Iva Katić [*]

Data Protection Officer as Preventive Mechanism of Infringements with Regard to the Tasks Prescribed by the General Data Protection Regulation

The demands made by the data protection officer, for most of the work collective, is additional burden, which makes work of data protection officer extremely lonesome. The essence of this position is to pay attention within the organization that there is no infringement of the Data Protection Law, which makes this position extremely responsible. Precisely in regard to above mentioned it may be said that the data protection officers may, by reason of the nature of their tasks, act preventively on the entire organization in relation to an infringement, and consequently on respect for one of the fundamental human rights, especially right to personal data protection.

Keywords: *Data protection officer, Personal data protection, Prevention of infringements.*

1. Introduction

Personal data is all around as. Even if an information at glance doesn't seem to be qualified as personal data, companies should think twice.

Name, date of birth, home address, e-mail address, IP address, ID number, health data such as dioptric of an individual, fingerprint, car registration number, photo and many other data are personal data.

In accordance with European law, Article 8. Under the EU Charter of Fundamental Rights, the protection of personal data is recognized as a separate fundamental human right.

Until the entry into force of the 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; hereinafter GDPR), the main EU legal instrument on the protection of personal data was the Personal Data Protection Directive[1].

However, due to the expansion of modern technologies, there was a need to reform legislation so that the legal framework could relatively effectively monitor personal data processing in the modern and digital age.

In this regard, the GDPR entered into force as a technologically neutral regulation that has become a pioneer in the protection of personal data on a global scale and a well-known role model.

[*] Secretary of the Cabinet Office at Croatian Data Protection Authority.

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

More than five years ago, GDPR has sparked a lot of public interest and has forced many subjects to make an X-ray in their organizations.

To comply with the data protection law controller must have the ability to carry out all the tasks prescribed by the law.

In recent years, it has become evident how valuable a data protection officer is for the organization.

It is highly recommended to appoint data protection officer within organization. The data protection officer can have a strong preventive effect on the organization in which they operate.

Appointment of the proper data protection officer may reduce the possibility of a personal data breach and infringements.

2. Preventive Impact of the Data Protection Officer Role within Organization

Let's imagine a complaint by the data subject complaining that the company has posted the personal data of data subject on the company's website.

Published data contained data subject's vehicle identification number (chassis number), general data about the motor vehicle and data on the damage under specific number.

At first glance, the average individual would say that published data was not personal data. However, by entering the chassis number on several websites person may receive feedback on the vehicle such as engine marking, color code or date of production and more.

In the beginning person cannot know too much about the owner of the motor vehicle, but having a chassis number enables to find out even exact identity of the vehicle owner.

Let's imagine that company didn't appoint data protection officer and claims that chassis number is not a personal data.

How will this company comply with transparency obligation set out in the Data Protection Law?

In this regard, within the company someone should have had identified the chassis number as personal data and should have had determined the legal basis for the processing and met transparency obligation by including information about legal basis for processing in the privacy notice.

According to the GDPR, data subject is an identified or identifiable natural person, directly or indirectly. Identifiers such as certain factors related to the physical, physiological, genetic, mental, economic, cultural or social identity of an individual contribute to identification[2].

Identity of the driver of the vehicle can be subsequently established by additional information, indirectly, by one or more factors specific to the specific person, location data, etc., therefore the chassis number of the vehicle should be considered as personal data.

Data protection officer (if appointed or had been adequately appointed) would have recognized the link to identity behind the "chassis number" and would have been familiar with the definition of the personal data. After identification of the personal data, the data protection officer would identify the legal basis for the processing prior to publication on the

[2] Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ec (General Data Protection Regulation), Article 4. Paragraph 1.

website, and then, in accordance with the principle of data minimization[3], would advise to publish the personal data only if it were necessary and inform the data subjects about such processing.

Data protection officer is an employee or external expert who has the high professional ethics and knowledge about Data Protection Law.

Such a person, must be aware of the obligations imposed by the Data Protection Law, must continuously monitor decisions taken by the supervisory authorities within the European Economic Area as well as the judgments of the Court of Justice of the European Union, recommendations and opinions of the supervisory authorities, as well as the European Data Protection Board guidelines.

Data Protection Officer is a type of inspection within an organization. For this reason, it is very important to have internal knowledge of the structure of the organization. Processes carried out by organizations, as well as the means of processing must be familiar to data protection officer.

An individual who is considered as an inspection within an organization should be of a certain type of personality. Not every person, however skilled, can communicate successfully with authority. Indeed, data protection officer has to oppose ideas that are in conflict with Data Protection Law. Also, not every person can address criticism to their colleagues and demand that the provisions of the regulations on the protection of personal data be complied with.

A major problem in practice is appointment of an inadequate person. When appointment is purely formal, organization cannot benefit.

2.1. Advisory Task Impact on the Prevention of Infringements

The data protection officer should have an advisory role. Whenever a new procedure or technology is to be introduced in an organization, data protection officer must be involved in the project in order to be able to act preventively on mechanisms that would risk personal data breaches or infringements.

Early involvement in the project is crucial. When developing new technologies into processes, a good expert will take into account data protection by design and default[4] and thus integrate some of the safely measures such as possibility of deleting the data after the retention period(s) has ended, ensure that access to personal data is restricted only to certain personnel who need to perform a specific task with personal data and only to a specific set of personal data they need to know, to ensure that the data cannot be read, copied, modified or removed without authorization (e.g. need-to-know basis), ensure that access to data can only be possible after authorized personnel have been successfully identified and authenticated etc.

GDPR is a risk-based regulation. The DPO should constantly assess the risks in order to be able to identify processing within the organization which may be problematic from the data protection aspect. For example, if a company's personal data is systematically and extensively profiled or new technological solutions are used in the processing of personal data, such as the application of the "Internet of Things", or personal data are being processed

[3]Ibid, Article 5. Paragraph 1.
[4] Ibid, Article 25. Paragraph 1.

by linking, comparing or checking matches from multiple sources, the data protection officer must light a red flag.

Data protection officers are not a burden for the company. They are not designated to forbid personal data processing. They serve to ensure that the processing of personal data is GDPR compliant. Data protection officer is here to look for a solution that will meet the demands of the employer as well as the requirements of the GDPR. DPO is a kind of a mediator.

However, if company doesn't see that it will be beneficial for them to seek an advice from the data protection officer and include them in project which include data processing it should bear in mind it could be investigated for not doing so.

Belgian DPA[5] investigated regional government agency for tourism which resulted in reprimands for not proactively including data protection officer in processing task prescribed by the Law which consequently led to a breach of Article 38 (1) GDPR and Article 39 (1) GDPR.

2.2. Monitoring Compliance with the Provisions of the Laws as Mechanism for Prevention of Infringements

The data protection officer is authorized to conduct audits. They can be initiated either on the basis of an external signal, for example, an individual submits a complaint to the company and data protection officer investigates the circumstances of the complaint or may be an internal signal based on a complaint or notice from a trade union commissioner, labor council, whistle-blower, but also any employee.

Company must provide the data protection officer with all the resources and relevant access to carry out the audits. Also, the company should inform its employees of the data protection officer's authority to conduct investigations (it would be good to give explicit guidance through the company's internal rules). A similar notice should also be made known to external service providers, suppliers, members of the supervisory board and all others who come into contact with personal data in the company.

Regular auditing can certainly detect (in time) certain problems in the processing of personal data and prevent a personal data breach.

2.3. Awareness-raising and Training of Staff Involved in Processing Operations

Most of the personal data breaches stem from an error by an employee of the controller, of course error can happen, however, it can also be prevented by proper education of employees.

Company in Norway[6] mistakenly conducted a credit check on one of the owners of another company which resulted in fine of 200,000 NOK. Infringement was caused by lack of familiarity with the system they used for requesting credit reports.

Case happened in Cyprus[7] where a typing mistake occurred with passport number in during the process of updating client's data in Hellenic Bank. After a while other individual

[5] APD/GBA (Belgium) - 162/2022 - GDPRhub [30.09.2023].
[6] Datatilsynet (Norway) - 20/04401 - GDPRhub [30.09.2023].
[7] Commissioner - 12.10.001.011.001 - GDPRhub [30.09.2023].

verified information, and his new passport had the number that the bank employee had mistakenly typed as previous client's passport number, hence other client has partial access through the web banking platform to other person's personal and financial data. This case didn't result with imposing a fine but it was demanded that the controller take some appropriate measures.

The Information Commission Office[8] reprimanded Ministry of Justice for confidentiality breach. Several people had access to confidential waste documents after they were left in prison holding area.

The Polish DPA[9] fined district court with 6,387 euros because an employee lost three USB sticks contain draft ruling and personal data of an unidentified number of individuals.

In this regard it is important to emphasis that one of the obligations arising from the General Data Protection Regulation[10] is to take appropriate organizational protection measures, which, among other things, include raising awareness within the organization.

Such an obligation of the controller is linked to the tasks of the personal data protection officer, whose task is to raise awareness among employees and train staff in order to prevent data breach.

There are numerous of examples in practice where the data protection officer would have a preventive effect on a personal data infringement only if awareness-raising activities on the importance of personal data protection were carried out within the organization.

When it comes to employee error, the intention to breach personal data is infrequent. As a rule, employees are not aware of the risks arising and their mistakes. They are also unaware of this incident, which they have to report in order to have a rightful influence on the impact that the infringement will have on the data subject.

2.4. Providing Advice in the Data Protection Impact Assessment Process

According to the GDPR[11] where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

Such an obligation of the controller is linked to the tasks of the personal data protection officer; whose task is to provide advice requested as regards the data protection impact assessment.

A data protection impact assessment serves to identify a high risk to the rights and freedoms of individuals when processing personal data.

[8] ICO (UK) - Ministry of Justice (1) - GDPRhub [30.09.2023].

[9] UODO (Poland) - DKN.5131.12.2020 - GDPRhub [30.09.2023].

[10] 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), Article 32. Paragraph 1.

[11] 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), Article 35. Paragraph 1.

Some of the factors/examples[12] that may involve high risk are: a financial institution that verifies its clients through the Anti-Money Laundering (AML) or fraud database, a biotechnology company offering genetic tests directly to consumers to assess and predict risks for the development of diseases/health risks, a company that produces behavioral or marketing profiles based on the use or navigation of their websites, General Hospital that keeps patient records, a private investigator who keeps details of criminal convictions or offences, extensive collection of genealogical information about the families of persons belonging to a particular to a religious group, the processing of data generated by the use of the so-called "Internet of Things" applications if the use of data has (or may have) a significant impact on the daily life and privacy of individuals.

The risk under assessment relates not only to the risks related to the right to the protection of personal data, but also to other rights and fundamental freedoms such as the right to private and family life, the right to freedom of expression and information, etc.

Therefore, for example, if a company wants to track the location of an employee's vehicle, there is a risk of processing personal data on the location of an employee at a time other than official opening hours, as it may affect their private and family life.

When a high risk is identified, it is necessary to assess whether it can be mitigated by applying appropriate technical and organizational protection measures. If the risk cannot be reduced, it is advisable to waive the processing of personal data.

In this process, the personal data protection officer plays a key role, depending on the advice, a personal data breach or infringement may be successfully (or unsuccessfully) prevented.

In the case of high risks which cannot be reduced by technical and organizational measures to 'eligible risk', the obligation referred to in Article 36 of the GDPR shall follow, which is a prior consultation of the supervisory authority.

2.5. Cooperation with the Supervisory Authority

The data protection officer shall cooperate with the supervisory authority. Cooperation may be initiated on its own initiative or at the initiative of the supervisory authority.

The data protection officer's relationship with the supervisory authority may affect compliance with personal data protection regulations.

3. Conclusion

The appointment of a data protection officer within an organization may act as a preventive mechanism for infringements of data protection rules, which sources from the nature of its tasks. Among other tasks, data protection officer must advise controllers and employees who are carrying out data processing, must encourage a culture of respecting the right to personal data protection within organization and must monitor the compliance with data protection regulations. Their appointment, enabling the performance of their tasks in a timely manner, taking into account their advices may ensure that personal data law is not violated. The link between data protection officer and preventive mechanism with regard to infringements of the law are related their risk-based actions in general which (provided that

[12] <https://azop.hr/wp-content/uploads/2023/09/DPO-prirucnik.pdf>, (173-178).

the data protection officer is an adequate person) is always two steps in ahead thinking how to improve compliance with the law and how to mitigate risks and balance business activities with request to protect personal data protection right.

Bibliography:

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
2. Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
3. <https://gdprhub.eu/index.php?title=APD/GBA_(Belgium)_-_162/2022> [30.09.2023].
4. <https://gdprhub.eu/index.php?title=Datatilsynet_(Norway)_-_20/04401> [30.09.2023].
5. <https://gdprhub.eu/index.php?title=Commissioner_(Cyprus)_-_12.10.001.011.001> [30.09.2023].
6. <https://gdprhub.eu/index.php?title=ICO_(UK)_-_Ministry_of_Justice_(1)> [30.09.2023].
7. <https://gdprhub.eu/index.php?title=UODO_(Poland)_-_DKN.5131.12.2020> [30.09.2023].
8. <https://azop.hr/wp-content/uploads/2023/09/DPO-prirucnik.pdf> [30.09.2023].