World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:12, No:01, 2018

Analyzing the Risk Based Approach in General Data Protection Regulation: Basic Challenges Connected with Adapting the Regulation

Authors : Natalia Kalinowska

Abstract : The adoption of the General Data Protection Regulation, (GDPR) finished the four-year work of the European Commission in this area in the European Union. Considering far-reaching changes, which will be applied by GDPR, the European legislator envisaged two-year transitional period. Member states and companies have to prepare for a new regulation until 25 of May 2018. The idea, which becomes a new look at an attitude to data protection in the European Union is risk-based approach. So far, as a result of implementation of Directive 95/46/WE, in many European countries (including Poland) there have been adopted very particular regulations, specifying technical and organisational security measures e.g. Polish implementing rules indicate even how long password should be. According to the new approach from May 2018, controllers and processors will be obliged to apply security measures adequate to level of risk associated with specific data processing. The risk in GDPR should be interpreted as the likelihood of a breach of the rights and freedoms of the data subject. According to Recital 76, the likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. GDPR does not indicate security measures which should be applied – in recitals there are only examples such as anonymization or encryption. It depends on a controller's decision what type of security measures controller considered as sufficient and he will be responsible if these measures are not sufficient or if his identification of risk level is incorrect. Data protection regulation indicates few levels of risk. Recital 76 indicates risk and high risk, but some lawyers think, that there is one more category – low risk/now risk. Low risk/now risk data processing is a situation when it is unlikely to result in a risk to the rights and freedoms of natural persons. GDPR mentions types of data processing when a controller does not have to evaluate level of risk because it has been classified as „high risk" processing e.g. processing on a large scale of special categories of data, processing with using new technologies. The methodology will include analysis of legal regulations e.g. GDPR, the Polish Act on the Protection of personal data. Moreover: ICO Guidelines and articles concerning risk based approach in GDPR. The main conclusion is that an appropriate risk assessment is a key to keeping data safe and avoiding financial penalties. On the one hand, this approach seems to be more equitable, not only for controllers or processors but also for data subjects, but on the other hand, it increases controllers' uncertainties in the assessment which could have a direct impact on incorrect data protection and potential responsibility for infringement of regulation.

Keywords : general data protection regulation, personal data protection, privacy protection, risk based approach
Conference Title : ICISDP 2018 : International Conference on Information Security and Data Protection
Conference Location : Zurich, Switzerland
Conference Dates : January 15-16, 2018