General Model for Personal Data Sensitivity Determination

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

Jozef Ristvej
Department of Crisis Management
University of Žilina
Žilina, Slovak Republic
email: jozef.ristvej@fbi.uniza.sk

Tomáš Loveček
Department of Security and Safety Research
University of Žilina
Žilina, Slovak Republic
email: tomas.lovecek@fbi.uniza.sk

Martin Hromada
Department of Security Engineering
Tomas Bata University in Zlín
Zlín, Czech Republic
email: hromada@fai.utb.cz

***Abstract*—This article is a presentation of a general model for personal data sensitivity determination, which is based on early PhD research on personal data protection. 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. But 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 model for personal data sensitivity was created as a tool to evaluate the sensitivity and assign appropriate security measures.**

Keywords - Personal data protection; security measures, data security; privacy.

I. INTRODUCTION

Right to privacy is one of the fundamental human rights recognized by many international and national conventions, treaties, constitutions and laws. In current security environment and unstoppable information technology development, securing the privacy is one of the grand challenges of today's democracies. General availability of information technology and cloud services, as well as widespread internet usage and increase of web-based transactions, use of social media, targeted advertisement, smart metering and others, create countless opportunities to collect, process, store, analyse and correlate massive quantities of personal data about individuals. To ensure adequate security of this data, processors are forced to ensure their safety by implementing various security measures. Some of the measures are stipulated in the national laws, but others are adopted or just recommended to implement from other sources of information data security documents (e.g., ISO 27 000). We can rarely find an applicable method on how to implement adequate security measures to personal data by taking into account sensitivity and categories of personal data, character of data subject and/or other information relevant for data protection. It is crucial to fully comprehend the interaction between the protection of privacy and the furtherance of security in order to attempt to set appropriate limits [1]. In Section 2 of this article the current process of application of security measures in Slovak Republic with pointing out some of most serious shortcomings of this system is described and later in Section 3 the assessment of the point of view of data subjects for sensitivity of their personal data and in Section 4 and 5 the model for personal data sensitivity determination and its evaluation process is described.

II. APPLICATION OF SECURITY MEASURES IN THE SLOVAK REPUBLIC

Like all European countries, Slovak Republic adopted a law on protection of personal data of individuals as well. Based on the European directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data (hereinafter referred to as "Directive"), our national legislation tries to issue instructions on how to process and secure personal data by processors to ensure the right balance between privacy and security. Although the European directive 95/46/EC established an obligation for member states to ensure that "appropriate technical and organizational measures should be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing;…whereas these

ISBN: 978-1-61208-493-0

measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risk inherent in the processing and the nature of the data to be protected" [2], neither in the directive nor in the Slovak laws or bylaws there is any hint on how to implement these security measures or any explanation of how to determine the appropriateness of security measures to the protected data. In Slovakian act No.: 122/2013 Coll. on personal data protection, our legislators stated that: "the processor is responsible for securing personal data. Therefore, he shall undertake appropriate technical, organizational and personal measures that correspond to the means of data processing, taking into account technical resources employed, confidentiality and importance of processed personal data…" [3]. The extent of appropriate security measures corresponds to specific conditions of processing personal data in filling system, to security risks resulting from the category of processed personal data (e.g., if sensitive data are processed) and to means of processing of such data [4]. However, there is no relevant instruction for processors on the appropriateness of implemented security measures, on the kind of risk assessment method they shall apply and on how to assess confidentiality and importance of processed personal data. Processors can just assume if the taken security measures are appropriate and most of the processors apply the ISO standards on information security to fulfil the requirements. According to our knowledge, there is no other method that would address personal data protection and appropriate security measures assignment along with consideration on data subject sensitivity.

III. Data Subject Point of View

Neither the EC directive nor the Slovak national legislation take into account the perspective of how the data subject feels about the security measures taken by processors. How to include data subjects into the process? The problem regarding personal view on data processing is mainly the possible change in opinions about sensitivity of personal data. People change, circumstances change, the position and situation of individuals change in time. Individual with no interest in special protection of his personal data can, in a few years, become a politician and, as a public officer, his interest to protect his privacy will increase. In that case, from his point of view, the implemented security measures might not be appropriate anymore and it is his prerogative to demand higher level of security. Of course, processors cannot treat each data subject individually when processing large amount of data about undefined number of individuals. But on the other hand, they should take into account sensitivity of personal data not only from their point of view but from point of view of data subjects as well. Assessing such sensitivity level is the very first step for implementation of appropriate security measures which will be not only in accordance with actual legislation but within the expectations of data subjects as well.

IV. Model for Personal Data Sensitivity Determination

Model for personal data sensitivity determination (hereinafter referred to as "model") is a model developed with the aim to include sensitivity of processed data to the data protection, to include data subject specifics and with additional knowledge about processed data to appropriate assign security measures to each specific data filling system. Within the model, various facts are evaluated and as a result, the level of sensitivity of processed data is revealed. With the specified sensitivity level, we can then assign effective, appropriate and adequate security measures to protect personal data in filling system of processor.

If we want to embrace sensitivity as the key factor for security measures implementation, we should use model for sensitivity determination in order to evaluate processed personal data. In order to do so, we should take into consideration a few facts and conditions that are relevant to this process. Legislation requires the processors to establish the conditions for data processing before the processing starts so the processors should evaluate the sensitivity beforehand.

There are three major areas the variables to the model are taken from. The first set is taken from legislation and is obligatory for each processor to include and determine these facts when processing personal data. The second set of variables is based on the type of filling system on conditions and background that are applicable. The third set is based on the knowledge of data subjects and categories of processed data. As the processor shall determine the sensitivity beforehand, it is important to estimate the information carefully and during processing regularly challenge these values to not to underestimate the changes and security measures that have been taken.

First of all first set consist of a few basic legal requirements, that each processor has to fulfil - to determine the nature and purpose of personal data filling system, processors shall define (1) purpose of processing, (2) legitimacy of processing (3) the planned length of time the data are to be stored.

The purpose of processing shall be clearly defined and data collected for specified, explicit and legitimate purpose only. It is forbidden to process data otherwise that is incompatible with those purposes [5]. For data subject, clearly defined purpose of data processing is a first sign of trust when the personal data have been given. The extent of processed personal data (number of personal data collected) is evaluated and the legitimacy of processing is established according the defined purpose.

Personal data may be processed only if the legitimacy of processing is within the Article 6 of Directive. "Personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of data subjects; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of data subject which require protection…" Slovak act No.: 122/2013 Coll. recognize two types of legitimate purposes for data processing – processing without consent of data subject and processing based on consent of data subject. Processor shall process data without consent of data subject if the purpose of processing, data subjects and the extent of processed data are specified in directly applicable EU law, binding international treaty, law about personal data protection or other particular law [6]. Besides these situations, data shall be processed without consent only in cases mentioned in the Directive, Article 6 and when it is necessary for purposes of journalism or the purposes of literary or artistic expression [7]. Processing data based on consent of data subject is applicable when the consent is freely given, informed and specific and signifies his agreement to personal data relating to him being processed [8].

The planned length of time the data is to be stored is relevant information to assess how long the data are vulnerable. Processors have to ensure that the personal data will be processed no longer than necessary to obtain the purpose of processing [9]. To this first set of information, we have to consider other facts that are subject to the specific settings of personal data filling systems and have relevance to sensitivity determination.

The second set of variables can vary in time but, in the end, the influence on sensitivity is obvious. That includes information about (1) transfer of personal data to other countries; (2) means of processing of personal data; (3) list and nature of third persons or recipients that have access to the data.

Cross-border transfer of personal data "may take place only if the third country in question ensures an adequate level of protection" [10] and "the personal data should be able to flow freely from one Member State to another, but the fundamental rights of individuals should be safeguarded" [11] at all times.

The means of personal data processing are up to processor, whether it is automatic or manual processing. Currently, when everything is online and is processed by information technology, manual processing can evoke more trustworthy and secure way of data processing. On the other hand, many security breaches are still caused not by overcoming the information technological security measures but caused by human error or betrayal.

By processing large amount of data, rarely the processors are able to maintain and administer their filling systems alone. It often depends on purpose but information sharing is often necessary to fulfil the goal of processing and providing access to the data to third persons or other recipients is inevitable. Third party usually means "any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the person who, under the direct authority of the controller or the processor, are authorized to process the data" [12] and recipient means "natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not" [13]. Recipients and third parties shall have legitimate reason why to gain access to the data and processors shall very carefully inquire why, when and to what extent to provide the data to such parties.

Third set is based on the knowledge of data subjects and categories of processed data. This is a crucial part as this information is the most relevant to determine whether the processed data are being considered as sensitive from data subject point of view. Processors have to research and gain detailed knowledge about (1) scope of personal data and their category and (2) information about count, nature and character of data subjects.

The directive and Slovak national law about personal data protection stipulate that processors can process only such personal data which scope and content correspond to the planned purpose of processing and are essential to achieve such purpose [14]. Except the proportionality of used data the requirement of using only correct, complete and if necessary up-to-date personal data is applicable and all other data shall be without delay repaired, completed or blocked and subsequently erased [15]. The category of personal data is determined by legislation for regular and special personal data but this division is, in our opinion, not sufficient, very subjective and does not reflect the real opinion of data subjects. Directive forbids to process special data except special circumstances defining special data as data which "reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the data concerning health or sex life" [16]. Slovak national law goes beyond this characteristic and as special category of personal data names **-** except types of data that are mentioned in Directive as well general identifier of citizens - information about psychical identity and competence, criminal records data, biometric data and image and video files containing any captures of individuals [17]. Extent of such personal data is wide enough to cause problems with processing such data and with assignment of appropriate security measures. For example, photo of individual is so commonly used in many filling systems that assignment of such type of personal data for special category, with strict security rules and permissions to process it, often causes difficulties for processors. Various individuals often have different opinions for special category of data, some of them value more their mobile number than their image/photo or are willing to share the medical data over the credit card number. It is therefore obvious that processors have to evaluate each type of personal data individually and estimate how sensitive such type of data will be for data subjects and accordingly threat (secure) such data.

The last variable relevant for the model is information about count, nature and character of data subjects. Again, processors have to estimate this information beforehand but it is important to update this information regularly in order to assign appropriate level of security to the filling system. Count of data subjects is related to the possible impact of security breach, nature and character of data subjects is relevant to the seriousness of possible security breach.

With all this facts we can estimate the sensitivity of personal data in order to implement such level of security for processor's processing operations that will be adequate, legitimate and appropriate but will also take into account the estimated sensitivity of data subjects.

V. Evaluation of Sensitivity

To evaluate sensitivity of filling system processing personal data, we have to evaluate each factor included into the model. For each factor, one or more questions to be answered are integrated into the model and to each possible pre-set answer there is a certain number of points assigned. After answering all the questions the final value is showing the estimated sensitivity according to the scale. The maximum number of points that are possible to gain is 85. With this high score, it is obvious that processed data are extremely sensitive and in further operation the security measures have to be very exhaustive and other procedures to limit the vulnerability shall be implemented. The minimum number of points that the filling system is able to receive is 18. In such case, most of the data are with low sensitivity and the security measures and vulnerability of the personal data is of low risk. Sensitivity is scaled into five distinctive levels of low, moderate, high, very high and extreme sensitivity.

TABLE I. Sensitivity Evaluation Scale

Evaluation	Points score
Low sensitivity	18 – 25
Moderate sensitivity	26 – 40
High sensitivity	41 – 55
Very high sensitivity	56 – 70
Extreme sensitivity	71 – 85

According to the sensitivity level, we can assign appropriate security measures to each specific data filling system. This is the second part of model where - after thorough risk assessment - effective, appropriate and adequate security measures that are in correspondence with estimated sensitivity of the processed personal data in the filling system could be assigned.

VI. Conclusion

To evaluate sensitivity of filling system processing personal data, we have to address many aspects and steps of processing procedure. Sensitivity level together with later risk assessment allow the processors or data subjects to confirm the expectations for security measures to be taken in any given filling system. Processors are constantly searching for most economical but still sufficient system how to determine and apply security measures for their system and data subjects expect the best security for their personal data. After recent development in massive personal data breaches and mass surveillance affairs, applying adequate security measures will become more and more important to general public in order to ensure their privacy [18]. As the view on personal data sensitivity is changing with various conditions, in the future, there will be more often demand for interactive system that will be able to determine sensitivity level and further help to assign appropriate security measures which will satisfy both processors and data subjects.

Acknowledgment

This work was supported by the research project VI20152019049 "RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems", supported by the Ministry of the Interior of the Czech Republic in the years 2015-2019.

References

[1] S. Stalla-Bourdillon, J. Phillips, M. D. Ryan, “Privacy vs. Security”, Springer: London, 2014, ISBN 978-1-4471-6529-3, pp. 5

[2] Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, Paragraph 46

[3] Law No.: 122/2013 Z.z. about protection of personal data, Paragraph 19

[4] Z. Válková, J. Dudáš, J. Palúš, “Zákon o ochrane osobných údajov. Komentár od autorov zákona”, Kaštieľ Mojmírovce, 2013, ISBN 978-80-971476-4-8, pp.149

[5] Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, Article 6, Section b)

[6] Law No.: 122/2013 Z.z. about protection of personal data, Paragraph 10

[7] Law No.: 122/2013 Z.z. about protection of personal data, Paragraph 10, Section 3, a)

[8] Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, Article 2, Section h)

[9] Law No.: 122/2013 Z.z. about protection of personal data, Paragraph 6, Section 2, g)

[10] Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, Article 25

[11] Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, Paragraph 3

[12] Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, Article 2, Section f)

[13] Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, Article 2, Section g)

[14] Law No.: 122/2013 Z.z. about protection of personal data, Paragraph 6, Section 2, d)

[15] Law No.: 122/2013 Z.z. about protection of personal data, Paragraph 6, Section 2, f)

[16] Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, Article 8, Section 1

[17] Law No.: 122/2013 Z.z. about protection of personal data, Paragraph 13

[18] S. Stalla-Bourdillon, J. Phillips, M. D. Ryan, “Privacy vs. Security”, Springer: London, 2014, ISBN 978-1-4471-6529-3, pp. 93