The Data Protection Officer (DPO) – Ensuring Greater Data Protection Compliance

Kakhaber Goshadze

Associate Professor of European University

KEYWORDS: Data protection, Data protection officer, General Data Protection Regulation

INTRODUCTION

Data protection legislations have been adopted in many countries, however, the level of protection provided varies by region and state. The need for global data protection mechanism is as desirable as never before, which shifts data protection importance to the next level. Luckily, data protection model within the EU is the most advanced one in the world which may serve as a good example for enhancing data protection mechanisms where needed.

By the Directive 95/46/EC,[1] the EU had established general basis for ensuring data protection compliance for two decades. However, rapid pace of technological advancement triggered the need for even higher standards of data protection and Directive failed to serve as a tool for achieving this purpose, especially from 2010s. As a result, new regulation was introduced in 2012 and after numerous discussions the final version of new data protection framework has been agreed upon. Known as the General Data Protection Regulation (GDPR)[2] it is the most refined and developed standard which is oriented on data

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

protection compliance in the EU. Its benefits are evident and aims to achieve positive outcomes. However, within this Article I want to emphasize one particular subject – the requirement of appointing the DPO in order to shift the level of data management to the more coherent and lawful manner.

In addition, mandatory requirement of appointing the DPO was not only introduced by GDPR, it is also prescribed in the Directive 2016/680,[3] which applies to personal data processing in the field of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

1. THE NEED FOR THE DPO

GDPR enshrines a cluster of rights and obligations for data controllers and processors. Additionally, it encompasses several specific conditions for data processing in specific sectors. Handling of personal data can be seen from the inward-facing and outward-facing perspective. Therefore, different mechanisms may apply depending on the type of data processed.[4]

The most common obligations that data controller is obliged to perform, can be divided into more generalized headlines, such as:

1. Requirement for compliance with data protection principles, inter alia, accountability, fairness, lawfulness, purpose specification, proportionality, keeping the data in correct manner and up to date, storing information for specific time period (retention proportionality), ensuring accountability towards data subject and having implemented adequate technical and organizational security measures. These principles are pillars on which the whole data protection standards are based
2. The next step in a compliance process is to ensure lawfulness of each particular processing operation. This is the stage where grounds for data processing come into play. These grounds may differ according to the data at place, in other words, handling the sensitive personal information requires to act within more restricted grounds for processing
3. Along with general data processing practices, in some circumstances, processing may be carried out for specific purposes, which may involve direct marketing, international data flows, etc. These practices need to be addressed differently, because of their specific nature, therefore, relevant approach is needed for performing relevant actions. In general, they are not difficult to be managed, however, some basic level of knowledge is favorable
4. The central part of data protection legislation is the fulfillment of data subjects' rights. It may be divided into three parts, namely, a right to obtain information and details of processing, a right to request modification of one's own data and a right to restrict processing or simply, the right to be forgotten
5. The whole data processing must be accompanied with relevant measures of security in technical and organizational regard. The method is never universal, instead, data controllers and processors must choose the level of protection that perfectly suits ongoing processing practices.

As it shows, data protection has several important directions where legal compliance requires relevant elaboration. This list of requirements is just a part and it involves further specific details. However, at a first glance, enlisting them in above mentioned way gives us a generalized view on the aspects of data protection. Therefore, the need for the DPO can be based on these

3 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

4 Lambert, P. (2017). The Data Protection Officer – Profession, Rules and Role. Taylor and Francis, 5.

benefits: 1. Fulfill the legal obligations regarding data protection; 2. Review and implement data protection policies and rules; 3. Organize internal trainings for organization members; 4. Provide expertise in relation to data breach aspects.[5]

2. THE APPOINTMENT OF THE DPO

Who should be occupied as the DPO? Although there is no such profession, still the minimum knowledge is preferable. GDPR states that "necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor."[6] It may be required for the DPO to have knowledge in legal acts, technical and organizational measures and procedures of security, knowledge on technical requirements for data protection by design and by default, awareness of the sensitivity of the data processed, ability to carry out internal audits, consultation, documentation, and reporting.[7]

It can't be said that the tasks of the DPO has to be performed strictly by legal practitioner or HR manager. This position requires mixed, nevertheless expert knowledge of data protection law and subsequent legislation. Data protection itself is not a new concept, however, requirement to appoint the DPO still stays as a novel approach.

GDPR prescribes three possible alternative cases where appointing of the DPO is mandatory, these are:

1. If the processing is carried out by a public authority or body (entity), however, this does not apply to courts when they act in their judicial capacity;[8]
2. The core activities of the controller or the processor involve processing operations, which due to their nature, scope and purpose, require regular and systematic monitoring of data subjects on a large scale;[9]
3. The core activities of the controller or the processor consist of large scale processing of special categories of personal data and data relating to criminal convictions and offences.[10]

GDPR does not define what a 'large scale' mean, but according to the guidance from Article 29 Data Protection Working Party, the existence of a 'large scale' is determined according to these factors: (a) the number of data subjects concerned, or a specific number or a proportion of the relevant population; (b) the volume of data and/or the range of different data items being processed; (c) the duration, either permanence of the processing activities; (d) the geographical extent of the processing itself.[11] Some data protection authorities in Europe issued relevant explanations or comments whether the processing can be regarded as a 'large scale.' For example, according to Dutch DPA guidance, data processing by hospitals, pharmacies, general practice centers are always regarded as a large scale, in addition data processing is large scale if it involves 10,000 registered patients treated on general basis and all their files are contained in one single filing system. On the other hand, Czech data protection authority has taken another way to define data processing on a 'large scale,' in this case this processing has to involve 10,000 data subjects in processing. In addition, processing the data by more than 20 branches of by more than 20 employees is considered as a large scale processing as well.[12]

The most important in this regard is that the DPO should be in a position to perform duties

5 Ibid., 209-210.
6 GDPR, Recital 97.
7 Lambert, 38.
8 GDPR, Art. 37(1)(a).
9 Ibid., (b).
10 Ibid., (c).
11 Article 29 Data Protection Working Party. (2017). 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, 10.
12 Breitbarth, P. (2018). On large Scale Data Processing and GDPR Compliance. [https://iapp.org/news/a/on-large-scale-data-processing-and-gdpr-compliance/].

and tasks in an independent manner.[13] In addition, the organization shall not interfere with or pressure the DPO in carrying out and exercising of tasks. DPO is also independent from direction or reporting requirements to other staff members and managers.[14] Also "the data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks [...]."[15] I will review the tasks of DPO in details later on.

One thing to notice here is that data controller and data processor has the option to appoint DPO from the existing staff members, or opt for outsource on the basis of service contract.[16]

3. POSITION AND DUTIES OF THE DPO

Enhancement in data processing methods and scenarios triggered the need for more privacy protection. For effectiveness of data protection standards, special duties may be designated to the DPOs. These duties are wide in range and are not limited to those that are provided by legislation, as an enhanced, balanced data protection is never unwelcomed. "Data protection is not limited to a mere compliance issue. There are many advantages, including competitive advantages, to respecting personal data. The data protection officer should be conscious of selling the advantages of data protection best practice to the management board."[17]

4.1. Specific guarantees for DPO

The DPO has to be involved in all matters of personal data protection by a data controller or data processor. This engagement has to be managed in proper and timely manner.[18] It ensures that the DPO will be aware of all processing activities. Therefore, the DPO should be able to cover all methods of data processing, namely, automated, semi-automated and non-automated ones. On the other hand, from a data controller and data processor standpoint, relevant support should be provided for the DPO to efficiently perform designated tasks. This support also extends to ensuring that the DPO has relevant expert knowledge in order to maintain tasks.[19] The latter may involve providing a possibility for the DPO to raise awareness and knowledge in the data protection field and to keep alert.

It is possible for the DPO to fulfil other tasks and duties as well. However, ensuring that any given task and duty does not cause a conflict of interests is of paramount importance.[20] This should be regulated under a contract and needs to be explicitly mentioned.

One important requirement under GDPR for the DPO position is that "the controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor."[21] Perhaps, this is the most difficult part to be executed in practice. The special emphasis is made on responsibilities of data controller and data processor, however it is achievable. The consideration of the fact that the DPO's independence is proportionate to the effectiveness of data privacy in organization and therefore can cause positive outcomes (which also may be figured in little or no inspections from data protection authority) and strong public image, it may be used as an important self-motivational tool.

4.2. Tasks of DPO

GDPR is clear in enlisting general tasks of the DPO, which is characteristic to the duties that should be performed. These involve five directions:

1. "To inform and advise the controller or

13 GDPR, Recital 97.
14 Lambert, 40.
15 GDPR, Art. 37(5).
16 Ibid., (6).
17 Lambert, 77.
18 GDPR, Art. 38(1).
19 Ibid., (2).
20 Ibid., (6).
21 Ibid., (3).

the processor and the employees [...]."[22] As this provision indicates, the DPO is a main contact point at the organization on the matters of privacy and data protection. Therefore, this position requires avoiding bias towards the management or the employees

2. The monitoring of compliance with GDPR, data protection laws of EU member states and policies of the organization itself, as well as, to ensure awareness-rising of the staff involved in data processing and, perform relevant audits.[23] Considering the legal nature of GDPR, it is not needed to adopt any domestic legislation in order to implement the provisions of GDPR, as it has direct effect in every member state of EU. Accordingly, the main, but not the only, objective of the DPO is to ensure that an organization acts according to the standards set under GDPR
3. "To provide advice where requested as regards the data protection impact assessment and monitor its performance [...]."[24] One of the main advantages of GDPR is to perform data protection impact assessment (DPIA), which ensures the revealing of possible gaps and shortcomings in data protection compliance. Therefore it is no surprise that the DPO has to be experienced in this direction as well
4. Cooperation with the supervisory authority.[25] As it is mandatory, every member state of the EU has to domestically designate independent data protection supervisory authority with the powers of establishing the standards of data processing operations, providing recommendations, performing inspections and have the powers to fine data controllers and processors if the data protection legislation is breached. Having a contact point at the organization is an effective way to control the data processing activities in that particular organization
5. Acting as a contact point for the supervisory authority on issues relating to processing.[26] This requirement can be viewed as an additional condition for the previous one. However, this is one of the important aspect to characterize the role of the DPO. This requirement is aimed to ensure that the communication between the data controller and data protection supervisor is likely to be effective and the DPO acts as a representative of data controller or processor.

4. MAKING THE DPO MANDATORY IN GEORGIA

The very first act on data protection in Georgia was adopted at the end of 2011. The Law of Georgia "On Personal Data Protection" was based on prescriptions derived from the Directive 95/46/EC, in particular law of Georgia shared the core provisions, such as data processing principles, grounds for data processing, the obligations of data controller and processor and data subject rights. This law is still valid in Georgia, on the other hand, European Union had undergone major changes in this regard.

According to the EU-Georgia Association Agreement Georgia has an obligation "to ensure a high level of protection of personal data in accordance with the EU Council of Europe and international legal instruments and standards [...]."[27] As a further reference to the EU standards, Agreement states that "each Party shall, in the context of the implementation of this or other Agreements, ensure a legal level of data protection which at least corresponds to that set out in Directive 95/46/EC [...]."[28]

It's worth mentioning that Directive was ad-

22 Ibid., Art. 39(1)(a).
23 Ibid., (b).
24 Ibid., (c).
25 Ibid., (d).
26 Ibid., (e).
27 Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Georgia, of the other part, Art. 14.
28 Ibid., Annex I.

opted in 1995, at the period when data processing operations were not as intense and versatile as they are now. The fact is that whenever the technological advancement is taking place, relevant legal provisions are needed to address challenges arisen from such a development. This served as the one of the prerequisites for starting the discussions on the new regime for data protection in EU. As a result the new General Data Protection Regulation was introduced and adopted in 2016, however it entered in force two years later – on 25th of May, 2018.

Did this shift towards higher standards impose new obligations for Georgia with regard to data protection legislation to be amended respectively? The short answer is yes, it did, but one may be interested what is the reason for making this kind of conclusion? Final provisions of GDPR contain special reference to the repealed Directive 95/46/EC. It states that wherever there is any reference to the Directive it shall be interpreted as a reference to the GDPR.[29] Accordingly references towards Directive into the Association Agreement shall be construed as a reference to the GDPR.

In order to fulfil this obligation, a new draft law on personal data protection was introduced in the Georgian Parliament, which, inter alia, requires the DPO to be appointed in a mandatory manner. As this is a proposed draft act, we can't review it in details, because the final version is yet to be adopted. On another hand, draft law shares the common approach of GDPR in prescribing the functions and requirements for appointing the DPO. However, it is worth to generally mention the core requirement, namely, an obligation for public institutions and sector specific organizations, as well as, for those medical institutions that process at least 10,000 data subject's personal data to appoint or determine the DPO.[30] As it was indicated previously, this practice of not imposing this requirement for all kinds of data controllers is common, prevalent in EU countries. This exception may be occurred from the fact that larger companies are at higher risk of data breach, therefore small businesses are free from this regulation. Additionally, from the data management perspective, small organizations may handle data processing effectively due to the size of the data processed. Therefore, these two reasons may be enough to explain the exception.

CONCLUSION

Decades of development in data protection field indicates the importance and role of safeguarding individuals' fundamental right. The creation of the DPO position was preceded by several aspects, namely, advancement of technology, intensification of data processing practices, development of methods and tools used for processing. This led to the creation of special position with the tasks which was not specific to any other position before. The DPO is important position within organization to ensure greater data protection compliance.

In Georgia, the requirement of appointing the DPO is not mandatory yet. So far we do not even have any optional reference in legislation to a person/entity which may perform duties characteristic to the DPO. However, the current development and practices of privacy and data protection in Georgia are indicating that we are about to improve the most fundamental aspects of data protection and act upon higher standards set by GDPR alongside with specific and complex requirements of the legislation. Therefore, general requirement to appoint the DPO within organizations and entities may become a pathway to reach data protection compliance goals.

29 GDPR, Art. 94(2).

30 Draft law of Georgia "On Personal Data Protection", Art. 33(1). [https://info.parliament.ge/file/1/BillReviewContent/222089?].

BIBLIOGRAPHY:

1. Lambert, P. (2017). The Data Protection Officer – Profession, Rules and Role. Taylor and Francis.
2. Breitbarth, P. (2018). On large Scale Data Processing and GDPR Compliance. [https://iapp.org/news/a/on-large-scale-data-processing-and-gdpr-compliance/].
3. Article 29 Data Protection Working Party. (2017). 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.
4. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
6. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
7. Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Georgia, of the other part.
8. Draft law of Georgia "On Personal Data Protection" [https://info.parliament.ge/file/1/BillReviewContent/222089?].