INTERNATIONAL HELLENIC UNIVERSITY

The responsibilities of the DPO according to the GDPR

Pavlos Cheimonidis

SID: 3307170002

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Communications and Cybersecurity

DECEMBER 2019

THESSALONIKI – GREECE

The responsibilities of the DPO according to the GDPR

Pavlos Cheimonidis

SID: 3307170002

Supervisor:	Prof. Komninos Komnios
Supervising Committee Members:	Assoc. Prof. Name Surname
	Assist. Prof. Name Surname

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Communications and cybersecurity

DECEMBER 2019

THESSALONIKI – GREECE

Abstract

This dissertation was written as part of the Master of Science (MSc) in Communications and Cybersecurity at the International Hellenic University during the academic year 2017-2018. Thesis is separated in 6 chapters.

In the introductory chapter, a historic flashback of the most important directives, treaties and legislations which created before the so much discussed GDPR will be presented alongside with some references to the first appearance of the term DPO.

In the second chapter, the issues of which organizations should have an appointed DPO, if there is a possibility of an external DPO are going to be presented. In addition, what skills and expertise a DPO should have in order to be able to fulfil his duties according to the GDPR will be addressed.

In the third chapter the new role and the position of the DPO will be further analysed, focusing mostly on the necessary resources that a DPO should have so as to be able to fulfil his/her tasks; in addition, the DPO's independence and conflicts of interest and issues regarding his dismissal or penalty for performing DPO tasks will be addressed.

In the fourth chapter the explicit tasks that a DPO holds under the GDPR as mentioned in Article 39(1) of the Regulation will be examined in detail.

In the fifth chapter the implicit tasks that a DPO holds under the GDPR will be examined in detail. The tasks and the responsibilities that he/she has to carry out and does not mentioned in the GDPR explicitly.

In the final chapter, which constitutes the dissertation's opinion, the responsibility of the DPO in cases of non-compliance is going to be analysed. Moreover, the advantages the GDPR has brought concerning the protection of personal data will be addressed.

At this point, I would like to express my sincere thanks to my supervisor, Prof. Komninos Komnios who has inspired me and instructed me in various ways and without his precious help I would not be able to complete this dissertation.

Pavlos Cheimonidis

December 2019

Contents

1 Introduction (Background and definitions)

Before the so much discussed European General Data Protection Regulation 2016/679(GDPR)[1], there were some other legal instruments introduced across the years starting with the N.108/1981 Council of Europe Convention for the Protection of Individuals, which integrated the first binding legal text to automatic processing of personal data[2]. Six years later, in 1987 the Council of Europe embraced the Recommendation No R(87)15 about the protection of personal data[3]. In addition articles 7 and 8 of the Chapter of fundamental rights of the European Union regulated privacy and the protection of personal data as fundamental human rights[4]. In 1995 the ancestor of GDPR, that is the Directive 95/46/EC (Data Protection Directive, DPD)[5], was created. Even the most optimistic people could not even imagine the extent of technology and the decisive role of the Internet in everyday life. As we all understand a directive that was created in 1995 would not be able to face the rapid changes in cyber world. Huge development in the sectors of technology and communications came along with a parallel increase to the cybercrime and therefore the European Union (EU) was forced to take preventive measures to mitigate the new

[1] 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)

[2] European Treaty Series –No. 108, Strasbourg, 28.1.1981 Council of Europe, Convention for the Protection of Individuals with regard to automatic processing of personal data

[3] Council of Europe, Committee of Ministers, Recommendation No R.(87)15, 17.9.1987

[4] Chapter of fundamental rights of the European Union, OJ 364/1, 18.12.2000

[5] 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 [1995], OJ L 281/31

risks. In this respect the directive on electronic commerce was created in 2000[6]. Additionally, based upon article 16 (ex article 26 TEC) of the Treaty of Functioning of the European Union (TFEU), the European Parliament and the Council was mandated to establish new rules about the processing of personal and about the flow of such specific data[7].

The GDPR came into force on 25 May 2018, and it is composed by 99 Articles and 173 Recitals[1]. There are some differences between the (DPD) and the GDPR which mostly focuses on that data subjects should be aware of what data is maintained about them and how it is processed. Whilst its main purpose is to consolidate data protection for individuals within the European Union, it also lays down rules relating to the free movement of personal data in the EU and focuses on how data transfer outside of European Union should be carried out. Data that is being processed both by processors and controllers should be acquired with transparency, lawfulness and fairness. In addition, all data that is being processed should be relevant, adequate and limited to the purpose of process. Furthermore, any individual or organization that processes data should have established all the necessary organizational and technical measures to prevent any unauthorized access, destruction and accidental loss or exposure of that data. There are strict accountability requirements (Art. 5 par. 2 GDPR) that all individuals or organizations that either process or control data should establish and - in case of non-compliance - fines can reach up to 4% of the business turnover and go as high as 20 million Euros (Art. 83 GDPR). Having in mind this regime it is easy to understand that individuals or organizations that process personal data are forced to enhance their security in order to avoid getting fined.

As regards the Data Protection Officers (DPOs)[8], they are persons who advise on compliance with data protection rules in organizations undertaking data processing. They are 'a cornerstone of accountability' since they facilitate compliance, while

---

[6] Directive 2000/31/EC of the European Parliament and of the Council, 8.6.2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market (Directive on electronic commerce), OJ L 178

[7] Treaty of Functioning of the European Union TFEU, OJ C 326/47, 26.10.2012

[8] From now on each reference to DPO will mean "he or she", "his or her"

also acting as intermediaries between the supervisory authorities, data subjects and the organization by which they have been appointed[9].

The DPO institution originated from Germany in the late 1977 in the German Federal Data Protection (FDPA)[10]. Since it was considered a success[11], it was followed by a lot of other Member States like France, Belgium, Estonia, Hungary, Lithuania, Luxembourg, Netherlands, Poland, Sweden and UK. Although the concept of the (DPO) is anything but new, the GDPR makes the appointment of a DPO compulsory under certain conditions for all Member States. Accountability and enhanced protection of personal data are tasks relevant to DPO position, his/her nomination should strengthen the trust of persons regarding to their data protection which is a fundamental right[12].

The Directive 95/46/EC has introduced the concept of the DPO as a possibility for the Member States to inform the competent supervisory authority in order to simplify or exempt from notification of processing operations. According to the DPD and under the Article 18(2) the exemption or simplification may be applied when a personal DPO is appointed by the complied with the law data controller. The DPO should be able among other tasks - to keep a record of the processing operations that are executed by the controller including the information of Article 21(2) and to be able to prove in an independent manner that the data protection law applies internally. The purpose of this function is to prevent rights and freedoms of data subject from affecting adversely by the data processing. Moreover, the recital 54 of the DPD indicates that both DPO and supervisory authority must ensure that every data processing will be safe for the data subjects. Another interesting observation

---

[9] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law (2018) 175*

[10] Thoma points out that 'Siemens created a privacy function which soon became the Data Protection Officer's organization already in 1976 and thereby even ahead of the German Data Protection Act (FDPA), *which came into force in 1977*, see Florian Thoma, 'How Siemens Assess Privacy Impacts' in David Wright and Paul De Hert, *Privacy Impact Assessment* (Springer 2012) 277.

[11] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation(GDPR)* (Springer 2017) *53*

[12] Miguel Recio, *Data Protection Officer*: The Key Figure to Ensure Data Protection and Accountability by Eur. Data Prot. L. Rev. 114(2017), 114-115

about the tasks of the DPO before the GDPR was the "*Case-92/09 Volker und Markus Schecke and Eifert*" in which the Court of Justice of the European Union (CJEU) held that the DPO must keep a register with the operations that the organization carries out but he/she isn't obliged to keep any records "*before the processing of the data concerned is undertaken*"[13].

Specific legal reference concerning the appointment of a DPO is also found in the Regulation (EC) No. 45/2001[14] which clarifies that at least one DPO should be appointed by Community institutions and bodies in case that they process personal data. According to the above mentioned Regulation, the following functions should be included among the other tasks of a DPO:

- raising awareness on both data subjects and controllers about their rights and their obligations;
- responding to request and cooperating with European Data Protection Supervisor (EDPS);
- internal compliance with the provisions of this Regulation;
- preserving a registry with the executable operations of the controller;
- in cases of data processing where specific risks are present they should notify the EDPS.

Additional guidance regarding the concept of the DPO has been published by EDPS, which clarified that full-time DPO is desirable because there might be conflicts between his regular task and his responsibilities as part-time DPO. In any case the DPO should be fully independent and able to perform their tasks with a sufficient degree of autonomy. At the same time the DPO should have a central role within the organization meaning that he should know what operations the organization carries out and what personal data is maintained. In addition, the DPO should be provided with all essential staff and resources to be able to complete his duties. Although there is no explicit reference to it in the Regulation (EC) No. 45/2001, the

---

[13] Case-92/09 Volker und Markus Schecke and Eifert (CJEU, 9 November 2010) ECL:EU:C:2010:662, paras 98-99.

[14] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L 8/1.

DPO should be able to handle and respond to all queries and complaints and also to carry out investigative actions either by his own or if he is ordered to. On the other hand a DPO has no power regarding the enforcement; the only thing he could do if any failure to compliance has been noticed is to bring the issue to the attention of the Appointing Authority[15].

There has been another document[16] which provides extra details about the profile of the DPO, minimum standards that he should have and his duties. According to the above mentioned document, the DPO needs both knowledge about the operation of the organization and expertise in data protection law and privacy criteria within the EU. In addition, for the first time there were clear indications about the continuous education that the DPO should receive in order to stay expertise in this area. Moreover, there were some recommended qualities that a DPO should possess, specific instructions under what conditions to remove or appoint a DPO and a more detailed guidance about his duties and how they should be carried out. Comparing to the Regulation (EC) No. 45/2001 and the following guidelines on the paper "*on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001*" one extra task for the DPO has been added: to advise the appointing organization about the provisions that need to be established for data protection and suggest improvements for the protection of the data. Having taken into consideration the variety of the EU institutions and bodies, the EDPS suggested best practices that a DPO may follow as a reference. Another innovative section in this paper is that there is a special section about the ethical standards of a DPO.

To sum up, in this introduction the subject of the thesis we spotted specific differences regarding the concept of DPO between the Directive 95/46/EC and the GDPR. Moreover, individual references about the data protection on some legal instruments, the creation of the concept of the DPO and its origin have been presented. As we have been moving closer to the creation of the GDPR, the concept of the DPO was gaining importance with more details, more tasks and even suggestions to

---

[15] Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, 28 November 2005 , Brussels

[16] Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001, 14 October 2010

best practices. It was the Regulation (EC) 45/2001 and the following papers about it that take the concept of the DPO to the next dimension as well as the raising of awareness about the protection of the data and how this can be achieved. All these references in guiding papers, directives and regulations have played a crucial role to the compulsory designation of DPO (under certain conditions) according to the GDPR. The GDPR recognizes that the DPO has a key role in the new data protection legislation and therefore a detailed framework regarding the DPO's designation, position, duties and tasks (Art. 37-39 GDPR). It should be mentioned that the Article 29 Working Party (WP29) adopted guidance on the role of the Data Protection Officer (DPO) under the new General Data Protection Regulation (GDPR) last April 2017[17].

To enhance the knowledge in the field, this thesis goal is to examine the functions of the DPO under GDPR, his responsibilities, duties and of course the decisive role that he plays to the protection of personal data within an organization. Furthermore, we are going to analyse the designation of DPO, his position and his tasks in the following four chapters.

The literature for conducting the research was laws, regulations, guidelines and legal documentation. Relevant parts of the GDPR have been read together with associated recitals.

[17] Article 29 Working Party (2017), *Guidelines on Data Protection Officers ('DPOs'),* WP 243 rev.01,last revised and adopted 5 April 2017. The Article 29 Working Party was an advisory body made up of representative from data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. On 25 May 2018, it has been replaced by the European Data Protection Board (EDPB) under the GDPR.

2 Second Chapter

In this chapter we are going to address the issues of which organizations should have an appointed DPO, if there is a possibility of an external DPO, what skills and expertise a DPO should have in order to be able to fulfil his duties according to the GDPR.

2.1 The mandatory designation of DPO

Under Article 37(1) of the GDPR, data controllers and processors must designate a DPO in any case where: "(*a) The processing is carried out by a public authority or body except for courts acting in their judicial capacity; (b) the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or processor consist of processing on a large scale of special categories of data or personal data relating to criminal conviction and offences*".

It should be stressed that designation of a DPO may be required "*in cases other than those referred to in paragraph 1*" depending on the member state and its national law, as stated in Article 37(4) GDPR.

The provisions of the GDPR concerning the DPO apply to both data controllers and data processors but it depends on who will fulfil the mandatory designation criteria above as to whether a DPO has to be appointed or not. The WP29 argues that even if only the data controller fulfils the mandatory designation, it may be good practice for the data processor to appoint a DPO anyway.

According to the WP29 key criteria concerning the mandatory designation of a DPO are the following:

2.1.1 Record

So as to comply with the accountability principle (Art. 5 para. 2 GDPR), the WP29 proposes that controllers and processors keep a record of their documented decision whether or not to appoint a DPO in order to be able to prove that all relevant prerequisites have been taken into consideration.

2.1.2 Processing by public authority or body

The notion of public authority is not defined under the framework of the GDPR; each Member State must define this notion under its national law. In most cases national, regional and local authorities as well as a range of bodies governed by public law[18] are included in this notion. Every Member State could define the framework of public authority or body that makes the designation of a DPO mandatory.

In addition, natural or legal persons governed by public or private law could carry out a public task: public transportation system, medical associations, road infrastructure and energy supplies are some examples of sectors that should appoint a DPO. In cases like the above mentioned the processing of the data is very similar to the processing that is being made by public authorities or bodies, data subjects have limited choice over how and whether there data is processed and thus the designation of a DPO will enhance the data protection. Although there is no requirement by the Regulation for an appointed DPO in such cases, the designation of a DPO is suggested by WP29 as good practice to cover all processing operations that the organization carries out independently if they are directly related to the exercise of public task or official duty[15].

2.1.3 Core Activities

Article 37(1b) of the GDPR refers that a DPO appointment is mandatory when the core activities of the organization (either the controller or processor) are processing operations that require systematic monitoring on large scale of data subjects[1].

In addition, article 37(1c) of the GDPR refers that a DPO appointment is also a necessity when, the core activities of an organization (either the processor or the controller) are processing operations that require a large scale processing of special categories of data pursuant to Article 9 as well as personal data that contains information about offences and criminal convictions of the data subjects referred to in Article 10[1].

In Recital 97 of the Regulation there are further clarifications on what can be considered as "*core activities*" for both private and public sector separately. Key operations that are vital for controller or processor in order to achieve their goals can be considered

[18] See e.g. the definition of '*public sector body*' and '*body governed by public law*' in Article 2(1) and (2) of Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public-sector information (OJ L 345, 31.12.2003, p. 90).

as core activities, but these actions include only the main operations of data processing of the organization and not the secondary – ancillary activities (e.g. organizations processing payroll data for their employees).

WP29 explain this by analysing the operation of a hospital. A hospital has as core activity to provide health care to all patients. This activity is inextricably linked to the processing of the health data of patients in order to be completed in a safe way. The aforementioned processing can be considered key operation and accordingly core activity of the hospital to achieve its goals, as a result the designation of a DPO is mandatory for the hospital[15].

2.1.4 Large scale

Article 37(b) and (c) GDPR refer to the "*large scale*" processing of data, but the GDPR leaves undefined what number constitutes large processing. Recital 91 states that "*large number of data*" means:

- processing of a big amount of personal data to regional or national level;
- processing that could affect a big number of data subjects;
- processing of personal data that involves high risks for the rights and freedoms of data subjects.

To sum up, both Articles and Recitals leave the area of the number regarding to a large scale grey.

Having in mind that this number refers either to the amount of data processed or the number of individuals concerned, it is rather impossible to give a precise number which would be applicable in all situations and that is the reason why a specific number hasn't been prescribed in the Regulation.

The WP29 tries to shed some light to this area having in mind the Recital 91 of the GDPR; it recommends that the following factors can be considered as large scale processing when determining what qualifies as "*large scale*" processing[15].

- The proportion of data subjects comparing to the population of a specific area
- The total number of data subjects
- The volume that a process of data is being done
- The processing duration
- The extent of the process geographically

According to the WP29 examples of large scale processing could be:

- processing of personal data for behaviour based advertising carried out by a search engine;
- data processing conducted by ISP and telephone companies;
- processing of real time geo-location data of customers of a fast food chain for statistical purposes by a specialized provider;
- processing of patient data in the regular course of business by a hospital.

Processing of personal data from a layer or a doctor does not constitute large scale processing notwithstanding the fact that this specific personal data contains health information and criminal convictions which is considered sensitive data. As long as this personal data is processed by an individual, it does not normally constitute large scale processing.

2.1.5 Regular and systematic monitoring

The aforementioned header is another grey section under the framework of the GDPR1 as the Regulation does not provide clarification of what should be considered as "*regular and systematic monitoring*". On the other hand in the recital 24 of the Regulation it is mentioned that "*in order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether 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*".

The WP29[15] tries to further clarify the meaning of "*regular*" as referred in the Regulation by giving some non-exclusive examples.

- Any action that is repeating at settled or prearranged times
- Any action that takes place periodically or constantly
- Any action that happens periodically or ongoing and has a specific duration

The WP29[15] also offers a more detailed interpretation of what can be considered as "*systematic*".

- Any action occurs according to a schedule
- Any pre-arranged or methodical action that takes place
- Any action that has been involved in data collection plan
- Any contain that has been contained in a strategic plan

Non-exclusive examples of what can be considered as regular and systematic monitoring could be: devices for tracking locations, providing telecommunication services, profiling for automated decisions or scoring, behavioural adverting, e-mail retargeting, fitness and health data via wearable devices, even home automations when they keep log files available for storage and review.

2.1.6 Sensitive personal data (special categories of data)

The Regulation is very specific on what data should be considered as "*sensitive*" personal data. In Article 9(1) more particularly it is provided that any processing that contains information about political opinions of the subjects, philosophical beliefs, racial or ethnic origins, generic data, biometric data, sexual orientation is strictly prohibited. The processing of all the aforementioned categories can be carried out when very specific prerequisites are fulfilled, (Article 9(2) GDPR). Such exemptions under which it is permitted to process sensitive personal data are for instance when personal data are made manifestly public by the data subject itself, or for statistical, scientific or research purposes. In addition, some more exemptions are when the data subject gives the explicit consent for this specific data to be processed, or when it comes to the protection of the vital interests of the data subject, or for purposes of substantial public interest in the area of public health and public safety, or in the course of legitimate interests. There are some more exemptions that allow this processing such as for specific purposes under which the processing is necessary such as in the field of employment law or in the social security or in the social protection law, or for preventive and occupational medicine purposes or even for the assessment of the working capacity of the employee falling within the professional secrecy.

Personal data relating to criminal offences and convictions as mentioned in Article 37(1c) GDPR, fall under the protective scope of Article 10 GDPR, in the sense that this type of sensitive data can be processed "- *only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority*".

2.1.7 Conclusions

Nowadays there is confusion in the area regarding the organizations and the mandatory designation of a DPO, but in the author's opinion as more legal papers regarding the Reg-

ulation are published providing more details and guidance the insecurity will be fully mitigated and no more grey areas shall exist. As already analysed, the GDPR makes appointing a DPO mandatory in three specific cases: where a public authority or body carries out the processing; where the controller's or processor's core activities consist of processing operations which require the regular and systematic monitoring of data subjects on a large scale or where the core activities consist of large-scale processing of special categories of data or personal data relating to criminal convictions and offences.

All other organizations are not legally obliged to appoint a DPO. However, the GDPR provides that controllers and processors may choose to voluntarily designate a DPO (Art. 37 (4) GDPR). The WP29 encourages such voluntary initiatives. However, when an organization appoints a DPO voluntarily, "*the same requirements will apply to his or her designation, position and tasks as if the designation had been mandatory*".

2.2 Expertise and skills of the DPO

Article 37(5) provides that "*the DPO 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 referred to in Article 39*". The necessary level of expert knowledge that a DPO should have depends on the processing operations an organization carries out and the required level of protection regarding personal data. For example, if data processing is particularly complex, or when a big quantity of sensitive data is involved, or if the organization systematically transfers personal data outside of the European Union, the DPO may need a higher level of expertise and support.

The WP29[15] gives some specific directions on the skills and expertise the DPO should have in order to be able to fulfil his tasks.

2.2.1 Professional qualities

There is no clarification about the professional qualities a DPO should have in order to be eligible for the position; according to the WP29, he should have expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR. Moreover, the DPO should be fully aware of the processing operations of the controller/processor and have in-depth understanding for every personal data record in order to be able to protect. The DPO should also posses understanding of information technologies and data security and knowledge of the relevant business sector and organization. The same holds in case that the organization is a public authority or body; moreover, in

the above mentioned case the DPO should have knowledge of the relevant administrative rules. The ability to promote a data protection culture within the organization is also of importance.

The supervisory authority should provide for adequate training for DPOs on regular basis in order to update and maintain their expertise in the data protection field as well as to be informed about the innovations in the information technology sector. Furthermore, DPOs are recommended to participate in EU teams that consist of people with similar tasks and duties, to exchange ideas and practices, cooperate with university research teams and also study documents that EDPS[19] and ENISA[20] will publish occasionally. Alongside with all the professional qualities that a DPO should have, it is recommended to dispose relevant personal skills so as to be able to perform his duties better; discretion, organizational skills, integrity, high professional ethics and perseverance are some of them. In addition, due to the communications task that he should complete, it is strongly recommended to have strong interpersonal skills such as conflict resolution abilities[13].

2.2.2 Ability to fulfil its tasks

Ability to fulfil its tasks is not restricted to the integrity and high professional ethics of the DPO. An appointed DPO in any organization should have as primary concern to enable and foster compliance of the organization to the Regulation. Every DPO should be able to perform both his tasks as a DPO and his work duties (in case he is a part-time DPO) without neglecting one or the other; he should be able to combine them, taking advantage of the key position that he holds within the organization. As analysed, he has a key role in raising awareness for data protection within the organization and in helping implement essential functions of the GDPR, such as notification and communication of data breaches as well as principles of data processing.

If we could use a diminutive, one could say that regarding data protection he is the "glue" in the framework of an organization that sticks everything together.

2.2.3 Level of expertise

There is no specific provision as regards the level of expertise a DPO should have, but it must be proportional to the amount of data and the sensitivity of this data that an organi-

[19] European Data Protection Supervisor

[20] European Union Agency for Network and Information Security

zation either holds or process. A recommendation would be for a DPO to have at least 3 years of relevant experience to an organization that does not process data as its main activity and at least 7 years of relevant experience to an organization that carries out processing as its main activity. We can clearly observe that the level of expertise of a DPO is absolutely dependant to what the core activities of the organization is. In addition, a single appointed DPO might not be able to handle a very complex organization system that carries out processing of sensitive data, therefore a team that will have many DPOs or a team that will have many experts that will be able to carry out tasks and activities to help the main DPO might be needed. In this latter case in order to avoid conflicts of interests for the team members, it is beneficial when every team member has limited assignments and clear allocations of his tasks while a lead member has the general overview. The last element that an organization must carefully examine before appointing a DPO is whether there is occasional or systematic transfer outside of European Union to organizations that are included in the EU-US Privacy Shield[21].

2.3 Appointment of a single DPO or more

Article 37(2) and 37(3) of the GDPR define that "*a group of undertakings may appoint a single DPO…" and "where the controller or the processor is a public authority or body, a single DPO may be designated…*" respectively.

Having in mind Article 37(2) of the Regulation, there is the possibility for a designation of a single DPO by a group of undertakings on condition that the single DPO is easily accessible from each establishment. The legislator did not specify what "*easily accessible*" means. The term could be interpreted as referring to technical or actual availability of the DPO[22]. The WP29 argues that "*the notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects, the supervisory authority but also*

[21] COMMISION IMPLEMENTING DECISION EU 2016/1250 of 12 July 2016-Pursuant to Directive 95/46/EC of the European Parliament and of Council on the adequacy of the protection provided by EU-U.S Privacy shield (notified under document C(2016) 4176.

[22] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR),* (Springer 2017) 55

internally within the organization". In this respect, the contact details of the DPO should be available[23].

2.4 Conclusions

A DPO should have expertise in law especially in the privacy and data protection law and furthermore to possess necessary knowledge about the security of an information system. His main task within the framework of an organization is to achieve the best possible compliance of the organization and raise the awareness of the employees about data protection. There are no specific provisions about the level of expertise a DPO should have, they depend totally of what operations an organization carries out and the amount and type of data it is processed.

[23] In this exact wording of the WP29 "The availability of a DPO (whether physically on the same premises as employees, via a hotline or other secure means of communication) is essential to ensure that data subjects will be able to contact the DPO."

3 Third Chapter

In this chapter the new role and the position of the DPO will be further analysed, focusing mostly on the necessary resources that a DPO should have so as to be able to fulfil his tasks; in addition, the DPO's independence and conflicts of interest and issues regarding his dismissal or penalty for performing DPO tasks will be addressed.

3.1 The new role

A new era has begun with the adoption of the GDPR; all organizations –even small ones- covered by the territorial scope of the Regulation (art. 3 GDPR) should comply with the GDPR. Compliance with data protection regime applies both to the processor and the controller. The role of the DPO as well as his responsibilities and tasks are regulated in Articles 37, 38 and 39 of the Regulation.

3.2 Necessary resources

Art. 38 (2) GDPR requires that the controller or the processor should provide the DPO all necessary resources so to be able to carry out his tasks effectively. The term "*resources*" does not refer only to financial resources; its meaning is a general support of the functions of the DPO by the organization. We can interpret the term "*resources*" as sufficient equipment, infrastructure and information about the personnel that a controller or a processor should provide the DPO with, in order the last to be able to complete his tasks in an effective way. In the framework of the organization these resources could be referring to elements of the Human Resources (HR) or the accounting or even of the information technology (IT) sector, or any part of the organization that is necessary for the DPO to complete his tasks. Given the fact that a DPO could be already part of the respective organization and has also work projects to complete, it is necessary that sufficient time will be given to the DPO to carry out his tasks. The DPO should not be impeded to perform his tasks. The DPO should be guaranteed sufficient time to fulfil his duties even if he isn't employee of the organization, meaning that he has no work projects to complete in parallel.

In the case that an appointed DPO is an employee of the organization a separation of duties is required between his work projects and his DPO tasks. A well-thought schedule must be created to ensure that the employee will have the necessary time to complete his DPO responsibilities

without neglecting them. If the employee has an overwhelming work program, then he should either reject the DPO position or ask for support (creation of an appropriate team to help DPO carry out his tasks). The position of the DPO is very responsible and whoever appointed, it must be ensured that the required time will be devoted in order for all of his tasks to be carried out effectively.

The DPO should be provided with all the appropriate support and knowledge about the organization and the operations that it carries out, and he should have access to all instances of the organization so to be able to gather every possible information regarding data protection. After the appointment of a DPO, he should communicate with every department of the organization, for instance with the IT sector, legal department, HR and even with the external associates, for instance the security company which is responsible for the installation and the maintenance of the CCTV. The DPO should have knowledge about everything within the operation framework of the organization having to do with data processing.

Another very important element is the training of the DPO. If we consider the concept of the DPO within the framework of the GDPR, his duties and responsibilities, we can easily understand the importance of continuous training. New amendments and recommendations are published every day; in these documents may be included extra information, additional guidelines and also best practices. Obviously new knowledge is of paramount importance for the DPO to perform his tasks adequately. In addition, except of the legal papers regarding to the data protection, the DPO must stay also informed about the technological sector. Innovations here are even bigger and more often. The DPO should be aware of new technologies in the information security sector and understand how they work and what extra security they offer, so as to enable enhanced protection of data and avoidance of personal data breach. To be able to handle all this vast need for knowledge updates, the WP recommends that the DPO attends seminars, workshops and training courses so as to increase his level of expertise both in legal and IT sector.

To sum up, the WP29 considers the following as being necessary resources:

- Active support of the DPO by senior management (such as board level)
- Sufficient time to fulfil their duties
- Financial, infrastructure and staff resources
- Official communication of the DPO appointment to all employees
- Access to stakeholders such as HR, Legal, IT, Security etc
- Continuous training

- A DPO team depending on the size and structure of the organization

All necessary resources required depend on the size and the complexity of the organization as well as the amount and the sensitivity of information it processes. For instance, a big hospital will need a team of DPOs, since a hospital carries out processing operations that contain sensitive personal data and the amount of patient is relative big. In this latter case, it will be hard for a single DPO to be able to perform his tasks effectively, considering the type and the amount of data, so as best practice a team of DPOs or a team devoted to DPO's support is recommended.

3.3 Participation of the DPO in everything that relates with the protection of personal data

Article 38 of the Regulation[1] provides that the DPO should be involved in all issues regarding the protection of personal data properly and in time; it is the responsibility of the processor or the controller to ensure this involvement. Either a single DPO or a team consisted of DPOs should participate in every issue relating to data protection from the very first stage in order to perform their tasks as efficiently as possible. This involvement is of paramount importance in order to avoid data breaches at early stages of processing operations.

Communication and cooperation from the early stage with the DPO will ensure compliance with the GDPR and privacy of individuals. In the framework of the data processing operations the DPO shall be seen as an advisor that will help the organization to protect personal data during its operations. Working groups and managers shall discuss every issue relating to personal data with the DPO and total transparency is necessary so that the DPO will be able to fulfil his tasks.

Having in mind all that, indicative examples of the DPO's involvement could be: participation of the DPO in senior, middle and even high management meetings as long as the point of discussion is the protection of data or at least it is a part of the meeting; everyday meetings in which employees are talking about everyday operations within the organization; when the organization is about to start a new action, even if this action does not involve data processing as its core activity, the update of the DPO about this new operation as well as his advise could be considered as best practice; when there is a data breach the DPO should be informed as soon as possible; when there is a disagreement between the managers of the organization and the DPO, WP29 suggests to document the reasons of disagreement.

As regards the conduct of a Data Protection Impact Assessment (DPIA), Article 35(2) GDPR specifically requires that the controller "*shall seek advice*" of the DPO when carrying out a DPIA. Article 39(1c) GDPR provides that the DPO should "*provide advice where requested as regards the [DPIA] and monitor its performance pursuant to Article 35*".

Indicatively, the WP29 recommends that the controller should ask for the DPO's advice on the following issues:"

- *whether or not to carry out a DPIA*
- *what methodology to follow when carrying out a DPIA*
- *whether to carry out the DPIA in-house or whether to outsource it*
- *what safeguards (including technical and organizational measures) to apply to mitigate any risks to the rights and interests of data subjects*
- *whether or not the data protection impact assessment have 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 the GDPR*".

3.4 Independence

Article 38(3) provides that the DPO shall not "*receive any instructions regarding the exercise of their tasks*", meaning that while completing his tasks he must be absolutely independent. This ensures that DPO's decisions or advice will not be affected by the managers of the organization in order to protect personal data in the best possible way. Moreover, article 38(3) states that "*the DPO shall directly report to the highest management of level of the controller or the processor*", and provides that the opinion of the DPO will be taken into consideration by the highest level, and will not be undermined or ignored within an organization. His advice or opinion in the matters of data protection will not be buried by the layers of bureaucracy.

Article 38(6) provides that the DPOs may "*fulfil other tasks and duties*" as well. Recital 97 states that "*whether or not the DPOs are employees of the controller, they should be in a position to perform their duties and tasks in an independent manner*". By interpreting the above statement we can assume that even if the DPO is an employee of an organization, his DPO tasks and responsibilities must not be affected by this position, meaning that total absence of conflict of interest between his regular work and his duties as DPO is required. The organization must ensure that every other task of this specific

employee will not affect his DPO tasks and even if this is the case then, all these tasks must be assigned to another employee of the organization.

Having in mind all the aforementioned there are some indicative examples of what positions a DPO should not have in order to avoid possible conflicts of interest: for instance a DPO should not be head of the marketing department, head of HR, director of the financial sector. Any position within the organization that may allow him or her to determine the purposes and the means of the processing of personal data should be avoided. It is absolutely necessary that the DPO has knowledge of the processing activity in the framework of the organization but this knowledge should not be food for second thoughts regarding his duties and responsibilities regarding the protection of personal data. This is especially difficult within small organizations that may be required by law to have a DPO because they belong to some category that the appointment of the DPO is mandatory. Employees in small businesses and especially top level employees are doing more than one task regarding their job and their position and there is no clear separation of duties. In my view these organizations should appoint an external DPO so as to avoid possible conflict of interest.

The term "*independence*" means that the DPO should not receive any instructions on how to deal with an issue regarding the protection of personal data or the processing of this data. Furthermore, he should be able to start any investigative actions when he receives any information or complaints without getting directions by the managers. Also, he should be able to consult the supervisory authority without any interference.

On the other hand the DPO has no power regarding the decision-making within the organization either he is already an employee that acts also as DPO or as external contractor; the organization can be either the controller or the processor. The last two are the only responsible for their compliance with the GDPR. The DPO can only advice new measures but he is not liable for implementing them. In case that there is an obvious conflict between the DPO's guidelines and the decisions of the organization regarding the processing of personal data, it is the responsibility of the DPO to express his opinion with clear way, so to be totally understood.

There will be times within an organization that the DPO's opinion will be in opposition with managers' acts or processing activities. I argue that it should be considered as best practice to follow and implement the DPOs' instruction since in any case he will not

be the one that will be liable for the organization's non compliance and he will not be the one that will be fined by the DPA[24].

The DPO or the team working as DPO must treat any disclosed information relating to personal data either in electronic form or in written with total privacy and confidentiality[25]. All these information must be used by the DPO only to carry out his tasks within the organization and for no case for personal use. This duty of secrecy/confidentiality does not mean that the DPO is prohibited from contacting and seeking advice from the supervisory authority. Article 39(1e) GDPR provides that the DPO can consult the supervisory authority, where appropriate, with regard to any matter.

3.5 Dismissal or penalty for performing DPO tasks

Article 38(3) by stating that the DPO can "*not be dismissed or penalized by the controller or the processor for performing [their] tasks*", provide the DPOs with protection to carry out their tasks and simultaneously reinforce their independence and autonomy within an organization. DPOs cannot be dismissed under the GDPR for performing their tasks. This gives the DPOs the opportunity to express their opinion without fear especially in cases that their opinions are against the will of the managers. Such a case may evolve for example when the DPO believes that the processor's or controller's processing activities could result in high risk for the data subjects and accordingly a DPIA is necessary. In this latter case the organization cannot dismiss the DPO for giving his advice even if this advice is in contrast with the organization's management. As mentioned above the GDPR aims to give freedom, autonomy and protection to the DPOs because this is considered as best practice to carry out their difficult tasks.

However, GDPR does not prohibit all penalties regarding the DPO; it prohibits only those that are imposed as a result of the DPO performing his tasks to protect personal data. Penalties may vary; for instance there could be intentional delay of promoting an employee acting as DPO or denial of some bonuses that all the other employees of this de-

[24] Data Protection Authority; responsible for fining organizations that fail to comply with the GDPR regarding the protection of personal data

[25] The DPO shall be bound by secrecy or confidentiality concerning the performance of its tasks, according to EU or EU Member State law, Art. 38 (5) GDPR

partment have received. In most cases a mere threat is enough rather than the implementation of these penalties.

Obviously general management rules of the organization as well as national law continue to apply to DPOs; accordingly any DPO can be dismissed for reasons other than carrying out his duties and responsibilities regarding the protection of personal data. A DPO can be fired for criminal acts or gross misconduct, such as theft, or physical, psychological or sexual abuse.

The GDPR does not define how a DPO can be replaced; one logical scenario is that the DPO is replaced when the specific employee reaches the age of mandatory retirement. It is strongly recommended that the DPOs have stable contracts to enhance their capability for acting independently with all the privileges this freedom offers regarding the protection of personal data

3.6 Conflicts

As mentioned above (section "2.3 Independence" paragraph 3), the DPO should not hold a position that will bring him in conflict with his responsibilities as DPO and we also gave some indicative positions within an organization which most likely do not match with the role of a DPO. In more general terms we could argue that no DPO should have a position by which he can control the means and the purposes of data processing within an organization, (for instance head of marketing department). This does not mean that a DPO may not hold a high level position in an organization; on the contrary, he can be chief of any department as long as his work tasks do not involve defining of the means and purposes of processing operations. On the other hand even lower level position within the framework of the organization could control the means and purposes of processing. Employees in this latter case are excluded from being a DPO within an organization. WP29[15] suggests relevant best practices for both controllers and processors to apply, depending on the size and the processing activities of each organization:

- Identification of all position and departments which should be excluded from the process of appointment of DPO, as long as the DPO is an internal employee of the organization. For instance, if there is an employee in a specific department that is the most capable of being a DPO within the organization, then the organization must take care of the transfer of this employee to another department

- A detailed explanation of what can be considered conflict of interest within the framework of the organization should be announced to all employees
- To enhance the trust of their employees to the function of the DPO, the organization must publicly clarify that there is no conflict of interest
- Even if the DPO is recruited externally the organization should provide sufficient evidence that there is no conflict of interest

4 Fourth Chapter

In this chapter the explicit tasks that a DPO holds under the GDPR as mentioned in Article 39(1) of the Regulation are examined in detail. These tasks are summarized as follows: give advice on DPIA and check its implementation; cooperate with supervisory authority; be the contact point for the supervisory authority; monitor compliance; advise and inform when necessary both the processor and controller of their obligations; analyse the risks associated with the processing operation.

4.1 Advice on DPIA

The controller is required to ask for the advice of the DPO as provided in Article 35(2) GDPR and is the responsibility of the DPO to provide his advice, when asked about the DPIA (Article 39(1c) GDPR). The aforementioned task has been already addressed above (under 2.2).

4.2 Cooperation with the supervisory authority

Pursuant to Article 39(1d) GDPR, the DPO bares the task to cooperate with the supervisory authority. The supervisory authority can gain access to information and documents that are related with personal data processing operations of the organization through the communication with the DPO. The supervisory authority can use this process to exercise its corrective and disciplinary actions. Cooperation with supervisory authority is not the only task that a DPO has in connection with the supervising authority. It is his responsibility to act as its contact point[26]. If the supervisory authority requests an investigative action of an organization, the DPO is obliged to provide the authority with information he receives, as he acquires knowledge about personal data within the organization. For instance, he may be asked to provide the authority with information such as types of personal data being processed by the organization or technical and organizational measures implemented by the organization to prevent data breaches.

The supervisory authority shall inform the DPO when they are about to conduct an audit to the appointing organization. I any case to avoid unpleasant surprises, it is rec-

[26] This includes the prior consultation according to Art, 46 GDPR

ommended as best practice that the DPO shall conduct the supervisory authority for any relevant matter.

4.3 The DPO shall be the contract point for the supervisory authority

It was always considered as best practice that the supervisory authority is informed who is the DPO in an organization and has his contact details (phone number, e-mail address) in order to be able to communicate with him in case there is a need; for instance, a data breach issue. Art. 37 (7) GDPR now demands that "*the controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority*". Still there is no official requirement for any form of registration of the organization, neither controller nor processor, itself with the supervisory authority under the new Regulation.

It is of paramount importance that communication between DPO and the supervisory authority be carried out in the most responsive and effective way in order for the upcoming issues to be solved as soon as possible.

The supervisory authority may contact DPO for many different matters; for example, enforcement issues, compliance with the GDPR, receiving complaints or even prior consultations. In addition, the DPO may contact the supervisory authority when they have queries on new or existed regimes or when he needs advice or consultation on a specific issue. As we mentioned above the communication between the DPO and the supervisory authority must be consolidated.

The recognition of the DPO as a contract point is the recognition of the new profession and its importance in data protection within the framework of the organization[27].

4.3.1 Acting as a contact point for data subjects

All requests and complaints of the data subjects are going to be addressed by the DPO; therefore, the DPO will help the organization to achieve compliance with the new Regulation and to carry out data processing activities without violating the rights of data subjects. Another important task of the DPO is to assist the controller, when the latter noti-

[27] Paul Lambert, *The Data Protection Officer, Profession, Rules, and Role* (Auerbach Publications, 2016) 131

fies[28] the data subject whose data has been violated in order to protect the data subject from further economic losses, (for instance a data subject will cancel their cards as soon as they are informed that there was a data breach regarding the credentials of their cards).

4.3.2 Notification of a personal data breach to the supervisory authority

As mentioned, Article 39(1) GDPR provides that the DPO should be the contact point for the supervisory authority in any matter relating to data protection, including prior consultation. In case there is an incident of data breach the supervisory authority must be informed as soon as possible by the controller; the maximum time limit has been set to 72 hours from the incident (Art. 33 GDPR). The DPO shall help to implement this essential element of the GDPR as well.

4.4 Monitor compliance

Regarding the minimum tasks of the DPO, Article 39(1b) of the Regulation reads as follows: "*to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor 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*". This Article provides for a variety of tasks regarding the DPO which we are going to analyse in the following sections.

4.4.1 Monitor compliance with GDPR

Recital 97 further specifies that DPO "*should assist the controller or the processor to monitor internal compliance with this Regulation*". The DPO is responsible for monitoring the compliance and also give his advice to achieve compliance but is not the one responsible for not achieving compliance in the organization. It is the liability of the controller or/and the processor to comply with the new Regulation (cf. Art. 24 (1) GDPR)[29].

[28] Art. 34 GDPR

[29] The WP20 Guidelines mention several times that 'DPOs are not personally responsible in case of non-compliance with the GDPR

Obviously the DPO can help to manage responsibility (of the above mentioned persons) by reducing the risk of any illegal data processing activity[30].

When monitoring compliance, DPOs may, according to WP29[31]: "

- *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*".

The more knowledge about the processing activities that have been carried out by the organization the DPO has, the best compliance will be achieved. The role of the DPO is to assess, review, amend and help implementing measures for data protection and in any case it is not limited to mere monitoring[32]. He should be allowed or even better urged to use any available tools to assist achieving compliance within the organization.

4.4.2 Monitor compliance with other EU Member States data protection provisions

Article 39(1) GDPR states that "*The Data Protection Officer shall have at least the following tasks: … (b) to monitor compliance with other Union or Member State data protection provisions*." The DPO must have the knowledge and the capability to adapt the compliance of the organization to the national data protection rules when the latter should be applied. In case that the organization offers goods or services in other countries also, besides the one that the headquarter is located, the DPO must adapt the organization to achieve compliance in all these countries if there are differences between the national law and the GDPR. Furthermore, the DPO must take into consideration any EU law that may apply to this specific organization and assist implementing it.

4.4.3 Monitor compliance with policies

As we mentioned above, Article 39 GDPR assigns multiple tasks to DPO; one of them is to monitor polices in order to achieve compliance. The goal of the DPO is to achieve compliance in every department of the organization, from marketing to HR, from

---

[30] Miguel Recio, *Data Protection Officer*: The Key Figure to Ensure Data Protection and Accountability by Eur. Data Prot. L. Rev. 114 (2017), 117

[31] Article 29 Working Party (2017), *Guidelines on Data Protection Officers ('DPOs'),* WP 243 rev.01, last revised and adopted 5 April 2017, 17

[32] Paul Lambert, *The Data Protection Officer, Profession, Rules, and Role* (Auerbach Publications, 2016) 123

doctor's office to IT, by providing every employee of the organization all necessary guidelines alongside with best practices that should be followed in order to protect the data. While the DPO is monitoring the policies in an organization, he may review the already established policies, initiate new policies regarding data protection issues or even recommend amending some of the existing if they are violating the rules of processing according to the GDPR.

The policies may be addressed to employees of the organization or to external suppliers or customers. Policies should be clear and simple in order to become totally understood by all parties that they are referring to without the need of providing extra clarifications.

The DPO must pay extra attention to every contract of the organization, including clauses, provisions, several terms and conditions because they may "hide" problems relating to data protection and accordingly the compliance of the organizations with the Regulation.

The DPO should review the existing policies and propose changes in order to adapt them to the new Regulation; for instance there might be a consent policy which uses the method of pre ticked boxes for consent. Under the GDPR that must change since pre ticked boxes are not considered valid for consent. Other policies could refer to data transfer or transparency; it is the responsibility and task of the DPO to adapt all policies of the organization to the GDPR and if they don't exist, he should recommend creating them. The DPO must have an active role even in the security policy document, which has been created by IT experts, for the protection of physical and information technology assets. For instance, the DPO must highlight that sensitive data (e.g. health records of employees need extra level of protection).

The DPO must assist the organization to create new policies and/or adapt the old ones in order to comply both with the GDPR and the national law; all these policies should be monitored and reviewed in order for the organization to keep its compliance. To sum up, monitoring compliance in general is an important, complex, wide-ranging and ongoing task.

4.4.4 Monitor assignment of responsibilities

The inclusion of the phrase monitor "*assignment of responsibilities*" as it is referred in Article 39(1b) GDPR, could mean that the DPO shall monitor the compliance in any kind of transfer. For instance, data transfer from controller to processor, data transfer from

controller to controller, contracts' transfer, assets' transfer, policies' transfer and even personnel transfer[33]. The main value that is being transferred in all the aforementioned cases may be personal data, or even if this is not the case, personal data will be included in the above transfer more or less. The DPO shall advice the organization on how to achieve compliance regarding the data protection in all the aforementioned transfers and in any transfer that may contain personal data and simultaneously monitor the level of protection that has been achieved in order to determine if these transfers are complied with the GDPR and the national law.

4.4.5 Awareness – raising and training of staff involved in processing operations

In recent years there is a growing concern regarding with the protection of personal data especially their movement through internet. Safer Internet Day and Data Protection Day are some of the many relevant international events; still most of the people are not very familiar with the concept of data protection. When it comes to the protection of the data within an organization, it is responsibility of the DPO to increase the awareness of the staff. All departments of an organization should communicate with the DPO, but there are some departments like the IT, the HR and the marketing that need to establish an ongoing relationship. The latter two departments normally carry out the most processing (if not all) of personal data within an organization whereas the IT sector is responsible for the majority of the data breaches and the best possible security of the organization. It is task of the DPO to train the staff in order to raise their awareness. The DPO must persuade people and make them understand about the risks that may evolve by a data breach and not just implement strict measures.

In the next paragraph we are going to suggest some best reasonable principles which a DPO should use in order to increase the effectiveness during their awareness initiatives in an organization and why they should use education through persuasion.

The nature of security awareness regarding data protection should be prescriptive, because information security guidelines are a kind of imperative, including, accomplishment-oriented commitment and internalization, for example. To explain this by a practical example, I argue that security people want end-users to internalize and follow given guidelines (prescriptive commitment) rather than to be aware of them; this is when a DPO

33 Paul Lambert, The *Data Protection Officer*, Profession, Rules, and Role (Auerbach Publications, 2016) 125

should enter and explain the IT experts why persuasion is considered to be better than mere application of rules. If a DPO fail to do that or just skip it, then the problem may be that employees will often know the guidelines, but they will fail to apply them correctly. The term ``prescriptive'' refers here to a situation where people see (internalize) a norm or guideline (X) as a matter, which they are bound and obliged to follow. This kind of accomplishment-oriented commitment can be external or internal as a form of motivation. It is possible to achieve moral responsibility if the security actions of any organization are seen as morally acceptable and desirable in the eyes of the employees and it is responsibility of DPOs to persuade the staff about it. In the long run, this obligation should be internal, coming from within the individual. External norms or guidelines, on the other hand, if they are so weighty and obligatory that they lead to prescriptive states, can cause greater risks in the form of negative implications. Successful organizational awareness or education requires more actions than merely the giving of a set of rules (as is often the form of security guidelines). This is the case, since awareness or education, reflecting data protection, which consist of imperatives, has more to do with the internalization of needs than with other issues. One problem with data protection is that only too often they are not justified in a relevant way. This is definitely a problem, for guidelines should always be justified, since they are norms that include imperative forms that need argumentation and justification. In that way people's cognitive states can be changed by giving the reasons for particular guidelines (arguments and justifications), with the result that, they may change their attitude and motivation towards the guidelines in the intended way. This kind of persuasive action, together with active participation, should constitute the basic tasks of a DPO regarding with the training of the staff. When defining a wanted action, we usually give examples and additional information in an attempt to persuade the listeners to accept our evaluation and to adopt the kind of attitude we want them to display. Persuasion through communication (persuasive communication) should be the main target of DPOs[34].

Moreover, awareness through persuasion as a goal has the characteristic that the object may be achieved in different ways. This postulation is based on facts concerning human nature. Given that the behaviour of human nature cannot be formalized nor fully pre-

[34] The impact of information security awareness training of information security behaviour: the case for further research

determined, all (awareness/education) methods are subjectively bounded in respect of situation, the instigator and the target person(s). The use of persuasion in data protection education is recommended. In addition to the occasional use of a reward and sanctions system, there are certain persuasion approaches reflecting motivational factors that data protection education can be used and pursued to ensure that listeners internalize the principles of given guidelines. So what DPOs need to do is try to persuade all the employees of any organization through education, of the importance of the data protection using the following reasoned principles:

- emotions. Emotions are an integral part of thinking and rational decision making. When people are confronted with a set of choices, emotional learning (past experiences), streamlines their decisions by eliminating some options and highlighting others. Consequently, security measures should aim at provoking emotions and appealing to them in order to affect attitudes.

- Morals and ethics. Morals strongly guide human behaviour. It is more intelligible to act for moral reasons than for non-moral ones.
- Well-being. Negligence of security measures and weak security may threaten the well-being of both the individuals and the organization. Therefore, employees should be made aware of such a threat to their wellbeing and how adherence to security guidelines would prevent this from happening[35].
- Feeling of security. Safety needs (the desire to feel safe and secure and free from threats to our existence) rank high among our needs. Although violations in terms of data protection would not endanger people's lives directly (other than in a hospital environment, for example), it is reasonable to assume that people will still want to achieve and maintain a feeling of protection through adherence to security procedures, given that such a need can be pointed out or awakened.

4.4.6 Related audits

The last part of the Article 39(1b) of the Regulation refers to "*related audits*", meaning that the monitoring of compliance includes the audit part from the DPO within an organi-

35 Dieter Gollmann, Computer Security, (Wiley&Sons, 3d edition, 2011), 18-21

zation. It is task of the DPO to carry out audits when they are necessary. Audits can be either internal or external.

Internal audits are carried out by the DPO; in fact it is considered to be best practice a DPO to carry out an internal audit when it starts working for an organization to make a first estimation about it. An internal audit can give the DPO a quick overview of what departments are processing data, what types of personal data are being processed, why the organization needs or does not need to process this data, what other organizations are cooperating with it. The DPO can also take advantage of this audit in order to make an evaluation of the awareness of the staff regarding protection of personal data. The latter is considered, in my view, the most important evaluation that a new DPO could make in order to create his plans to achieve compliance. One extreme example could be an organization that processes various types of personal data and the employees have no clue about the protection of this data while the organization has no security measures at all. In this specific case the DPO could start by explaining the employees of the organization what is considered personal data, raise their awareness about it and cooperate with the necessary departments to establish the necessary measures. In contrast an organization in which the employees have already attended seminars of what is personal data, why they need to protect it and also there are adequate security policies and measures, in this case the task of the DPO is much simpler regarding to the internal audit because most likely the first evaluation relating the data protection will be very good. After the DPO completes the first estimation, a timetable should be created and internal audits should be carried out according to it. This is of paramount importance in order for the organization to check that all the processing which is carried out is in compliance with the Regulation and all new actions have been checked. In this way any organization can maintain its compliance.

The other type of audits that could be carried out within the framework of an organization are the external audits. External audits could be carried out both by another organization and the supervisory authority. In the first case, a third party may be asked to perform a specific audit for the organization or to answer certain questions related to the audit or an aspect of the audit, such as to advise on specific IT-related issues[36].

This could be initiated by a complaint, a data breach or by the type of personal data that the organization processes, for instance children's personal data or personal data re-

[36] Paul Lambert, *The Data Protection Officer, Profession, Rules, and Role* (Auerbach Publications, 2016) 128

lating to criminal convictions. The organization must be prepared for these audits and compliance should have already been achieved in order to avoid being fining. In the case of the external audits it is the DPO that should provide all necessary documentation and help to the supervisory authority.

4.5 Advise and inform when necessary both the controller and the processor for their obligations

Article 39(1a) GDPR indicates the advisory and information-providing part that a DPO should have within the framework of an organization. In addition, the DPO should also advise the employees of the organization.

It is the task of the DPO to inform the organization (controller or processor) for their obligations. The clarifications of what an organization should or should not do regarding the processing of personal data should be given by the DPO and each organization should adapt its action to them. Data breaches, damaged reputation, reduce of trustworthiness and financial losses are some of the consequences that may happen in case the organization does not follow DPO's advice and accordingly fail to comply with the Regulation. In addition, under the new regime fines are huge and penalties could reach millions of Euros. As already clarified, it is responsibility of the organization to achieve compliance with the new Regulation and to be able to demonstrate it; the DPO should advise the organization on how to achieve compliance but he is not responsible for failing can he cannot get fined in case of non - compliance.

The DPO should also advise and inform the employees of the organization regarding the data protection regime. As we mentioned in the previous paragraph 3.4.5 it is among the tasks of the DPO to raise awareness of the staff regarding with the protection of personal data. These separate tasks are actually one task. The DPO by advising and informing the employees of an organization simultaneously raising their awareness about the protection of personal data.

4.6 Risk-based approach

Article 39(2) GDPR requires that the DPO "*have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing*".

The provision requires DPOs to prioritize and focus, primarily, on the higher-risk areas without neglecting lower risks.

4.7 Conclusions

Having seen in detail all explicit tasks of the DPO we can now conclude that each one of them as well as their combination have one target which is the best possible compliance of the organization with the Regulation. The DPO should participate actively in all the aforementioned activities and give his advice but it is the organization that will held liable for not achieving compliance. The DPO could also support any investigative actions by the supervisory authority. Finally, they are the data subjects who benefit from the best possible compliance of the organization because they are their personal data which are more secure.

5 Fifth Chapter

In this chapter we are going to examine the implicit tasks of the DPO[37]. Moreover, we are going to analyse the necessary knowledge that the DPO should have about the obligations of data processor and data controller with regards to security measures required and the audits. Lastly the role of the DPO in connection with the rights of the individuals under the new regime will be presented.

5.1 Record's keeping

Records' keeping is one of the many implicit tasks of a DPO, although it is the obligation of the controller or the processor to keep these records. This is provided by the Article 30(1) and (2) GDPR. It is considered best practice and has already been established under many national laws according to WP2915 that the DPO should keep a record of all processing activities relating to personal data of the organization, based on the information that the organization has provided to him. According to Article 30 of GDPR, this record should contain: prior collection information, purposes of processing, categories of data subjects, categories of personal data, disposal of personal data, transportation of personal data, time-table for erasure of personal data, security measures both technical and organizational.

Nothing can stop either the processor or the controller from assigning these records' keeping task to DPO[38]. The DPO should make the most out of these records in order to be fully aware about everything that relates with personal data and data processing within the framework of the organization. This documentation process boosts organization's effort to comply with the regulation because it adds to the accountability.

[37] Paul Lambert, *The Data Protection Officer, Profession, Rules, and Role* (Auerbach Publications, 2016) 104

[38] Ibid, 168

5.2 Maintain proper and timely involvement in all data protection issues

Article 38(1) GDPR states that "*The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues that relate to the protection of personal data*." The DPO should be involved in everything that contains processing of personal data; if this is a new action then the DPO must check every aspect of this processing in order to comply with the Regulation before the organization adopts it. So, the DPO should be fully aware and should act proactively when this is possible[39]. Another aspect of this Article is that the managers and directors of the organization should value the DPO as an important person of the organization and invite him in every high-level meeting which contains as main or secondary topic of discussion processing operations that may contain personal data. This is important because DPO has an expert knowledge of what is considered personal data and he can ensure the organization if a processing contains this kind of data or not and what measures should be implemented in order for the organization to carry out this processing in order to comply with the GDPR.

5.3 Resources necessary to carry out tasks

Article 38(1) of GDPR states that "*The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge*". As mentioned above, this Article clarifies that is obligation of the controller or the processor to provide resources to the DPO, but it is responsibility of the DPO to use all these resources in order to access every processing operation that contains personal data in order to carry out his tasks[40].

5.4 Ensuring compliance with the obligations of data controller or data processor

The GDPR imposes strict obligation to data processors and data controllers; these obligations may vary depending on the quality and quantity of the data being held or processed.

---

[39] Paul Lambert, *The Data Protection Officer, Profession, Rules, and Role* (Auerbach Publications, 2016) 132-133

[40] lbid, 133

In any case it is task of the DPO to be fully aware of the obligations that the data controller or data processor has in order to be able to guide them in the most effective way. One of the first things that a DPO should do within the framework of the organization is to ask as many information as he needs to determine the amount, context, categories of data being held or processed; then he must assess them and advise the organization about the obligations it has according to the GDPR. Clearly, there will be huge differences relating to the security measures that each organization has to establish; for instance, there is a difference between an organization with 10 employees that keeps only some personal data of its employees and an organization that has 500 employees and processes huge amount of its customers' personal data, it keeps health records of its employees and carries out direct marketing. Although the basic obligations of the two organizations are the same there are huge differences in the sub-categories that each organization has. For example, the security policy of the first will be much simpler than the second.

5.4.1 Security policy

Very few organizations (we refer mostly to management) were aware of the term information security policy, especially these that are not information technology companies. Although the IT sector of the organizations has some knowledge, the available budget for information security was minor. So, one could argue that the GDPR is going to "introduce" the term information security policy to all businesses that use information systems, pretty much to every business.

Information security policy is the document that does not refer only on how to protect our information systems against attacks and viruses; it also contains very useful guidelines on how we should use the assets of information system. The new thing regarding to very famous among IT people, information security policies and unknown to most others, are the personal data. Information security policies, at least the new ones, have special references to how employees, third parties and contractors should use personal data that belongs to an organization in order to keep their integrity, availability and confidentiality. The document of information security policy and the rules and guidelines in it should apply to all departments of the organization and to all employees, suppliers, contractors, and associates who, in the context of their work responsibilities and contractual obligations to the organization, have access to them and the related information and data. Although information security policy is normally being created by IT, either external associates or employees of the organization, the DPO has the responsibility to cooperate

with them in order to be able to protect the personal data stored in the information system in the best possible way. For example, the DPO should explain to the IT personnel that a database with health records, or criminal convictions should have additional safety measures comparing to a database that does not contain sensitive personal data. It is considered as best practice, the DPO to have an active role in the creation of the information security policy.

Having referred to security policies we could not avoid referring to the importance of the ISOs, especially ISO 27001[41]. Established in Geneva, the International Organization for Standardization (ISO) creates and publishes codes of practices and international standards for many sectors, including the information technology sector. Companies that have the certification of ISO 27001, in my opinion, need to change only very few things to comply with the Regulation in the part of information system. ISO contains established and standard procedures and automations within the framework of the organization. In general, I argue that it is a very useful document that each organization that has an information system should have. In addition, as regards cyber threats and cyber security, ISO raises considerably the defence measures of the organizations, making them even more secure[42]. Although it doesn't establish an IDPS[43], it raises the awareness of the employees and simultaneously establishes standard procedures for every possible action relating to information system security.

5.4.2 Information audit

Every organization that needs to comply with the GDPR has to conduct an information audit. This originates from the general rule of the Regulation that every file or data base should have an owner. This procedure may seem easy but for an organization that has thousands of files in its possession and many of them were acquired years ago, it is very hard to locate their origin. It is implicit task of the DPO to conduct an information audit as part of the first general audit in order to collect as many information as possible to be able to cover the aforementioned matter in depth. If the organization's file system is big

[41] https://www.iso.org/isoiec-27001-information-security.html

[42] https://www.iso.org/news/2015/12/Ref2032.html

[43] Intrusion Detection Prevention System: it is considered the best defence mechanism nowadays, since it can detect existing and new types of threats, attacks and virus and it is able to take all necessary safety measure against them.

enough then the DPO should be assisted by the information technology and marketing departments in order to track any information they can about the files the organization owns. Every organization - either a processor or controller - should conduct an information audit. Information audit can be considered as part of the internal audit of the organization.

5.4.3 Additional safeguards

A key principle of the GDPR is that organizations process personal data securely by means of "appropriate technical and organizational measures" – this is the 'security principle'. Every organization - either processor or controller - have to establish appropriate organizational and technical measures in order to be able to protect the personal data stored in the organization (Article 32(1) GDPR). Organization measures will reinforce the physical security of the organization and accordingly the information that is stored in physical form. Technical measures will enhance the information system and accordingly the information stored in electronic form. Every organization has to adapt both its physical and electronic security in order to protect the personal data it holds in the best possible way.

It is the task of the DPO to help the IT department in order for the latter to install all necessary safeguards to protect the information system in the best possible way. The DPO should examine various factors in order to be able to suggest the appropriate technical measures, such as the available budget and the kind of personal data the organization stores in its information system. For example, there is a clear difference between a hospital which treats thousands of patients and keeps their health records and a small company that the only personal data it keeps is the first and last name of their customer and some extra personal data of their employees. That doesn't exclude the latter from installing appropriate technical measures but there is a clear separation between what safeguards should be installed in each case. For example, in my opinion the hospital needs IDPS systems and vulnerability scanner which has an extra annual cost; also the hospital should have an information technology department with information security experts who will be able to deter possible attacks and handle possible system's failure in order to prevent a data breach which may have a huge impact both for the patient and the hospital. The scenario that malicious attackers corrupt a data base which stores patients positive to HIV[44]

[44] Human Immunodeficiency Virus

and get access to the names of these patients is not just vivid imagination. To be able to prevent this kind of attack the DPO should collaborate with the information technology staff and find the best possible counter measures. For instance, they could use double encryption in every data base which stores sensitive personal data; moreover, they could use SHA256 combined with 3AES[45]. Also, the physical access to the server room should be very restricted and only few members of the staff should have a magnetic card or a key; also, there should be a record of who has this card and it should be stored in safely. On the other hand, the small company may only install a good anti – virus software with some extra features such as detect malicious IP addresses, close false TCP ports and impose control in network traffic.

There are many different technical measures that can be implemented in order to enforce both physical and electronic security. Each case is different and the DPO should be able to evaluate the different aspects involved in order to be able to suggest appropriate measures to protect personal data in the best possible way.

5.5 Rights of data subjects

As regards the rights of the data subjects, the new regime has created new data protection rights and in parallel enhances the existing ones. The DPO should have expert knowledge of the rights that the data subjects have, under the GDPR in order to ensure compliance of the organization with the regulation[46]. In the following units we are going to analyse the aspects of the data subjects.

5.5.1 Right to be informed

The data subjects should be informed without charge, in a clear and understandable way about the information (personal data) which relate to them are held or processed by an organization. In general, every data subject has the right to know what personal data about them is processed by an organization. The right to be informed is actually the right to transparency because through that data subjects are fully aware of what data is held by an organization and how it is processed. In order to enforce their rights, the individuals must be given access to the information about the relevant supervisory authority and contact

[45] Advanced Encryption Standard

[46] Paul Lambert, *The Data Protection Officer, Profession, Rules, and Role* (Auerbach Publications, 2016) 139

details of the DPO. It should be stressed once more that the DPO should be easily accessible as a point of contact for employees, individuals and the relevant supervisory authority. The contact details of the DPO are to be published and communicated to the supervisory authority (Article 37 (7) GDPR).

Since consent is an important lawful basis in order to process personal data (Article 6 (1a) GDPR), it is considered the task of the DPO to create a lawful consent form in order to ask permission from the individuals in order for the organization to process their personal data.

5.5.2 Right of access

The right of access is another fundamental right which ensures transparency, because according to it, the data subjects must be able to obtain full access in every information about them and confirm what data about them has been processed by an organization[47]. This latter action ensures the right to transparency because the data subjects are fully aware of what data is held about them and for what purposes is used. The right of access could provide data subjects the following information depending on each case:

- what is the purpose of processing;
- to whom their personal data has been disclosed;
- an estimation of period for which their personal data will be stored by the organization and why do they need the specific period;
- what information about them does an organization holds or processes.

In general, the right of access should be free of charge, but there could be cases that an organization could ask for a small fee, for instance if the request is happening repeatedly. In cases where the personal data of a data subject is transferred to a third-party country or to an international organization, the data subject has the right to ask and learn about the safety measures that the organization had been implemented in order for the transfer to be secure. Another change that the GDPR has brought is the reduction of time period in which the organization must comply with the request of a data subject from 15 days[48] to one month. The organization must be able to answer the request of the data subject within the aforementioned period unless the request is too complicated; in that case the time period could be expanded as long as up to 2 months.

---

[47] Paul Lambert, *The Data Protection Officer, Profession, Rules, and Role* (Auerbach Publications, 2016) 142

[48] Article 12 (4) Greek Law,2472/1997

The right of access is not limited to customers of an organization, the same right has employees of an organization (including retired and fired employees), job applicants that are not employees of the organization, providers and everyone that their personal data is processed by the organization.

It is the responsibility of the DPO to evaluate each case separately and establish the necessary safety measures according to the information that has been contained in the specific data; for instance, the DPO must ascertain that different security measures apply to personal data that contain criminal records/health records and to non-sensitive personal data. The DPO must install a request log in order for him to be able to answer the requests with the most effective way and check who is asking for what information.

5.5.3 Right of rectification

The right of rectification gives the individuals the possibility to enter and check what types of personal information is processed by an organization and to ask for rectification, in case that this information is inaccurate or incomplete[49]. The right of rectification is actually a subsequent of the right of access; cause in order for rectification to take place the individuals must first obtain access to their personal data.

In addition, when a rectification takes place, the specific organization must inform every other organization in which the rectified data has been disclosed about the change. For instance, the controller must inform the processor which carries out processing activities on behalf of the controller about the rectification. In most cases, if not all, the DPO will carry out the communication with the data subjects. For rectification of inaccurate or incomplete personal data relating to a data subject, the DPO is expected to inform other organizations (that the aforementioned personal data has been disclosed) about the change that has taken place in order for the latter also to make the necessary rectifications.

5.5.4 Right to erasure

The right to erasure is presented under article 17(1) of the GDPR, it is also known as the right to be forgotten. The aforementioned right gives to the data subject the power to ask from the controller for erasure of his/her personal data without undue delay, accordingly the controller have the obligation to erase his/her personal data when he/she demand it.

[49] Paul Lambert, *The Data Protection Officer, Profession, Rules, and Role* (Auerbach Publications, 2016) 146

There are certain conditions that need to be fulfilled in order for the data subject to request for an erasure of his/her personal data and accordingly the controller to apply it, as they are referred under article 17 of the GDPR. These are:

- there is no reason for data subject's personal data retention;
- withdrawal of consent by the data subject;
- there is no legal ground for processing and the data subject objects to this processing;
- unlawful processing;
- erasure of data for compliance with the regulation.

If one or more of the aforementioned conditions are met, then the data subject can request the controller for erasure. It is task of the DPO to evaluate if this request is based on legal grounds and if there is, then the controller is obliged to erase the specific data.

On the other hand, even if the data subject makes a request for erasure based on legitimate grounds and one or more of the above conditions are met, Article 17 GDPR provides reasons for a controller to reject such request; for instance, in the sector of public health for matters of public interest, for defence of legal claims, for exercising the basic right of freedom of expression and information or for statistical or scientific purposes.

A DPO should advice the organization to have established automated actions in order to check and erase personal data that is no longer necessary for the purpose of processing. In addition, a well-organized file system will help DPO to handle the requests of individuals and answer to them in the most effective way.

5.5.5 Right to data portability

The GDPR has introduced a quite new right in Article 20, the right to data portability. According to this, the data subjects have the right to request and receive in readable format, personal data relating to them and transfer this data to another controller of their choice, under the conditions that they have prior consent to it and the processing operations of the latter are legitimate[50]. This consent should be pursuant to Article 6(1) or 9(1) GDPR or when the processing is carrying out for contractual agreements pursuant to Article 9(2) GDPR.

When a data subject makes such a request, the controller is obliged to answer to this request without undue delay and without charging any additional fees. In cases the re-

[50] Paul Lambert, *The Data Protection Officer, Profession, Rules, and Role* (Auerbach Publications, 2016) 149

quest is too complicated for a fast response the controller could take an extension of up to two months to answer the request.

There are strict requirements for the IT systems of the organization that stores and process personal data in order to be able to handle these requests. The established systems should store files in a CSV[51] format, since the latter format allows data to be stored in files in a table structured format.

It is another task of the DPO to inform the organization both for the rights to data portability that data subjects have and also to implement a time schedule for effective and fast replies. In addition, the DPO must inform the management and the IT department of the organization about the very specific requirement of CSV format in order for the latter to be able to adapt the systems, if possible, or buy new ones. CSV systems are extremely important for every organization that seeks compliance with the Regulation.

5.5.6 Right to object

The right to object is introduced in Article 21 of the GDPR; according to this data subjects gain the right to object processing regarding their personal data under specific conditions; for instance: for scientific or historical purposes, profiling, statistics, legitimate interest, direct marketing and tasks of public interest[50]. In case there are one or more of the aforementioned situations, the data subject could request from the data processor or data controller to end all processing activities and the latter two are obliged to do so. Any exception for continuing processing must be based on legal grounds which go beyond freedoms and rights or the data subject.

In cases that the processing is made for tasks of public health, for example a lethal spreading virus, then, the data controller and data processor are not obliged to stop processing when the data subject asks for it.

It is the task of the DPO to help the organization in order to create a proper privacy notice or adjust the old one to the changes that the GDPR has brought. In addition, it is the DPO who will normally receive all complaints regarding the right of data subjects to object, asses them and act accordingly. If their requests are based on the specific conditions as they have been mentioned above, the DPO should inform the data processor or data controller to end processing. On the other hand, in any other case in which data con-

[51] CSV (Comma Separated Values) https://www.lifewire.com/csv-file-2622708

troller or data processor are not obliged to end processing for the purposes we have mentioned, then the DPO should inform the data subjects accordingly.

5.5.7 Rights relating to automated decision making and profiling

The rights relating to automated decision making and profiling are provided by GDPR under Article 22 which clarifies that data subjects have the right not to be the subject of any kind of automated decision making, including profiling, when the results of it may legally affect him/her; for instance, the denial of a social benefit granted by law such as child or household benefit. Automated decision making means any decision that has been taken for a human without human's involvement. All the aforementioned shall not applied when automated decision making is:

- necessary for the performance of a contract between the data subject and the data controller;
- the data subject has given his/her explicit consent;
- authorized by member state law or Union law and the data controller has taken all necessary measures of protection.

Profiling means any form of automated processing activity of personal data aiming to evaluate the performance of a person or a people in a specific task. According to the WP29[52] three aspects must be included in a processing activity to be considered as "*profiling*":

- automated processing (processing using machines and algorithms);
- personal data must be processed;
- the aim of processing is to evaluate aspects of personal life about a natural person.

Examples of profiling may include analysis of collected data to gain insights into behavioural characteristics, taken into consideration the credit score of an individual before granting a mortgage.

First of all, the data processor or data controller in cooperation with the DPO or the DPO teams must assess every processing activity that can be considered as automated decision making or profiling within the framework of an organization. The DPO should identify if a legal ground for automated decision making and profiling activities exists and

[52] Guidelines on Automated individual decision-making and Profiling for the purpose of Regulation 2016/679, adopted on 3 October 2017, last Revised and adopted on 6 February 2018

advice management accordingly. In addition, the DPO should create or update the existing privacy notices so as to inform data subjects about profiling activities and their rights to object to them. Another task of the DPO is to establish a process in order for the data controller or data processor to be able to answer individuals' request about profiling or automated decision-making activities.

Lastly the DPO should cooperate with the management of the organization and the IT, in order to establish all necessary safeguards to eliminate any potential risk that maybe emerge because of this processing for the freedoms and rights of data subjects. Finally, after all the steps an organization should be able to address the following matters if it wants to have a lawful basis for carrying out profiling or automated decision making and accordingly compliance with the GDPR.

- The organization should document profiling or automated decision making in data protection policy.
- The organization should be able to explain how people can access details of the information the organization used to create profiles.
- Who provide the organization this kind of information.
- The organization should inform data subjects by sending them a link to its privacy notice when it has obtained their personal data indirectly.
- The organization should have procedures in place in order for the data .subjects to be able to access their profiles and check for accuracy.
- The organization should inform data subjects how to object profiling.
- The organization should have additional safeguards for profiles or automated decision making systems to protect vulnerable groups such as children.
- The organization should carry out DPIA to address potential risks relating with profiling or automated decision making.
- If it is possible the organization should anonymize the data in profiling activities.

5.5.8 Right to restrict processing

Data subjects have the right to restrict processing under Article 18 of the Regulation. According to this, the data subjects have the right to restrict processing in four cases; one of them refers to automated decision making and profiling as we have mentioned in the previous paragraph. The other three cases are:

- when the data that has been collected by the controller is no longer needed for the purposes of processing but the data subject needs this specific data to defend or exercise legal frames;
- when the processing is unlawful and the data subject asks for a restriction of processing but not for total deletion of his/her personal data;
- when the data controller investigates a prior request that has been made by a data subject concerning the accuracy of his/her personal data, for the period that the controller needs to verify the accuracy of the data[53].

The DPO is expected to take care and solve in the most effective way all the aforementioned problems that may arise in a data controller or a data processor.

5.6 Ensuring compliance internally

All the aforementioned rights apply both to customers of an organization as well as to employees. Every employee in each organization can be considered as data subject it-self. Therefore, it is task of the DPO to inform the latter accordingly, in order for the employees to be fully aware of their rights.

The DPO should train the employees of the organization in order for the latter to be able to recognize a data breach and accordingly inform the DPO. The organization should assist the DPO by providing him with all necessary resources in order to be able to establish an effective educational program with seminars and leaflets. If an employee of an organization is able to detect a data breach or a violation of the provisions that the GDPR has introduced, then the DPO may be informed in time and assist the organization to carry out all corrective actions to solve the problem at minimal cost.

5.7 Conclusions

The DPO should be able to carry out his implicit tasks effectively. He should be fully aware of the basic rights of the data subjects that apply both on customers and on employees of an organization and in addition he should advice the management accordingly so as to adjust all operations of an organization to them. It is task of the DPO to recommend all necessary measures to ensure the best possible compliance.

---

[53] Paul Lambert, *The Data Protection Officer, Profession, Rules, and Role* (Auerbach Publications, 2016) 151

Moreover, the DPO should play an active role in the creation of security policy and discuss with the IT department in order for them to establish all necessary measures to protect the personal data that are stored and processed in the organization. Audits are of immense importance for the organization's compliance with the GDPR and it is among the tasks of the DPO to establish a time schedule for their prosecution.

6 Conclusions

In the final chapter, which will also serve as the concluding part of the thesis, the responsibility of the DPO in cases of non-compliance will be addressed. Moreover, the advantages the GDPR has brought concerning the protection of personal data will be addressed.

6.1 Responsibility of DPO in case of non-compliance

The DPOs will play a very crucial role in the organizations in which they will be appointed. Accordingly, I argue that they are the "key" for the organizations that seek compliance. As analysed in many parts of this thesis, it is the DPOs' responsibility to advice organizations about all the necessary measures that need to be established in order for the latter to comply with the GDPR[54]. However, since he/she does not have any managerial decision-making abilities but an advisory role[55], in cases of non – compliance, the DPO has no personal responsibility[56]. Compliance is the responsibility of the controller or the processor (Article 24(1) GDPR) and they are the ones that will be considered liable before the Supervisory Authority for not achieving compliance and be fined accordingly. Nevertheless, the DPO is generally responsible for fulfilling its tasks properly[57].

6.2 Increased confidence

It goes without saying that following the scope of GDPR, the new legal regime is expected to cultivate confidence. Every individual that can be considered as data subject, customers or consumers, employees, third parties and external associates of an organization will feel safer. As time passes and more organizations comply with the GDPR, data

---

[54] Guidelines on *Data Protection Officers* ('DPOs'), Adopted on 13 December 2016, As last revised and Adopted on 5 April 2017, 24

[55] Centre for Information Policy Leadership, Ensuring the Effectiveness and Strategic Role of the *Data Protection Officer* under the General Data Protection Regulation, CIPL GDPR Interpretation and Implementation Project, November 2016, 21

[56] Ibid, 4, 24-25

[57] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR),* (Springer 2017) 62

subjects will have greater confidence regarding their personal data processed by organizations. In addition, in cases of data breach or violations of provisions that GDPR has established; data subjects will always have a person (DPO) to contact and ask details about what happened and what actions the organization carries out to fix it.

6.3 Direct and better communication

DPOs will be the contact points with supervisory authority in cases of audit or data breach. This direct communication will help both of them (the organization and the supervisory authority) to address the problem effectively reducing the possible consequences for the data subject to the minimum. Obviously, DPOs will play a key role to the aforementioned communication.

6.4 Better security

Organizations that will appoint a DPO will increase their security. The role of the DPO is: to inform and advise both the controller and the processor, to help organizations comply with the new Regulation, to monitor compliance, to enhance security in order to avoid data breaches. It is obvious that each organization that will appoint a DPO will inextricably increase its security.

6.5 Last word

Considering the recent scandal about the selling of personal data by Facebook[58] that overwhelmed the media and the public worldwide, many individuals have lost their faith in big companies, meaning that they do not know who is collecting what and how they use it regarding their personal data. The new Regime aims at mitigating this mistrust; and the DPO will play an important role in order for the organizations to gain the trust of the data subjects again. After all, personal data belong to data subjects, privacy is a fundamental right and nobody should process them without a legitimate ground.

[58] https://www.bbc.com/news/technology-44793247

Bibliography

1. Centre for Information Policy Leadership, Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation, CIPL GDPR Interpretation and Implementation Project, 2016
2. European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, 2018
3. Gollmann, Dieter, Computer Security, Third edition, Wiley & Sons 2011
4. Lambert, Paul, The Data Protection Officer, Profession, Rules and Role, Auerbach Publications, 2016
5. Recio, Miguel, Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability by Eur. Data Prot. L. Rev. 114 (2017), 114-118
6. Sotiropoulos, Vasileios, The DPO, A Toolbar for the new institution in public and private sector, Sakkoulas Publications, 2017 (in Greek)
7. Voigt, Paul and von dem Bussche, Axel The EU General Data Protection Regulation (GDPR), Springer 2017
8. Wright, David and De Hert, Paul (eds.),Privacy Impact Assessment, Springer 2012

Legislation – guidelines

1. 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).
2. European Treaty Series –No. 108, Strasbourg, 28.1.1981 Council of Europe, Convention for the Protection of Individuals with regard to automatic processing of personal data.
3. Council of Europe, Committee of Ministers, Recommendation No R.(87)15, 17.9.1987.
4. Chapter of fundamental rights of the European Union, OJ 364/1, 18.12.2000.
5. 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 [1995], OJ L 281/31.

6. Directive 2000/31/EC of the European Parliament and of the Council, 8.6.2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market (Directive on electronic commerce), OJ L 178.
7. Treaty of Functioning of the European Union TFEU, OJ C 326/47, 26.10.2012.
8. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L 8/1.
9. Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, 28 November 2005 , Brussels.
10. Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001, 14 October 2010.
11. Article 29 Working Party (2017), Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, last revised and adopted on 5 April 2017. The Article 29 Working Party was an advisory body made up of representative from data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. On 25 May 2018, it has been replaced by the European Data Protection Board (EDPB) under the GDPR.
12. Professional Standards for Data Protection Officers the EU institutions and bodies working under Regulation (EC) 45/2001, Finalized at the meeting of DPO network on 14 October 2010, Network of Data Protection Officers of the EU institutions and bodies.
13. Article 29 Working Party (2017), Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, last revised and adopted 5 April 2017, 17.
14. Guidelines on Automated individual decision-making and Profiling for the purpose of Regulation 2016/679, adopted on 3 October 2017, last Revised and adopted on 6 February 2018.

Cases

Case-92/09 Volker und Markus Schecke and Eifert (CJEU, 9 November 2010) ECL:EU:C:2010:662

Reference links

https://www.synectics-solutions.com/Contact/News/entryid/91/gdpr-data-protection-act-what-does-it-mean-for-business (*last visit: 22.08.2018*)

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling (*last visit: 25.09.2018*)

http://www.kemplittle.com/site/articles/kl_bytes/a-guide-to-gdpr-profiling-and-automated-decisionmaking (*last visit: 25.09.2018*)

http://www.dpa.gr (*last visit: 30.10.2018*)

https://www.iso.org/standard/66435.html (*last visit: 02.10.2018*)

https://www.iso.org/isoiec-27001-information-security.html (*last visit: 02.10.2018*)

https://www.iso.org/standard/54533.html (*last visit: 02.10.2018*)

https://www.iso.org/obp/ui/#iso:std:iso-iec:27017:ed-1:v1:en (*last visit: 02.10.2018*)

https://www.iso.org/news/2015/12/Ref2032.html (*last visit: 02.10.2018*)

https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412 (*last visit 05.10.2018*)

https://www.bbc.com/news/technology-44793247 (*last visit: 02.10.2018*)

Abbreviations

1. GDPR – General Data Protection Regulation
2. DPD – Data Protection Directive
3. EU – European Union
4. TFEU - Treaty on the Functioning of the European Union
5. DPO – Data Protection Officer
6. FDPA - German Federal Data Protection
7. CJEU - Court of Justice of the European Union
8. EDPS - European Data Protection Supervisor
9. WP29 – Article 29 Working Party
10. ISP - Internet Service Provider
11. ENISA - European Union Agency for Network and Information Security
12. US – United States
13. HR – Human Resources

14. IT- Information Technology
15. CCTV – Closed-Circuit Television
16. DPIA - Data Protection Impact Assessment
17. DPA – Data Protection Act
18. ISO - International Organization for Standardization
19. IDPS – Intrusion Detection Prevention System
20. HIV – human immunodeficiency virus
21. AES – Advanced Encryption Standard
22. CSV – Comma Separated Values