of the researcher to ensure technical and organizational security measures in a quasi-self-regulatory regime. This is always in conjunction with the need to carry out an impact assessment study on the rights of the citizen in the case of high-risk processing, which is provided for in *Articles 35 et seq. GDPR*.

The accountability principle applies to all controllers, including SMEs. This means that SMEs need to make provisions for their GDPR compliance documentation.

Moreover, being accountable aims at demonstrating compliance with three entities: Data subjects, data protection authorities, and business partners. Accountability, according to Opinion 3/2010 (on the principle of accountability) of the *Article 29 Data Protection Working Party*, *"would focus on two main elements: (i) the need for a controller to take appropriate and effective measures to implement data protection principles; (ii) the need to demonstrate upon request that appropriate and effective measures have been undertaken. Thus, the controller shall provide evidence of (i) above".*

By integrating accountability as a principle, GDPR states that the controller, and not the Data Protection Authorities, must demonstrate that the entity is compliant with data protection principles. Thus, GDPR compliance and data protection impact assessment framework should demonstrate the SMEs' accountability regarding the handling of personal data.

4. EXTRATERRITORIAL APPLICATION

According to *Article 3 of the GDPR*, the scope of the Regulation extends to the activities of an establishment of a controller or processor that takes place within the EU, but also to the activities of an establishment of a controller or processor outside the EU when the processing concerns data subjects located in the EU (e.g. in cases of e-commerce and profiling)[22]. In accordance with *Article 3(3)*, the GDPR applies to the activities of an establishment of a controller or processor within the EU, meaning that the criterion of the place of establishment of the controller is adopted to determine the scope of the Regulation. The CJEU has given a broader interpretation to the concept of establishment, moving away from a purely formalistic approach[23]. Moreover, *para. 2 of Article 3* extends the scope of the GDPR to the activities of a controller or processor with an establishment outside the EU, where the processing of data of subjects located in the EU is carried out, which relates to (a) provision of services or goods to subjects, independently of whether a payment is requested (e.g. in cases of e-commerce); and (b) the monitoring of the behavior of data subjects within the EU.

On 4 June 2021, and following the annulment of the Privacy Shield by the CJEU in July 2020 due to the failure of the US to provide a satisfactory and equivalent level of protection to that of the EU, the European Commission introduced the "New Standard Contractual Clauses (SCCs)"[24], under which transfers of personal data from the EU and the European

[22] See in detail F. Panagopoulou-Koutnatzi, *Constitutional implications of the mechanisms for extending personal data protection beyond the EU: extra-territorial application of the GDPR and cross-border data transfers,* DiMEE 2019, p. 504 et seq.

[23] See CJEU, Case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) και Mario Costeja González,* 13.05.2014; European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation, 2018, p. 5.

[24] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

Economic Area (EEA) to third countries whose data protection regimes have not been assessed by the Commission, would henceforth be carried out. According to the European Data Protection Board (EDPB), in the absence of a Commission adequacy decision, the controller is competent to judge the status of the Member State. The same was held by the CJEU in the Schrems II Decision[25].

In the adoption of the New Standard Contractual Clauses, the Schrems II Decision of the CJEU has undoubtedly played an important role, as it seems that the new clauses are adapted to new technological developments and challenges, since data transfers to third countries may have extraterritorial application.

In general, the adoption of the new SCCs by the EU for secure cross-border data transfers, as a result of the annulment of the Privacy Shield, is a major institutional development regarding cross-border data transfer law.

Furthermore, the recent EU-US agreement to adopt the New Trans-Atlantic Data Protection Framework[26], expected to be implemented as a foundation for a future adequacy decision, is also relevant to cross-border data transfers.

At the level of guidelines on compliance with the GDPR, the EDPB's Opinion 1/2022[27] on the draft decision of the Luxembourg Supervisory Authority is of great importance, as it highlights a new perspective on the compliance of SMEs, through the establishment of certification mechanisms by national Supervisory Authorities. Moreover, for an SME to be certified, specific criteria need to be met, which will be provided for by the mechanism concerned.

Notwithstanding the above, the EDPB has identified some deficiencies in the draft decision concerning the content of the criteria and their practical application when an SME is under assessment, and how they should be applied. For example, the adoption of technical and organizational measures and whatever else the applicant should take into account when carrying out assessments.

Finally, it is important to stress that the extraterritorial application of the GDPR is not in

[25] Case C-311/18, Judgment of the Court (Grand Chamber) of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*.

[26] European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework of 25 March 2022.

[27] EDPB, Opinion 1/2022 on the draft decision of the Luxembourg Supervisory Authority regarding the GDPR-CARPA certification criteria.

any way associated with the size of an organization. It affects all controllers, including SMEs that are not established in the EU, as long as their goods/services are addressed to EU citizens.

V. EPILOGUE

The above analysis shows that the compliance of SMEs with the GDPR is complex and costly, as it is based on both legislation and the case law practice of independent authorities. SMEs that do not have legal counsel find it difficult to comply with the strict requirements of the Regulation and, therefore, it is critical to create compliance tools that are tailored to the needs of the individual business concerned.

Moreover, it appears that, since the implementation of the GDPR to date, there is still a lack of compliance or incomplete compliance with the GDPR, which is a conclusion that can be drawn from the Decisions of national Supervisory Authorities concerning violations of the GDPR by SMEs. In reality, the failure of some SMEs to comply properly, practically, and effectively with the GDPR is a real and undeniable problem, reflected by the fines imposed by national Supervisory Authorities. Consequently, the practical and effective compliance and implementation of the GDPR is a pressing problem for SMEs.

In view of the above, SMEs should seek out safer, more effective, and holistic ways to comply with the GDPR and to safeguard their customers' assets through compliance tools that can provide them with the security and efficiency they lack.

Currently, GDPR compliance assessment toolkits rely heavily on manual activities. In addition, only assessment experts/assessors are authorized to use these tools. Progress beyond the state-of-the-art is seen by *SENTINEL* partners as the efficient digital transformation of these toolkits to enable participant organizations to autonomously both self-assess accountability and self-determine privacy and data protection risks for GDPR compliance. Such compliance tools can directly assist SMEs to take the required technical and operational measures with minimal human intervention, including education, training, implementation and validation of checklists and any other measures necessary to achieve the intended data protection resilience and GDPR compliance, in a truly cost-effective way.

Furthermore, it is very important to ensure that, if SMEs manage to guarantee their compliance with the GDPR, they will not be at risk of being reported for GDPR violations or getting fined by the supervisory authorities and that, once they achieve that, they can then ask certification bodies and national supervisory authorities (whose existence is encouraged by the GDPR) to investigate whether they are subject to certification.

In conclusion, taking the necessary steps to ensure a data privacy-oriented work ethic is vital for SMEs. All SMEs should be aware of their duties that have been set out in the GDPR. Compliance with the GDPR does not only protect SMEs from the imposition of high fines, but it can also function as a key influence on corporate identity. In fact, research has shown that businesses that demonstrate a significant amount of transparency to consumers are rewarded with a considerable amount of trust. Therefore, the assistance of a reliable compliance tool such as *SENTINEL*, can undoubtedly enhance the level of readiness of SMEs to comply with the GDPR. In this way, the rights of data subjects will be fully respected and protected, and SMEs will be able to achieve the desired assurance of compliance. This is precisely the kind of assurance that will keep them away from risks and fines, and which will undoubtedly add business value and contribute to their business prosperity, health, and progress. ❑