EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

Position Paper on the Evaluation of the General Data Protection Regulation (GDPR)

European Federation of Data Protection Officers

June 2020

EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

Introduction

In various legislations, data protection officers (DPOs) has played an important role in the architecture of data protection (self-)control since the 1980s. The General Data Protection Regulation (GDPR) does not exhaust this role to the fullest extent possible. While the GDPR sees the data protection officer primarily as an instance of self-regulation (advising and monitoring), the data protection officer could play a much more supportive role, particularly in the area of small and medium-sized enterprises (SMEs). In fact, the data protection officer is already doing so to the extent legally permissible. In addition to the formal DPO role, an additional role has formed in practice supporting the organizations, named data protection managers or coordinators and the like. A stronger anchoring of these roles in the GDPR would at the same time reduce the bureaucratic burden created by the GDPR. The activities of the data protection officer can also be carried out by external experts, so that a (risk-)appropriate structure can be created for any company without additional economic burden.

With respect to the risks inherent to modern data processing, data protection officers should be more widely used as risk managers specialised on the risks to individuals in particular. In this way Data Protection Officers can help companies to implement GDPR in the most efficient and cost-effective manner.

The reduction of bureaucracy through closer involvement of the data protection officer must be encouraged. After all, the bureaucratic burden of the GDPR does not exist because, but despite the data protection officers. The absence of a data protection officer in a company in no way reduces the requirements and the bureaucratic burden caused by the GDPR, but the company management is left alone with this task. In this area relief can be achieved for SMEs without lowering the level of data protection.

Many positive effects, which already define the model of "data protection made in the EU" with the GDPR, could have an even greater impact. From the point of view of the EFDPO it is already apparent that the unified view within the EU has a positive effect because the global players in particular, work towards GDPR compliance and even use GDPR as a global benchmark. Nevertheless, there is of course still potential for optimization of the GDPR. The goal may also be to relieve companies and simplify some aspects for the benefit of companies, but also of citizens.

Current situation of requirements

With its comprehensive, extensive and overlapping obligations, the GDPR addresses the respective duties of the controller (Art. 4 No. 7 GDPR) and the processor (Art. 4 No. 8 GDPR) with regards to the management of the business. These duties and responsibilities of the management remain unchanged, even if no data protection officer has been designated. The designation of a qualified data protection officer,

however, means that the necessary competence for this purpose comes to the company. The data protection officer has a relieving effect. This relieving function can be further expanded in the GDPR.

Recommendations

a. Adaptation of the breach notification

In its current state the notification of personal data breaches to the supervisory authority poses considerable problems and burdens to SMEs but also to the supervisory authorities. The majority of incidents involve the disclosure of e-mail addresses through open mailing lists, infections with malware on desktop workstations or loss of data media or devices. Many of these incidents carry limited risks for the data subjects.

The notification process itself varies significantly between the supervisory authorities regarding the information required and the form in which it is to be provided by the companies. This adds to the considerable uncertainty for SMEs regarding the notification obligation, and this is often linked to risks of fines. The involvement of the data protection officer is crucial to assess the incident and take further action, if only because of his specialist knowledge to the matter. Data protection officers work closely with the company, have detailed insights into the company , are domain experts with process knowledge and can therefore better assess the resulting risks.

In order to ease the burden on companies in particular, but also to reduce the work load of supervisory authorities, the EFDPO sees the option of simplifying the notification obligation for SMEs: All incidents must first be reported to the DPO without any delay. The DPO prepares the necessary documentation of the cases, draws up a risk assessment and submits these documents to the person responsible for the final decision on notification. Indeed, the key problem for companies is not primarily the decision to notify or not to notify, but the compilation of relevant information and the assessment of whether an incident is notifiable.

The documentation of any violation of the protection of personal data stipulated in Article 33 (5) GDPR could be structured in such a way that the DPO keeps this register of "data breaches" and monitors the counter measures defined by the controller. This would relieve the burden on the controller.

Due to the mandatory involvement of the data protection officer, the reporting obligation can be adapted for companies that have designated one, so that they do not have to report to the supervisory authorities at a low risk already, but only at a high risk. This is the same threshold as for the notification of data subjects. This notification is recommended by the DPO. After approval, he or she carries out the notification and is also the contact person for the supervisory authorities. The risk

assessment with regard to data subjects is thus in the hands of the data protection officer – who is qualified for these tasks.

This also relieves the burden on the supervisory authorities, because the time-consuming minor cases do not have to be reported to them. The supervisory authorities also do not suffer any loss in terms of a "broad security situation" because they can already demand documentation in accordance with Art. 33 (5) GDPR.

b. Adaptation Data Protection Impact Assessment (DPIA)

Where processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out a prior assessment of the personal data protection implications of the planned processing activities. This data protection impact assessment has already proved its value in the past and has been carried out under the former directive 95/46 EN.

A specific result of Art. 35 GDPR, which is often overlooked in practice without the support of the expertise of a DPO, is that every processing activity has to be assessed in accordance with Art. 35 GDPR in order to determine whether a full data protection impact assessment is required. Art. 35 GDPR thus requires two steps: preliminary assessment to decide on the requirement of a DPIA and, if necessary, implementation of a full DPIA.

The requirement that every processing activity be subject to prior checking in any case poses a considerable burden on the company, especially on SMEs. This is because even this preliminary examination requires data protection expertise which is not available to the average business manager. Placing this preliminary assessment in the hands of the DPO and thus relieving the management of this task, would in practice - especially for SMEs - provide a considerable relief and a reduction of risks of fines. The increasing digitalisation and the growing use of AI systems make a systematic approach to reduce the risks absolutely necessary. For this reason, the DPIA as an instrument for planning is an essential component of responsible organizational activity.

In practice, however, the EFDPO has observed that the implementation of the DPIA – which may be necessary after the preliminary assessment – also poses major challenges for companies because of its complexity, the lack of management know-how and lack of experience with the instrument in general.

Currently the role of the DPO with regard to the DPIA is a supervisory and advisory one. In order to relieve some of the burden on companies, the EFDPO proposes to perform the data protection impact assessment with a more active participation of the DPO. The company should remain responsible for the performance of the DPIA, but the DPO could be given a more supportive role instead of just controlling the result. In particular, the risks for data subjects could be assessed by the DPO. With the

involvement of the specialist departments, the DPO can efficiently prepare the data protection impact assessment on the basis of his or her expertise. The planning of protective measures is the responsibility of the implementing entity. The DPO shall assist in the definition of appropriate and adequate protective measures. The result of this impact assessment is then bindingly determined by the management of the responsible company and the planned measures are implemented.

c. Keeping the records of processing activities

Controllers and processors shall keep records of the processing activities in their company which are within the sphere of their responsibility. This is a key element of self-regulation and of facilitating control by data protection supervisory authorities. This is because these records, based on the criteria of Art. 30 GDPR, map any processing of personal data in the company. It is in fact the basic "data protection inventory" of the company, which must be dynamically updated.

This inventory is the basis for compiling the data for the information obligations under Art. 13, 14 GDPR and accompanies the accountability under Art. 5 (2) GDPR. Without an inventory it cannot be assessed for each processing activity which specific obligations apply, e.g. whether a DPIA is necessary or not.

In practice, the compilation of the inventories is fragmented, and very heterogeneous results are collected. As a rule, in many areas the controllers and processors lack sufficient knowledge, which leads to deficient results both in documentation and in practice.

Due to his professional expertise and his understanding of the interrelationships of the documentation obligations, the data protection officer can, by taking over the documentation, make things considerably easier for the company management which would otherwise have to deal with it.

The obligation to provide the DPO with the necessary substantive statements remains essential. Whether these are already available in the form of processing records plays a subordinate role. The DPO can then coordinate the actual establishment of the records of processing activities, and finally the DPO will maintain the records updated. The DPO checks the inventory with regard to completeness, plausibility and lawfulness. The controller or processor thus creates the individual entries with the advice of the DPO and releases the records as correct. It would be therefore essential for the EDPB to emphasize the outlined role of the DPO in creating and maintaining the records of processing activities.

d. Relief through harmonization and simplification in the GDPR

The main burden for the companies regarding the the GDPR is not a lawful processing of personal data, but all the documentation obligations that come with it.

This is particularly true for SMEs, which rarely break new grounds with Big Data, Smart Data, AI, Machine Learning and other challenges of digitalisation.

The requirements of the GDPR that are perceived as unnecessary bureaucracy are first and foremost the numerous documentation obligations. To name but a few, companies have documentation obligations under Art. 5 (2), 13, 14, 30, 32, 33 and 35 GDPR. They are not congruent, but they overlap in terms of content. Nevertheless, non-compliance with each of these documentation obligations is subject to an individual fine. In the context of data protection, management is thus more concerned with keeping documentation up to date than with the actual question of lawful processing.

The EFDPO recognises and acknowledges the purpose of these documentation obligations because in the GDPR every question of lawfulness corresponds with a documentation obligation and every obligation to act with an organizational obligation. This makes the GDPR an efficient law for achieving its objectives. However, this creates a considerable amount of bureaucracy. This bureaucracy exists with its fine sanctions for company management regardless of whether a DPO must be designated or not.

Under the GDPR, the qualified DPO therefore does not represent a burden, but rather a relief for the management. Because he is familiar with the organizational, technical and legal aspects due to his qualification.

This relief can and must be further developed for SMEs by enabling DPOs to become more involved by taking over more of these activities. Instead of exempting management from its obligation, it should be taken into account as a mitigating factor that the company has actively involved its DPO in these activities. Practice shows that the complexity and extent of these requirements almost inevitably leads to a risk of fines for SMEs and that this overload is already being taken into account in the decision on fines, although it is of course true that "ignorance does not protect against punishment".

The EFDPO especially acknowledges the efforts of the EDPB to harmonization. The positions are perceived as very helpful. With the goal of harmonization, the EDPB has practiced consultation procedures for the position papers. Recently this valuable practice was suspended in some cases. The EFPDO highly appreciates chances of feedback from the practice of DPOs on such important documents.

e. Qualification and certification of DPOs

The position of the EFDPO stresses the need for qualified DPOs. The need for qualified DPOs varies between the EU member states. It was recognisable that not all data protection consulting was backed by the required expertise. The expertise of DPOs and other consultants in the domain of data protection should not only consist

of legal expertise, but also include domain, general business performance and technical expertise. In some countries supervisory authorities and professional associations worked together to develop a trustworthy certification, based on international certification standards (ISO 17024). The acknowledgement of certificates by supervisory authorities can be a countermeasure against the huge number of arbitrary certificates available with almost no trustworthy evidence regarding the real qualification of the DPOs. EFDPO supports these efforts, and would also appreciate European harmonization on this issue.

f. Improvement of the information obligation

According to the experience of the EFDPO members, some aspects of the current information obligations can be improved considerably. The goal of transparency with regard to data subjects is considered essential as an important foundation for data protection and information self-determination. The current practice resulting from the legal requirements does not sufficiently ensure transparency. Above all, it is not sufficiently adapted to the needs of the data subjects. It can be observed that

- too much information is given, which then leads to data subjects no longer being aware of the essential information,
- self-evident topics are repeated endlessly,
- legal formalities dominate over substantial statements,
- the times and situations the information is presented do not contribute to a serious perception of the content,
- the duty to inform and the right to information are not coherent,
- the accountability for the information obligation leads to procedures equivalent to consent with immense effort, e.g. physicians requiring signed information documents before medical procedure,
- the high costs incurred by companies make only a small contribution to improving transparency on the part of the data subjects.

The added value of merely stating the legal basis in the information can be seriously questioned. For the data subject it makes no difference whether, in addition to naming that processing is based on a weighing of interests or based on consent or based on a contract, an additional statement of "Art. 6 (1) sentence 1 lit. f GDPR", "Art. 6 (1) sentence 1 lit. a GDPR" or "Art. 6 (1) sentence 1 lit. b GDPR" is part of the information. For the layperson as the addressee of the information obligation, no added value is generated, but rather more confusion. In fact, this proves to be a gateway for law firms specialized on warning notices and damage claims, especially with regard to

SMEs as easy victims. It is precisely this duty that SMEs see as a prime example of the deplorable bureaucratization of data protection.

The aim of this regulation, to make it easy to check from the outside whether the controller has actually checked the lawfulness, is of course commendable. However, this can also be achieved through the other documentation obligations mentioned above and the involvement of the DPO.

To this end, a number of improvements can be made to the regulation. In some points, it is not even a question of actually changing the regulation itself, but rather, in some points, placing stronger emphasis to certain provisions already contained in the GDPR. One example is the requirement – also advocated by the European Data Protection Board (WP 260) – to explain the rights of data subjects in any information. The resulting similarity leads to monotonous explanations which are always the same and which are ultimately no longer perceived by data subjects. On the other hand, information already known does not have to be communicated (cf. Art. 13 (4) GDPR). To what extent this also includes common knowledge also needs clarification. The intention of the idea to use iconic symbols provided for in Art. 12 (7) is currently not put into practice, in particular due to a lack of standard icons. The layered information is hardly ever used.

Particular consequences have been caused in part by accountability. The fact that no individual proof is needed that the data subject has acknowledged the information about data processing could be emphasised more clearly.

EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

EFDPO contacts:

EFDPO Press Office, phone +49 30 20 62 14 41, email: office@efdpo.eu,

President: Thomas Spaeing (Germany)

Vice Presidents: Xavier Leclerc (France), Judith Leschanz (Austria), Inês Oliveira

(Portugal), Vladan Rámiš (Czech Republic)

About EFDPO

The European Federation of Data Protection Officers (EFDPO) is the European umbrella association of data protection and privacy officers. Its objectives are to create a European network of national associations to exchange information, experience and methods, to establish a continuous dialogue with the political sphere, business representatives and civil society to ensure a flow of information from the European to the national level and to proactively monitor, evaluate and shape the implementation of the GDPR and other European privacy legal acts. In doing so, the EFDPO aims to strengthen data protection as a competitive and locational advantage for Europe. The new association is based in Brussels.

Founding members:
• Austria: Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter privacyofficers.at
• Czech Republic: Spolek pro ochranu osobních údajů
• France: UDPO, Union des Data Protection Officer - DPO
• Germany: Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.
• Greece: Hellenic Association for Data Protection and Privacy (HADPP)
• Liechtenstein: dsv.li-Datenschutzverein in Liechtenstein
• Portugal: APDPO PORTUGAL Associação dos Profissionais de Proteção e de Segurança de Dados
• Slovakia: Spolok na ochranu osobných údajov