Advances in Economics, Business and Management Research, volume 31

4th International Conference on Management Science and Management Innovation (MSMI 2017)

Determination of Personal Data Sensitivity and Security Measures Assignment

Tomasz Lovecek
Wyższa Szkoła Oficerska Wojsk Lądowych
i. Gen. T. Kościuszki, Wydział Nauk o Bezpieczeństwie
Wrocław, Poland
e-mail: t.lovecek@wso.wroc.pl

Jozef Ristvej
Department of Crisis Management
University of Žilina
Žilina, Slovak Republic
e-mail: Jozef.Ristvej@fbi.uniza.sk

Marián Magdolen
Department of Security Management
University of Žilina
Žilina, Slovak Republic
e-mail: marian.magdolen@fbi.uniza.sk

Roman Ondrejka
Transport Research Institute, Inc.
R&D Division, www.vud.sk
Žilina, Slovak Republic
e-mail: ondrejka@vud.sk

***Abstract*—Protecting privacy and personal data is in current environment a more and more challenging task not only for government institutions, but for small and large businesses as well. With the information technology advancements more and more personal data are processed automatically each year. That is the reason why effective, adequate and economic security measures have to be adopted to protect privacy of data subjects. By applying security measures blindly without deeper knowledge about sensitivity of such personal data, will not address the expectations for both, processors, for cost and maintenance effectiveness and data subjects, for most secure and trustworthy security measures. To overcome this conflict of expectations, a system for evaluating personal data sensitivity was created, as a tool to assign appropriate security measures according the correct level of sensitivity. This system complements current security measures assignment methods, which do not include data subjects to the process.**

Keywords–personal data protection; sensitivity; security measures; data security; privacy

I. Security Measures Assignment According the Legislation

Current legislation in the Slovak Republic and the European Union leaves a relatively wide scope for independent evaluation to an operator, what security measures shall be adopted in order to protect personal data. In the regulatory framework for the protection of personal data which was adopted by the European Union, the Directive No 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as "Directive 95/46/EC') is security of personal data stipulated in Article 17. Directive 95/46/EC lays down the obligation to guarantee the protection of personal data through the implementation of "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing." Also provides an explanation of security measures and that "having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected." Method of risk analysis and the adequacy of the measures taken is in the competence of processors, who are in a position to do so on the basis of their own discretion and often regardless to the nature of the persons.

In the Slovak legislation, Act No. 122/2013 Coll. on protection of personal data, security of personal data in information systems is responsibility of the processor. He/she is obliged to protect processed personal data before their damage, destruction, loss, alteration, unauthorized access and accessing, by providing or disclosure, as well as against any other irregular means of processing. For this purpose, he/she shall take appropriate technical, organizational and personnel measures (hereinafter referred to as "security measures") corresponding to the means of personal data processing, taking into account in particular applicable technical resources, confidentiality and importance of processed personal data, as well as the extent of risks which are likely to disrupt safety or functionality of information system." [1] Processor is obliged to document applied security measures in the security documentation, and also in the case of inspection demonstrate scope and content of such measures. When establishing and adopting security measures law specifies that they must be in accordance with the safety standards and at the same time also with the generally binding legal regulation, issued by the Office of personal data protection.

The operator determines the range of appropriate security measures before start of processing, but also during processing itself. "Range of appropriate security measures corresponds to particular conditions of personal data processing and security risks arising from the category of personal data, which relates to the increased risk of abuse, and from the way of processing. Appropriate security

measures shall ensure an adequate level of protection in terms of their safety, reliability and performance, as well as from the point of view of confidentiality, integrity and availability of personal data." [2]

II. Problems of Current System

When laying down the rules of personal data protection, it is necessary to take into account not only the legal system, interests of the State and the personal data processors, but the rights and obligations of the data subjects as well. The fact is, that the sensitivity of personal data is due to the nature of the person and nature of the data different for each individual and this sensitivity may at any time for objective or subjective reasons to change. To determine an appropriate protection of personal data not only the legal categorization of personal data is decisive, but the subjective sensitivity of personal data, which is not based on legal categorization, is crucial too. Subjective sensitivity is the result of subjective perceptions of certain personal data by a particular person, who may have on the sensitivity and the protection of particular personal data other point of view as a processor, legislation or practice. It is not the exception that individuals protect the different personal data more than those to which greater protection is prescribed by a legislation (such as photos - sharing content on social networks, etc.).

The current system does not take into account the perception of personal data by individuals, which changes with passage of time, status of the data subject, employment, social role or working position or from other hardly predictable reasons. In current system of security measures assignment, it is almost impossible to address these changes in sensitivity, and thus differences of opinion between the data subjects, processors and authorities on adequacy of security measures can be substantial.

III. Model for Personal Data Sensitivity

In the current legislative settings, sensitivity of personal is taken into consideration only in the distribution of personal data into two categories of personal data that the law recognizes. Regular, or "ordinary" personal data and a "special" personal data "which are regarded as sensitive" [3] and which are listed in full in Article 13 of Personal data protection Act.

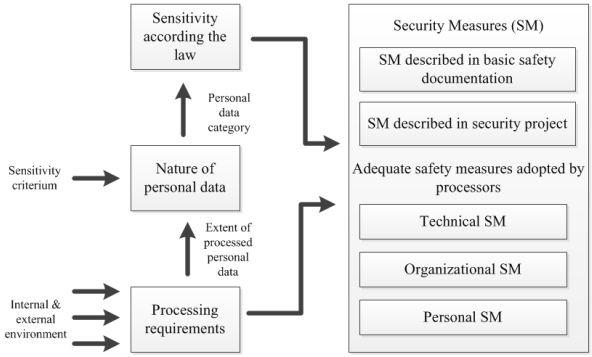

Figure 1. Current system of security measures assignment

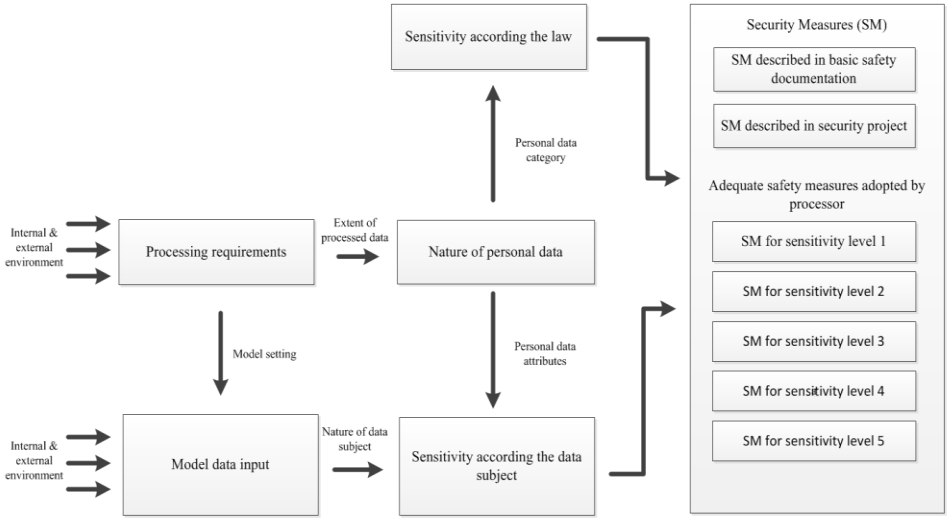

Figure 2. Proposed system of security measures assignment

For the processing of the special category of personal data the law has more stringent criteria and specifies exact conditions for processing. On the basis of this division law defines certain specific security measures for each category of personal data and the rest of security measures leaves to determine to the processor. These security measures have to be documented in the safety documentation that is part of a security project in concrete information system.

To improve current method for appropriate security measures assignment and for the consideration of personal data sensitivity from the data subject point of view we created and designed model for personal data sensitivity determination. This model takes into account not only all legislative requirements, as described above, but in particular takes into account subjective sensitivity of personal data, the estimated value of the assets in the form of personal data and assigns adequate security measures according to a specified level of sensitivity.

IV. Requirements for Personal Data Processing

Processor is obliged prior to processing to identify the purpose of the processing and define the legal basis on which the personal data will be processed. [4] On the ground of an identified purpose and legal basis the requirements for personal data processing are set, which should be determined before the actual start of processing. These requirements have to be evaluated and updated even during or after the end of the processing.

Processor sets out processing requirements or, in some cases can be determined according the law or directly binding legislation of European Union or international treaty, which is bound for Slovak Republic". [5] Processing requirements shall mean "means and methods of personal data, as well as further requirements, criteria or guidelines related to the processing of personal data or execution of the operations that serve to achieve the purpose of processing either before the processing, or during the processing". [6]

"The processing requirements includes technical and organizational issues related to security of personal data processing (e.g.: what kind of personal data will be processed; what will be the method of processing; whether automated means of processing will be used, which processing operations will be carried out, who and in what extent will have access to the personal data, etc.)". [7]

By consistent and responsible determination of processing requirements the processor is being prepared both organizationally and methodically for processing and creates grounds for technical, organizational and personal security measures establishment, which results from the conditions.

V. Nature of Personal Data and Data Subject

Processor is obliged to ensure that, „only such personal data shall be processed that are corresponding in extent and content to the purpose of processing and are necessary for its achievement". [8] Extent of personal data must be strictly assessed within the purpose of the processing, or must be defined in a legally binding document that defines processing requirements and determines which personal data may be processed for the purpose. The law sets out the types and categories personal data, which is not allowed to process, or they can be processed only under certain strict conditions or for a legal purpose.

Between such personal data may be included, for example, special categories of personal data pursuant to section 13 of the Law, which prohibits to process personal data, "revealing racial or ethnic origin, political opinions, religion or beliefs, membership in political parties and political movements, membership in trade unions and data concerning health or sexual life". [9] In the same paragraph the law stipulates types of personal data that can be processed only on the basis of a legal authorization, or may be processed only by persons with specific education.

Data subject for the purposes of personal data protection is “any natural person to whom the personal data are concerned". [10] This means that data subject can also be a person whose data are not directly processed in an information system, but it in some way the data concerns the person.

Taking into consideration that every individual is different and in his essence unique, to determine sensitivity of his personal data, which are processed in an information system, his nature must be taken into account. The nature of the data subject is based on his characteristics and affects the possible consequences that may arise from the disruption of integrity, availability and the confidentiality of personal data, which are processed in the filling system.

VI. Consequences of Violation of Personal Data Attributes

The important information to evaluate appropriate security measures is the value of the assets and consequences (the value or the impact volume), which would occur in the event of disruption of one of the personal data attributes or in the case of personal data leak from the filling system. The event can be understood as incident of information security, which constitutes the undesirable, or unexpected events in information security, or a series of such events that can with a significant probability compromise operations and activities within the organization and threaten safety information. [11]

An event result is a loss of fundamental attributes - integrity, confidentiality and availability, or other attributes (non-contradiction, responsibility, authenticity, reliability, etc.) of the data, which we can later evaluate and quantify. [12] Each attribute relates to a feature of the information or its characteristics and to protect this feature it is necessary to protect any attribute with different security measures. With protection of integrity we protect accuracy and completeness of personal data, with protection of availability we protect accessibility and usability of personal data and with protection of confidentiality we protect feature that information is not available or is not exposed to unauthorized individuals, entity or process. [13]

VII. Evaluation of Model for Personal Data Sensitivity

To determine level of personal data sensitivity, it is necessary to obtain from data subjects information for an evaluation of nature of the person and expected

consequences in case of disturbance of any of the personal data attributes. Processor sets out processing requirements based on means and method of processing, purpose and legal basis of processing as well as extent and category of personal data processed in the filling system.

Based on this processing requirements – scenario – explanation of personal data processing is prepared for data subject. According this scenario, data subject has the possibility to add information about his nature and impacts that are likely to happen in case of disruption. Processor shall evaluate available data and according the model determines the level of sensitivity of processed personal data according the data subjects.

The final level of personal data sensitivity is valid for a particular data subject that such assessment carried out and for a specific attribute, whose consequences was evaluated. The general level of sensitivity is made of partial evaluations as an average of partial sensitivity levels. The general level is more objective as more data subjects provide the necessary information. The sensitivity can be different to each evaluated attribute (integrity, availability, confidentiality) and according these levels appropriate security measures can be assigned to protect attributed, that is valued as most sensitive.

VIII. Security Measures Application According to the Model

The model for personal data sensitivity determination and security measures assignment divides and suggests assignment of security measures from the list of measures. The list consists of two main sources of security measures.

First one – actual legislation on personal data protection sets a group of security measures, that are compulsory to implement according the type of security documentation that is processor obliged to prepare. This security measures have to be implemented regardless of sensitivity or category of processed personal data and are exhaustingly stipulated by the law.

The second source is aimed to provide appropriate security measures for selected level of sensitivity and to enable to scale the measures according the needs of processors. Security measures are structured to three basic types – technical, organizational and personal security measures and each security measure is scaled according the level of sensitivity and type of attribute that is able to protect. These measures came from all kinds of relevant sources as legislation (on personal data protection, classified information, recommendations of relevant institutions, or technical standards in the field of information security - STN ISO/IEC 27001, ISO/IEC ISO 27002, and others as - EN 1627, EN 50131-6 and STN 36 9510-1).

These measures take into account the personal data sensitivity not according to the category set by the law, but according to foreseeable consequences of personal data attribute disruption (integrity, availability and the confidentiality), the nature of data subjects and processing requirements. Individual measures are scaled in the extent and by the means of implementation (if the scaling is possible) according the sensitivity and the processor can immediately implement correct measures for ensuring the safety of personal data.

In the case when some measure can be implemented for different levels of sensitivity (based on different attributes), processor shall implement the measure in the higher sensitivity level achieved by the model.

IX. Estimated Theoretical and Practical Benefits of the Model

By establishing the model for sensitivity level determination and security measures assignment for the particular filling system, quick, comprehensible, easy to use and effective method for protection of information systems will be developed. By application of the model and by selecting appropriate security measures we expect to provide benefits for any interested party when processing personal data.

Processors can gain transparency, efficiency and simplification of the obligations resulting from the legislation and they may obtain a considerable cost savings and effectiveness of processes in the activities in which the personal data are processed. By determination of sensitivity level based on specific data subjects, processors are communicating with their customers and are able to reflect requirements of these persons and, at the same time to fulfil all legal obligations to establish appropriate security measures. In the case obligation to carry out a security analysis of the information system, which is a prerequisite for a security project, processors can use the model as an appropriate tool for primary assets value determination (value of processed personal data) as part of risk assessment required by the ISO/IEC 27005. When the processor is aware of the value of processed data he/she can more adequately assign appropriate security measures to preserve protection of filling system as well as to identify critical processes in personal data processing and to better understand and protect this processes.

By application of the model data subjects can acquire very quick overview of expected level of security and which security measures are appropriate to implement for protecting their personal data. By comparing their sensitivity level to the others they receive a comparison of their expectations to the rest of data subjects. The list of security measures divided by the sensitivity level could be an inspirational guideline what to demand from processors when they are processing their personal data.

Inspection authority can through the model simply evaluate and review adopted security measures and perform more effective inspections. Evaluation of the adopted security measures may be reviewed not only on the basis of legal requirements (in accordance with the categories and with access to the public computer network), but also on the basis of up to now unavailable data subject's opinion on personal data sensitivity.

In addition to involvement of data subjects in the process of personal data processing, raising public awareness on the personal data protection, the inspection authority is gaining valuable statistical data about subjective sensitivity levels of different personal data types and scopes as well as of various

processing requirements and filling system character. Just as a valuable information could be an evaluation of personal data from the data subject's point of view and their opinion on adopted security measures.

For interested public the model can serve as an inspiration and an example of minimal security measures, that shall be adopted when processing personal data and to obtain a better overview of the possibilities, conditions, categories and security measures when processing such data. We refer possibilities of use to norms and other authors such as [11], [12], [13], [14], [15].

Introduced model can in the same time as the only available method determine the level of sensitivity for individual personal data attributes, and so adapt the security measures to the sensitivity levels, to reflect the requirements for their protection. By evaluation of sensitivity of individual attributes, the processor can adapt composition and extent of security measures with respect to the expectations of the data subjects, to improve provided personal data protection and to increase trust between processor and data subjects.

X. CONCLUSION

A conventional practice in the protection of personal data forgets on one key subject – data subject whose active involvement does legislation or processors not foresee. The input and knowledge of individual requirements for protection would significantly increase the awareness, security and efficiency when processing of the personal data.

The suggested model is a way how on the basis of the requirements and assessments of the nature of the data subjects and expected impacts in the event of disturbance of personal data attributes, to evaluate more objectively personal data sensitivity and to identify and assign adequate security measures to ensure their protection.

In article we have addressed the manner of personal data processing and adequate security measures assignment in accordance with the legislative conditions and on the basis of identified shortcomings we proposed a way how to include the data subject in the processing of the personal data to increase personal data protection level. With this inclusion of data subject, we could reform the personal data processing system.

ACKNOWLEDGMENT

"This article was created as a one of project outcomes of work co-funded by the Slovak Research and Development Agency under the contract No. SK-CN-2015-0015 Enhancing Cooperation of the Ningbo University of Technology and the University of Zilina in research, innovation and cooperation within the topic of Intelligent Transport Systems."

"This article was created as a one of research project outcomes VEGA 1/0749/16 Risk Assessment and Treatment of Industrial Processes in Relation with Integrated Security and Safety within Lower Tier Establishments."

The views expressed, however, are solely those of the authors and not necessarily those of the institutions with which they are affiliated or of their funding sources.

The authors are solely responsible for any errors or omissions.

REFERENCES

[1] Slovak republic Act No. 122/2013 Coll. on protection of personal data, Article 19, paragraph 1.

[2] Valková, Z., Dudáš, J., Palúš, J.: Zákon o ochrane osobných údajov: Komentár od autorov zákona / Act (Act No. 122/2013 Coll.) on protection of personal data – comments from authors of the act. 2013, p. 149.

[3] Macová,M.,Vrabko,M.: Zákon č. 122/2013 Z.z. o ochrane osobných údajov s komentárom / Act No. 122/2013 Coll. on protection of personal data – with comments. 2013, p. 77.

[4] Slovak republic Act No. 122/2013 Coll. on protection of personal data, Article 6, paragraph 2, a).

[5] Slovak republic Act No. 122/2013 Coll. on protection of personal data, Article 4, paragraph 2, b).

[6] Slovak republic Act No. 122/2013 Coll. on protection of personal data, Article 4, paragraph 3, e).

[7] Valková, Z., Dudáš, J., Palúš, J.: Zákon o ochrane osobných údajov: Komentár od autorov zákona / Act (Act No. 122/2013 Coll.) on protection of personal data – comments from authors of the act. 2013, p. 61.

[8] Slovak republic Act No. 122/2013 Coll. on protection of personal data, Article 6, paragraph 2, d).

[9] Slovak republic Act No. 122/2013 Coll. on protection of personal data, Article 13, paragraph 1.

[10] Slovak republic Act No. 122/2013 Coll. on protection of personal data, Article 4, paragraph 2, a).

[11] ISO/IEC 27000:2016: Information technology - Security techniques - Information security management systems - Overview and vocabulary. 2016, p. 12.

[12] ISO/IEC 27005:2011: Information technology - Security techniques - Information security risk management. 2011, p. 39.

[13] ISO/IEC 27000:2016: Information technology - Security techniques - Information security management systems - Overview and vocabulary. 2016, p. 9.

[14] Holla, K.: Dealing with Key terms in Risk analysis and Phenomenon of uncertainty in this process, In: Communications - Scientific Letters of the University of Zilina, vol. 9, No. 4, p. 59-61, 2007, ISSN 1335-4205.

[15] Zanicka Holla, K., Moricova, V.: Human Factor Position in Rise and Demonstration of Accidents, In: Communications - Scientific Letters of the University of Zilina, vol. 13, No. 2, pp. 49-52, 2011, ISSN 1335-4205.