SECURITY OF GEOGRAPHICAL INFORMATION SYSTEMS – HOW TO ENSURE THEIR CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE?

Kamil Czaplicki, Ph.D.
Law and Administration Faculty
University Cardinal Stefan Wyszynski in Warsaw
Warsaw, Poland
e-mail: k.czaplicki@uksw.edu.pl

Abstract

The article describes basic obligations of personal data controllers in connection with ensuring confidentiality, integrity, availability and resilience of IT systems. Those obligations stem from 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 which has been in effect since 25 May 2018.

Key words: GDPR, confidentiality, integrity, availability, resilience, IT Systems, identification

Introduction

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, commonly known as GDPR or the General Data Protection Regulation, took effect in the European Union on 25 May 2018.

Together with additional legal acts (including the new Act on the protection of personal data of 10 May 2018), the GDPR will replace previously existing regulations in the area of personal data protection. The currently adopted personal data protection model is expected to be a response to dynamically developing technological progress as well as increased demand for global processes of personal data processing. Technological progress as well as globalization have brought new challenges in area of personal data protection. Public entities as well as private individuals now process personal data to a much greater extent than before. Due to the development of the Internet, in particular social media, natural persons share their personal data more and more often. Previously existing legal regulations seemed not to be able to catch up with the changing World and new global challenges.

GDPR goals include departure from a rigid personal data protection framework and its replacement with a liberal approach based on the risk of infringement of the rights of data subjects. The very name of the regulation, i.e. "on the protection of natural persons with regard to the processing of personal data..." is suggestive as it replaces previous expression "on the protection of personal data". The change reflects the new approach of European legislative bodies which assumed that protection of data subjects is the core value and "physical" protection of personal data will be one of the consequences of that protection.

The changes which took effect on 25 May 2018 can be seen in the areas such as: rights of data subjects, obligations of personal data controllers and other entities which are involved in personal data processing (e.g. processors), personal data security, procedural changes connected with a new body, i.e. President of the Personal Data Protection Office, or sanctions for violation of GDPR regulations.

The definition of personal data has not been significantly changed in comparison with the previous regulation. According to Article 4 point 1, 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

According to Article 2 item 1 of the Regulation, it applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

From the point of view of this article, one should ask the question whether data processed in widely understood geographical information systems is personal data and whether the General Data Protection Regulation applies to it.

A geographical information system is a system for acquiring, collecting, verifying, integrating, analyzing, transferring and disclosing spatial data, within a wide meaning it includes methods, technical measures, including hardware and software, spatial database, organization, financial resources and people interested in its functioning" (GAŹDZICKI). Spatial data is collected and processed in those systems. Due to the wide definition of personal data which includes all information concerning identified or identifiable natural persons, it must be assumed that at least some of the data processed in spatial information systems needs to be considered personal data. By way of example, one could argue that address data is included in personal data in reference sources (BARTA, 2015; DROZD, 2014), while in its judgment of 17 November 2000 (judgment of 17 November 2000, II SA 1860/00), the Supreme Court of Administration pointed out to geographical (address) data as data which makes it possible to identify a person's identity. Data from e.g. GPS transmitters which is managed by an individually-assigned person must also be considered personal data. Personal data is also data which directly concerns natural persons, including without limitation, data on buildings if we can assign it to an identified or identifiable natural person.

Principle of integrity and confidentiality

The GDPR introduced the principle of integrity and confidentiality which had not been known in the previously existing personal data protection act. Pursuant to that general principle, personal data needs to be processed in a way ensuring proper personal data security, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage by means of appropriate technical and organizational measures. The principle is made more specific in Article 32 of the GDPR which obliges both data controllers as well as data processors to ensure a level of security of data processing, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The proper level of security must be ensured through implementation of adequate technical, organizational and procedural measures.

According to Article 32 item 1 letter b), a personal data controller and processor have to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. The duty has been imposed on each of the aforementioned entities and cannot be transferred by them onto another entity.

The notions quoted in the above article, i.e. confidentially, integrity, availability and resilience are not defined in the GDPR, however due to the fact that they refer to processing systems and services, not to personal data itself, the notions need to be understood in the way which was traditionally adopted in sciences devoted to the security of IT systems. Confidentiality means making sure that information is only available to authorized people, integrity is ensuring accuracy and completeness of information and processing methods, availability is making sure that authorized people have access to information and related assets when necessary while resilience is systems' capacity to function correctly despite significant overload (KACZMAREK, 2009).

Contrary to the previously applicable act on the protection of personal data, the GDPR is based on the evaluation of risk of varying likelihood and severity of infringement of the rights and freedoms of natural persons and on the proportionality principle, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing. That means that not all data controllers and processors need to apply the same system protection methods but they do need to choose methods which are adequate to their own case on the basis of, inter alia, a risk analysis. Thus, the legislators departed from the rigid framework which specified obligations in ensuring personal data security in favor of flexible methods based on the evaluation by the controller and the processor themselves who are expected to independently specify the level and methods of security applied through the prism of risk (BIELAK JOMAA et al., 2017). This means that different protection measures for confidentiality, availability, integrity or resilience will be implemented in big international medical corporations and in small companies.

Confidentiality of an IT system can be ensured by correct identification of the people authorized to access it. Among many access control methods (CZAPLICKI, 2016), the GDPR sets a legal basis for a wider use of biometric identification (CZAPLICKI, 2016) in controlling access to systems. Pursuant to Article 4 point 2 § 2 of the bill on amending some acts in connection with ensuring implementation of Regulation 2016/679 (bill version of 23 March 2018), processing of an employee's biometric data is admissible also when provision of such data is necessary for the purposes of controlling access to particularly important information whose disclosure might expose the employer to a loss or access to premises which require special protection. Therefore, it seems possible that biometrical information might be used at a wider scale in employee identification. Biometric identification enables effective and at the same time safe

methods of controlling access to key data processing systems. Introduction of the GDPR and the implementing act should contribute to popularization of this method and thus replacement of less secure methods, i.e. those based on passwords.

System integrity can be ensured by implementing proper methods of protection against attacks from the outside. Antiviral software seems sufficient in small systems but intelligent firewalls (e.g. in email) are necessary in bigger ones.

Ensuring availability of the system, i.e. making sure that it can be used whenever it is needed, is a big challenge to the data controller. Availability can be breached on many planes - from power failures to internet provider's equipment malfunctions. There are many methods of preventing loss of systemic availability - the most frequent ones include making backup copies, systemic backup, duplicated power supply or hardware backup.

Ensuring system resilience, i.e. making sure that it can function despite significant overload, is also a challenge. At the moment, fighting against DDOS attacks is difficult. Examples of attacks on Polish IT systems from 2012 show that even the biggest and the best services (e.g. Premier.gov.pl, ABW.gov.pl) suffered from short-term resilience failures. Available are IT methods which improve resilience to such attacks, using e.g. excessive disk matrix. However, it seems that in the case of small GIS systems, application of such solutions will be ineffective both from the organizational as well as financial point of view. It is worth pointing out that system resilience is not a classic objective of IT infrastructure security (BIELAK JOMMA et al., 2017).

Personal data breach

The process of implementing mechanisms ensuring confidentiality, integrity, availability and resilience of IT systems is a continuous one. Due to technological development, once introduced mechanisms might not be sufficient later on. When inadequate protection measures are introduced or none are implemented, data security might be breached. According to Article 4 point of the GDPR, 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

In the case of a personal data breach, the controller must undertake proper remedial actions and, in accordance with Article 33, shall notify the personal data breach which results in a risk to the rights and freedoms of data subjects to the President of the Personal Data Protection Office. The notification shall be made without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. The notification must describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned, describe the likely consequences of the personal data breach; describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. In the case of breaches which do not result in risks to the rights and freedoms of natural persons, such breaches must be recorded in a dedicated breach register.

Summary

The introduction of the GDPR forces data controllers and processors to implement proper mechanisms for securing personal data as well as IT systems in which this data is processed. In the case of GIS systems, some data which is processed in them meets the personal data criterion, and thus must be processed in accordance with the GDPR. Security measures applied by controllers need to ensure data confidentiality, integrity, availability and resilience adequate to the risk to the rights or freedoms of data subjects. Adequacy means that not ever controller will use the same rigid security mechanisms and their type and form will depend on the risk analysis carried out by system administrators.

References

BARTA, J., FAJGIELSKI, P., MARKIEWICZ, R. 2015. *Ochrona Danych Osobowych. Komentarz LEX*. 6th edition, Warsaw. Online access: www.lex.uksw.edu.pl.

BIELAK JOMMA, E. (ed.), LUBASZ, D. (ed.), CHOMICZEWSKI, W., CZERNIAWSKI, M., DROBEK, P., GÓRAL, U., KUBA, M., ŁUCZAK, J., MAKOWSKI, P., WITKOWSKA-NOWAKOWSKA, K., ZAWADZKA, N. 2017. *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz.* Wolter Kluwer. Online access: www.lex.uksw.edu.pl.

CZAPLICKI, K. 2016. *Identyfication in cyberspace*. In Geographic Information Systems Conference and Exbibition „GIS ODYSSEY 2016". Conference proceeding, p. 85- 89.

CZAPLICKI, K. 2016. *Dokumenty tożsamości, jawność i bezpieczeństwo*. C.H. Beck, Warsaw, p. 306-309.

DROZD, A., 2004. Ustawa o ochronie danych osobowych. Komentarz, Wzory pism i przepisów. LexisNexis. Onlone access: www.lex.uksw.edu.pl.

GAŹDZICKI, J. *Internetowy leksykon geomatyczny Polskiego Towarzystwa Informacji Przestrzennej (PTIP)*.

KACZMAREK, A. 2009. *Bezpieczeństwo przetwarzania danych osobowych – obowiązki administratora danych osobowych*. GIODO.