**SECURITY DIMENSIONS**
NO. 34; 2020 (256–267)
DOI 10.5604/01.3001.0014.5614

# The Analysis of Risks to Personal Data Security

Sylwia Kosznik-Biernacka*

## ABSTRACT

Article 32 of the EU General Data Protection Regulation imposes the obligation to implement appropriate safeguards to protect personal data. It states that the application of adequate measures is to be preceded by a risk analysis and evaluation. In the current paper, as the main risk factors, probability and consequences were assumed that take into account the basic attributes of information, i.e. confidentiality, integrity and availability. Next, a risk analysis methodology based on the risk matrix is proposed. The issue discussed in the publication is currently valid and still requires careful analysis in order to develop universal standards aimed at establishing certification mechanisms as well as quality labels and markings in terms of personal data protection.

* Sylwia Kosznik-Biernacka, Ph.D., Pomeranian University in Slupsk, Słupsk, Poland; correspondence address: Arciszewskiego 22a, 76-200 Słupsk, Poland; email: sylwia.kosznik-biernacka@apsl.edu.pl

ARTICLE INFO

*Article history*
Received: 8.09.2020 Accepted: 27.11.2020

*Keywords*
risk, personal data, GDPR

## 1. Introduction

Providing information security, and, within it, ensuring the security of personal data, is one of the most important areas of activity of entities, as well as areas of social impact, in civilizationally and technologically developed countries.[1] The security of personal data is one of the important elements of information security, which, in turn, is one of the elements of national security.[2] The right to privacy is ensured in the Constitution of the Republic of Poland[3] and is an important component of personal security, since its violation may lead to, e.g. violation of a citizen's personal rights.

This paper introduces the principles of estimating the risk of personal data security. The currently applicable provisions in this matter in Poland result 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 the Polish *Act of 10 May 2018 on the protection of personal data*.

The topic is currently valid and worth being taken up, because along with the implementation of the General Data Protection Regulation (GDPR), the previous *Regulation of the Minister of the Interior and Administration of 29 April 2004 on the documentation of the personal data processing and technological and organizational conditions which shall be met by devices and IT systems used for the personal data processing* was repealed. This act contained

[1] M. Byczkowski, J. Zawiła-Niedźwiecki, *Analiza ryzyka w zarządzaniu bezpieczeństwem danych osobowych. Zarządzanie ryzykiem w kontekście ochrony informacji*, "Monitor Prawniczy", 2014, no. 9, special supplement: *Aktualne problemy prawnej ochrony danych osobowych*, p. 46.

[2] P. Budzyń, *Ochrona informacji niejawnych w świetle krajowych aktów prawnych*, "Bezpieczeństwo. Teoria i Praktyka", 2015, no. 3 (XX), pp. 13–26.

[3] *The Constitution of the Republic of Poland of 2 April 1997*, Journal of Law No. 78, item 483, as amended: "Everyone has the right to legal protection of private and family life, honor and good name, and to decide about their personal lives".

very detailed instructions regarding e.g. the desired length of passwords for personal data processing systems. However, in the era of very dynamic IT development, it was necessary to implement slightly more general solutions so that the legal act itself does not devalue as a result of the appearance of new technological solutions, and, thus, new, more sophisticated threats. The GDPR recommends the use of adequate and appropriate measures not specified by law, but effectively protecting personal data.[4]

The GDPR is to ensure consistent and uniform application throughout the European Union of the provisions on the protection of fundamental rights and freedoms of natural persons in relation to the processing of personal data. It regulates the rights to the protection of personal data to a much broader extent than was previously established, giving more rights to data subjects.

## 2. Legislation

Article 4 of GDPR, provides basic definitions of :

- *personal data* mean 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 by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person;
- *filing system* means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized, or dispersed on a functional or geographical basis;
- *processing* means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Article 9 of the GDPR defines *special categories of personal data* as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; as well as genetic data, biometric data processed for the purpose of uniquely identifying a natural

[4] M. Aptekarz, *RODO Moduł S11 – ECDL Standard*, Katowice 2018, p. 19.

person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Article 5 of the GDPR presents the following principles regarding the processing of personal data.

1. Personal data must be:

a) processed in accordance with the law, fairly and transparently for the data subject (**lawfulness**, **fairness** and **transparency**);

b) collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (**purpose limitation**);

c) adequate, relevant and limited to what is necessary for the purposes for which they are processed (**data minimization**);

d) correct and updated as necessary; all reasonable steps must be taken to ensure that personal data that is incorrect in light of the purposes of its processing is promptly deleted or corrected (**accuracy**);

e) stored in a form that allows identification of the data subject for no longer than is necessary for the purposes for which the data are processed (**storage limitation**);

f) processed in a way that ensures adequate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, by appropriate technical or organizational measures (**integrity and confidentiality**).

Article 32 of the GDPR clarifies the rules of security of personal data processing.

1. Taking into account the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of processing, as well as the *risk* of violation of the rights or freedoms of natural persons with different probability of occurrence and, the administrator and the processor shall implement appropriate technical and organizational measures to ensure a level of security corresponding to this risk, including but not limited to:

a) the pseudonymisation and encryption of personal data;

b) the ability to continually ensure the confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. When assessing whether the level of security is adequate, one should take into account in particular the risks associated with processing, particularly those arising from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed.
3. The administrator and the processing entity shall take steps to ensure that any natural person acting under the authority of the administrator or the processing entity who has access to personal data, processes it only on the instructions of the administrator, unless required by Union or Member State law.

### 3. Estimating the risk of personal data security

The basic attributes related to information protection are:

- *Confidentiality*: it informs about the required degree of information protection against unauthorized access;
- *Integrity*: it means that the data and information are correct, intact and have not been manipulated;
- *Availability*: it indicates whether data, processes and applications are available in accordance with user requirements or system requirements.[5]

### 3.1. Definitions

There are many definitions of risk related to different types of losses, e.g. financial, health. However, in the context of information security, another definition of risk should be adopted, according to the Polish Standard (PN), which says that *risk* is "the probability that determines the possibility of a given vulnerability being used by a given threat to cause a loss or destruction of a resource or group of resources, and thus negatively affecting the institution directly or indirectly".[6]

*Vulnerability* is to be understood here as a defect or gap in the physical structure, organization, procedures, staff, management, administration,

[5] K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, p. 19.

[6] *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych PN-I-13335-1*, Warszawa 1999; K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2009, p. 70.

hardware or software that can be used to cause damage to the IT system. Vulnerability is only a condition or set of conditions that allow a system to be damaged or an attack to interfere with user activity. A *threat*, in turn, is a potential breach of IT system security.

### 3.2. An example of a methodology for estimating personal data security risk

In this section, a modification is proposed to the method of estimating the risk for personal data proposed in a 2018 guide issued by the Polish Personal Data Protection Office.[7]

Risk assessment proposed there was based on the formula:

$$Rp = P \times (S_d + S_i + S_p)$$

where: (1)

Rp – level of calculated risk

P – value assigned to the probability of materialisation of a threat in the range {0, 1, 2, 3, 4}, where:

0 – unlikely event
1 – almost unlikely event
2 – unlikely event
3 – highly probable event
4 – almost certain event

$S_d$, $S_i$, $S_p$ – consequences of the event in terms of information availability, integrity and confidentiality respectively in the range of {0, 1, 2, 3, 4}, where:

0 – event has no effect (does not occur)
1 – the event has little effect
2 – the event has a significant effect
3 – the event has a very significant effect
4 – the event causes catastrophic effect

However, the formula below takes into account the guidelines of the PN-ISO-13335 standard saying that risk is a function of the value of resources at risk, the possibility of threats, the ease of using vulnerabilities

[7] A. Kaczmarek, M. Młotkiewicz, A. Łapińska, A. Miłocha, M. Mazur, *Jak rozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 1*, Warszawa 2018, p. 10.

by threats and existing security measures that can reduce the risk. Therefore, the following formula was used to analyze the risk[8]:

$$R = P \times S \tag{2}$$

where P is the probability of the materialization of a threat, and S its broadly understood effect, resulting not only from the value of the asset, but also from the far-reaching consequences of its loss or violation of confidentiality, integrity and availability, including potentially lost future transactions due to loss of trust.

In formula (2) it is proposed to set the P level on a five-point scale {1,2,3,4,5}. When determining the P value, it is advisable to consider the following:

- method of data processing (paper or electronic);
- number of electronic and non-electronic workstations where personal data are processed;
- number of persons having access to data during the performance of official duties;
- the amount of data processed;
- employee competences (current training, susceptibility to social engineering attack, employee loyalty);
- effectiveness of the security measures used (network connection, data encryption, validity certificates, timeliness and adequacy of security measures); in the case of paper documents, properly secured lockers;
- accountability of personal data processing, implemented regulations and procedures; accountability is an important attribute when processing personal data in the sense of identifying users and the services they use. It enables, for example, effective post-burglary analysis;
- other.

These issues should be reviewed regularly in the risk assessment process and risk should be modelled depending on the answers given. Parameter P is relatively variable in the risk evaluation process.

However, when determining the S value, the following component should be taken into account and evaluated on a five-point scale {1,2,3,4,5}:

[8] K. Liderman, *Analiza ryzyka…*, *op. cit.*, pp. 70, 94.

- type of information resource (ordinary personal data or belonging to a particular category of data) and legal consequences of its violation, and thus the validity of information in the context of the business process, including in the event of its loss or violation of integrity, confidentiality or availability

The far-reaching consequences of a threat to personal data, including the loss of trust and potential clients/contractors, are very difficult to estimate in the form of a specific amount of money, so it is perfectly reasonable to place this value on a point scale. For example, unauthorized acquisition of student email addresses will potentially result in a smaller loss than acquisition of email addresses of production company customers (in this case, competition may take over potential customers in a dishonest manner). Thus, each type of resource should be considered in the context of the business process and legal compliance. The value of information in the context of business impact analysis (BIA), as a determinant affecting the entity's activities, should be considered here. In the event of a breach of confidentiality, integrity and availability, the business continuity at least at the current level may be disturbed[9] (e.g. by taking over customer data by competitors and thereby taking over by the competition of the sales market; or by loss of trust as a result of data leakage and, as a consequence, unrealized transactions).

Therefore, the second component of consequences is proposed:

- accidental impact assessment of loss of confidentiality, integrity and availability

It should be remembered here that the attributes of information, i.e. confidentiality, integrity and availability, in the context of personal data security are not a disjoint set.

[9] *Zarządzanie ryzykiem – przegląd wybranych metodyk*, D. Wróblewski (ed.), Józefów 2015, p. 85.

All threats to the resources are directly related to the violation of any of these attributes; for example, *denial-of-service* (DoS) *or distributed denial-of-service* (DDoS) attacks target availability. Data theft is an attack on confidentiality, and an unauthorized change of information (e.g. as a result of hacking an organization's website) is an attack carried out on integrity. Many types of attacks can target more than one of the three aforementioned attributes: for instance DoS affects both confidentiality, integrity and availability, as it is about preparing the area for buffer overflow and executing the code chosen by the attacker to steal or change or destroy information. A hardware failure can affect the availability and integrity of information, and improper account policies can lead to violations of confidentiality and integrity. The key is to understand that one needs to protect personal data taking into account all three attributes of information security: availability, integrity and confidentiality.[10]

While creating threat scenarios, it should be kept in mind that reducing the processing susceptibility to one of the risk factors may cause an increase in vulnerability to other risk factors. Failure to comply with one obligation may affect the correct performance of the others.[11] Therefore, instead of adding the values of $S_p$, $S_i$, $S_d$ in formula (1), their average value is proposed as the resultant value. It should be taken into account that the average value is sensitive to extreme values, so it would be more accurate to take the median value of the $S_p$, $S_i$, $S_d$ value or another mathematical parameter[12], e.g. the floor function, as a resultant. The parameter S defined in this way is relatively constant in the risk evaluation process for a given asset or group of assets.

It should be assumed in the evaluation process in standard circumstances (e.g. permanent regulations) that the effect determined according to a set scale is a relatively constant value from period to period. Therefore, in the evaluation process, the value of risk is directly influenced by the P value, so it should be determined on the scale with particular precision and it should be meticulously observed from period to period. The P value directly determines whether the risk is acceptable or unacceptable.

[10] R. Janus, *Zarządzanie ryzykiem a bezpieczeństwo informacji – definicje*, "IT Focus", http://itfocus.pl/dzial-it/bezpieczenstwo/zarzadzanie-ryzykiem-a-bezpieczenstwo-informacji-definicje/ (accessed: 19.03.2020).

[11] A. Kaczmarek *et al.*, *Jak rozumieć…*, *op. cit.*, p. 15.

[12] K. Liderman, *Bezpieczeństwo…*, *op. cit.*, pp.183–186.

If one follows the above guidelines and sets the P level on a five-point scale; and then sets the S level by determining the components of S due to the type of resource and the importance of information on a five-point scale, as well as the resultant of confidentiality, integrity and availability – also on a five-point scale; then, ultimately, the S level will be determined as the product of the established level of type and validity of information and the resulting confidentiality, integrity and availability. With this methodology, it can take values from the set {1,2,3, … ..25}. In this case, the product of the component parameters is a mathematically more precise determinant of the S level than the sum of the component parameters, because it retains the weight (proportions) of the validity of the component parameters.

With the above methodology, one can obtain the following risk matrix consistent with the Polish standard.[13]

Table 1. The risk matrix created according to the proposed methodology

| Risk | Consequence | | | | |
|---|---|---|---|---|---|
| Probability | <1,5> | <6,10> | <11,15> | <16,20> | <21,25> |
| 5 | **5** | **6** | **7** | **8** | **9** |
| 4 | **4** | **5** | **6** | **7** | **8** |
| 3 | **3** | **4** | **5** | **6** | **7** |
| 2 | **2** | **3** | **4** | **5** | **6** |
| 1 | **1** | **2** | **3** | **4** | **5** |

Source: own elaboration.

The risk ranges from 1 to 9, and the presented risk matrix sets out three levels of risk (threats):

- <1; 3> residual risk that should be monitored in the risk evaluation process;
- <4; 6> acceptable risk for which a cyclical action plan should be defined;
- <7; 9> risk that must be immediately reduced (unacceptable risk).

The methodology set out in this way is the starting point for choosing adequate and appropriate security measures, and for setting priorities as well as the amounts of their financing.

[13] *PN-ISO/IEC 27005:2014-01 – wersja polska, Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*, Warszawa 2014, p. 62.

## 4. Summary

It seems highly likely that large institutions will use personal data security risk analysis in the near future using certified standards.[14] For now, certification is voluntary and the process of obtaining it must be transparent. GDPR in point 13 (in which, due to the special situation of micro, small and medium-sized enterprises, it provides for an exception regarding the recording of data processing activities for entities employing less than 250 employees) allows small enterprises to apply the methodology of personal data risk analysis based on their own capabilities. When choosing such a methodology, one should take into account applicable regulations while realizing that risk analysis is a process that is subject to continuous evaluation, which should be included in the adopted methodological tools. Risk management in small and medium enterprises can be successfully implemented in an MS Excel spreadsheet.

## References

Legal acts:

1. *Act of 10 May 2018 on the protection of personal data*, unified text, Journal of Laws of 2019, item 1781.
2. *The Constitution of the Republic of Poland of 2 April 1997*, Journal of Law No. 78, item 483, as amended.
3. *PN-ISO/IEC 27005:2014-01 – wersja polska, Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*, Warszawa 2014.
4. *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)*, Official Journal of the European Union, L 119/89, 4 May 2016.
5. *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych PN-I-13335-1*, Warszawa 1999.

[14] See *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)*, Official Journal of the European Union, L 119/89, 4 May 2016, Article 42, points 1 and 2.

Literature:

1. Aptekarz M., *RODO Moduł S11 – ECDL Standard*, Katowice 2018.
2. Budzyń P., *Ochrona informacji niejawnych w świetle krajowych aktów prawnych*, "Bezpieczeństwo. Teoria i Praktyka", 2015, no. 3 (XX), pp. 13–26.
3. Byczkowski M., Zawiła-Niedźwiecki J., *Analiza ryzyka w zarządzaniu bezpieczeństwem danych osobowych. Zarządzanie ryzykiem w kontekście ochrony informacji*, "Monitor Prawniczy", 2014, no. 9, special supplement: *Aktualne problemy prawnej ochrony danych osobowych*, pp. 45–49.
4. Janus R., *Zarządzanie ryzykiem a bezpieczeństwo informacji – definicje*, "IT Focus", http://itfocus.pl/dzial-it/bezpieczenstwo/zarzadzanie-ryzykiem-a-bezpieczenstwo-informacji-definicje/ (accessed: 19.03.2020).
5. Kaczmarek A., Młotkiewicz M., Łapińska A., Miłocha A., Mazur M., *Jak rozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 1*, Warszawa 2018.
6. Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2009.
7. Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012.
8. *Zarządzanie ryzykiem – przegląd wybranych metodyk*, D. Wróblewski (ed.), Józefów 2015.

Cite this article as:

S. Kosznik-Biernacka, *The analysis of risks to personal data security*, "Security Dimensions", 2020, no. 34, pp. 256–267, DOI 10.5604/01.3001.0014.5614.