Available online at www.worldscientificnews.com

World Scientific News

WSN 85 (2017) 68-73 EISSN 2392-2192

Data protection by design on the ground of a general data protection regulation

Piotr Siemieniak

Faculty of Law and Administration, University of Gdansk,
6 Jana Bażyńskiego Str., 80-309, Gdańsk, Poland

E-mail address: piotr@upsecure.pl

ABSTRACT

Each member of the information society generates, often quite involuntarily, noticeable amounts of data being closely related to them. The range of such data may be extremely extensive as it may encompass the details on the geographical positioning, the data regarding the network behaviours or the data on ID numbers for the devices used. Hence, there exists a more and more intensified and permanent risk of the right for privacy, one of the most fundamental human right, being infringed on. Data controllers attempt to enter any personal data which are easily accessible due to the operational peculiarities applicable to various technological solutions. Such actions may infringe on the rights included into the charter of fundamental rights, namely the right for privacy and the right for personal data protection. Consequently, the data controllers remain under obligation to carry out a series of duties within the area of personal data protection that are related to appropriate technical and organisational means being applied in order to achieve full legal compliance on the matter. Privacy protection remains a complicated process involving the interactions from various areas including the law, software engineering, cycle management or ethics. One of the legal solutions to be introduced by the general data protection regulation is , the so called, "privacy by design" model. The following publication is intended to present the privacy by design model on the ground of the general data protection regulation.

***Keywords*:** data protection, privacy protection, privacy by design, general data protection regulation, information security

1. INTRODUCTION

In the era of the information society the majority of information is processed by means of modern and innovative technologies. Each action performed in any area of human life results in the information about us been left behind. On numerous occasions we are not aware of the amounts of information being collected about us which are subsequently analysed and used for the purposes unknown to us. This brings about the limitation of information privacy under circumstances when we intended to keep such information secret. On the other hand, however, actions taken which take advantage on the information regarding us may lead to the limitations in decisive privacy. Data disclosure would also result in the infringement on the interests of the person involved and would influence their entire functioning as well as the lives of their close relations.

Most of us do not have any protective measures to secure our interests. This results from the fact that very few people are knowledgeable about the functioning principles for various IT systems and algorithms used therein. The process of data collection, their analysis and decisive algorithms do not have a transparent character for the data subjects. Hence, it is extremely important to create the effective mechanisms serving to enforce the position of an individual and to protect their privacy.

The aforementioned circumstances contributed to the fact that personal data protection has received noticeable interest since the end of XX c. Providing an individual with privacy is related not only to the introduction of the relevant legal solutions regulating the issues regarding personal data processing. This constitutes an initial step only within a complicated process that forces the data processing entities to commence the actions and implement the procedures intended to protect the personal data. Therefore, their controller must be provided with the relevant tools securing privacy to an individual along every stage of data processing.

Leading the aforementioned postulate to fruition is not an easy task at all. On top of that, it requires noticeable financial investment. Hence , it is extremely important to equip the data processing entities with guidelines and criteria based on which efficient products or services could be created taking advantage of the relevant technological advances.

The guidelines as to how the proper personal data protection system is to be created have been set forth in the concept “privacy by design” (privacy protection during the designing phase), which focuses on the assumption that privacy protection should be included into every stage of development for a given system, process or service.

2. PRIVACY BY DESIGN - HISTORICAL BACKGROUND OF THE PRINCIPLE

The concept commonly referred to as “privacy by design” has not been formulated based on the European legal thought. Its roots must be traced back to Canada. There, in the 90-ies of XX c. Ann Cavoukian Ph.D., an Ombudsman for information and privacy at those times, postulated to include privacy protection principles into every stage of development for IT systems as well as business and technological processes in a wide understating of the term. The concept resulted from the outcomes regarding to the information circulation taking advantage of the new data processing technologies communication methods. They had a direct or direct impact over the pace of development for information society [1].

Ann Cavoukian assumed that privacy is a certain value which cannot be neglected in any projects adopted in public administration sector or business environments. The idea of privacy protection ought to remain an integral element of any project, regardless of its objectives or character.

The original assumptions for "privacy by design" evolved strongly at the turn of XX and XXI centuries in order to meet the needs of information society advocating its right to control private information as well as of progressing technological solutions in communications. The idea itself was described in 2009 in the publication entitled "Privacy by Design: Take the Challenge".

Privacy by design has gained popularity in no time and has become commonly acceptable within the environments dealing with personal data protection due to its simple assumptions supporting the process to formulate further, more detailed conclusions on privacy protection.

The "privacy by design" principle has been addressed by the resolution on privacy during the designing phase, passed by the 32nd International Conference for Commissioners for Data protection and Privacy held between 27th and 29th October 2010 in Jerusalem. The said resolution stipulates that the principles adopted into the "privacy by design" concept remain an indispensable element for privacy protection and should constitute the guidelines aiming at privacy protection as a default course of action within an organisation [5,6].

The principles included in the aforementioned resolution have been taken into account by the EU legislator in the general regulation on data protection, which will enter into force on 25th May 2018 [4].

3. PRIVACY BY DESIGN - THE RANGE OF THE TERM

The concept of "privacy by design" is a certain way of action based on several basic principles. Their application and introduction is intended to provide personal data protection at the stage of designing the solution to process the data. Privacy by design refers not only to IT and communications systems, but to marketing actions as well as any products and services directly or indirectly related to personal data processing [1].

The position elaborated during the 32nd Conference for Commissioners for Data Protection and Privacy must be paid special attention as well. Its participants then assumed that the "privacy by design" model is not attributed solely to designing the telecommunications solutions. It should also be included into the entire organisation management process. Currently, its application extends over any processes and is not limited to designing phase only. Privacy protection ought to be a default action along each and every stage of the project or process involving data processing [1].

The resolution also recognises the previously elaborated set of seven principles for privacy by design. Above all, privacy protection ought to have a proactive and preventive character.

Data controller should focus on taking any actions to prevent any situations leading to the infringements on privacy protection from occurring rather than take corrective measures once such incidents have occurred (Principle 1: Proactive not Reactive; Preventative not Remedial).

Privacy should be a default value for all participants taking advantage of a given solution. Nobody is supposed to be forced to take any additional actions in order to protect their own privacy (Principle 2: Privacy as the Default).

Privacy protection should be embedded into the process of designing and development of IT and business systems. It shall not be regarded as a disruptive additional but shall remain an integral part of the entire project and construction process for a given solution. Actions taken in order to provide privacy protection should not lead to a diminished functionality of a given solution (Principle 3: Privacy Embedded into Design).

The concept of "privacy by design" introduces the principle of, the so called, positive sum instead of "neutral sum". This means that it is possible to create a solution which will include all functionalities and will not have to compromise. The said principles is intended to avoid frequent disputes on privacy versus safety and proves that having both features at the same time is possible (Principle 4: Full Functionality—Positive-Sum, not Zero-Sum).

Privacy protection should be included into the product lifecycle, i.e. from a conceptual phase through developing and testing a given solution until production implementation and project liquidation. Each stage of the project should be analysed for personal data lifecycle with special emphasis put over data deletion process (Principle 5: End-to-End Lifecycle Protection).

Personal data processing should be characterised by full transparency. The concept "privacy by design" aims to ensure that all participants in the project lifecycle and project itself process the data in line with its objectives and assumptions, which can be subject to independent verification - „trust but verify" (Pricinple 6: Visibility and Transparency).

Data controllers shall predominantly bear in mind the fact that the solution to be created must be focussed on the solution users (Principle 7: Respect for User Privacy).

Implementation of the aforementioned principles by an organisation is frequently related to the introduction of numerous innovative solutions and procedures. They ought to be adjusted to the character and the scale of operation as well as to the information which is to be processed by an organisation. Taking into consideration the assumptions of privacy by design may increase the privacy protection level.

4. LEGAL REGULATIONS ON DATA PROTECTION BY DESIGN IN THE GENERAL DATA PROTECTION REGULATION

The new frameworks of data protection contained in the resolution of the European Parliament and Council (UE) 2016/679 of 27th April 2016 on protecting physical persons with regards to personal data processing and on free flow of such data as well as on lifting the Directive number 95/46/WE, i.e. the general data protection regulation (hereinafter referred to as gdpr), do not use the term "privacy by design" in a straightforward manner. The document also known as gdpr uses the term "data protection by design", which is identical in meaning with "privacy by design".

However, this does not mean that the aforementioned act does not address the issue of data protection during the designing phase or fails to impose the obligation to implement it over the data processing entities.

The obligation has been included into article 25 of gdpr, which sets forth the factor to be considered in order to provide privacy by design. Data controller ought to implement the

relevant technical and organisational measures in order to protect the data in a proper manner and, hence, meet the requirements stipulated by gdpr. Data controller shall take numerous factors into consideration such as technical knowledge, implementation costs, character, range , context as well as objectives for processing or a risk of an infringement on the rights and liberties of physical persons. It is possible to acknowledge the fact that the requirements imposed by gdpr are met by the implementation of an approved certification mechanism pursuant to article 42 of gdpr.

The said norm clearly indicates that data protection is to be included into the entity's operations at every stage of data processing in order to prevent problems from occurring and not to react to them afterwards.

Taking into account the range of the general data protection regulation, one must bear in mind that the range of factors and requirements which are to be included by a data controller is very wide and encompasses, but is not limited to, the fulfilment of information duties, documentation obligation, risk assessment or procedures on the cases of data protection infringements (incidents) [7-14].

5. CONCLUSIONS

Privacy by design is based on several general principles which may seem too extensive, ambiguous and hard when being applied [2]. However, comprehension of the "privacy by design" principles and applying them in practice by a data processing entity along the entire process of data processing will, without a doubt, contribute to enhanced level of privacy protection.

Acting in accordance with the said concept will ameliorate the process of accountability assurance, as a data controller will be able to confirm that they have taken real steps towards the implementation of proper technical and organisational means to counteract to personal data infringements [3].

The concept of "privacy by design" in the gdpr has one major disadvantage – it fails to refer to the entities that do not act as data controllers nor processors nor data recipients. This means that the manufacturers of some electronic devices will neglect the requirements related to privacy protection and may avoid responsibility pursuant to the gdpr provisions [2].

References

[1] Cavoukian, A. Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. *IDIS* 3 (2010) 247. doi:10.1007/s12394-010-0062-y

[2] Demetrius Klitou, Privacy-Invading Technologies and Privacy by Design. The Value, Safeguarding Privacy, Liberty and Security in the 21st Century. T.M.C. Asser Press, The Hague, 2014. doi:10.1007/978-94-6265-026-8_9

[3] Ilten, C., Kroener, I., Neyland, D., Postigo, H., Managing Privacy through Accountability, Palgrave Macmillan UK, 2012. doi:10.1057/9781137032225

[4] C. Easton, Information Systems for Crisis Response and Management: The EU Data Protection Regulation, Privacy by Design and Certification. Proceedings of the ISCRAM 2016 Conference - Rio de Janeiro, Brazil, May 2016

[5] M. Colesky, S. Ghanavati. Privacy Shielding by Design — A Strategies Case for Near-Compliance. *Requirements Engineering Conference Workshops (REW). IEEE International*, pp. 271-275, 2016.

[6] P. Blume. Will it be a better world? The proposed EU Data Protection Regulation. *International Data Privacy Law*, Volume 2, Issue 3, 1 August 2012, Pages 130-136.

[7] James Lee Jr., Merrill Warkentin, Robert E. Crossler, Robert F. Otondo. (2017) Implications of Monitoring Mechanisms on Bring Your Own Device Adoption. *Journal of Computer Information Systems* 57: 4, pages 309-318.

[8] Nigel Martin, John Rice, Robin Martin. (2016) Expectations of privacy and trust: examining the views of IT professionals. *Behaviour & Information Technology* 35: 6, pages 500-510.

[9] Shuk Ying Ho, Patrick Y. K. Chau. (2013) The Effects of Location Personalization on Integrity Trust and Integrity Distrust in Mobile Merchants. *International Journal of Electronic Commerce* 17: 4, pages 39-72.

[10] Ruidong Zhang, Jim Q. Chen, Ca Jaejung Lee. (2013) Mobile Commerce and Consumer Privacy Concerns. *Journal of Computer Information Systems* 53: 4, pages 31-38.

[11] Shiu-Wan Hung, Min-Jhih Cheng, Pei-Che Chen. (2012) Reexamining the Factors for Trust in Cultivating Online Customer Repurchase Intentions: The Moderating Effect of Perceived Waiting. *International Journal of Human–Computer Interaction* 28: 10, pages 666-677.

[12] Alexander Benlian, Thomas Hess. (2011) The Signaling Role of IT Features in Influencing Trust and Participation in Online Communities. *International Journal of Electronic Commerce* 15: 4, pages 7-56.

[13] Paul Benjamin Lowry, Jinwei Cao, Andrea Everard. (2011) Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures. *Journal of Management Information Systems* 27: 4, pages 163-200.

[14] Bin Mai, Nirup M. Menon, Sumit Sarkar. (2010) No Free Lunch: Price Premium for Privacy Seal-Bearing Vendors. *Journal of Management Information Systems* 27: 2, pages 189-212.

(Received 12 August 2017; accepted 30 August 2017)