Proceedings of the 33rd International Conference on Information Technologies (InfoTech-2019)
19-20 September 2019, Bulgaria

ISO 27552 AS A MODEL FOR ESTABLISHMENT PERSONAL INFORMATION MANAGEMENT SYSTEMS

Digest of paper[1]

Tzanko Valkov Tzolov

Member of the Commission for Personal Data protection
tzolov@cpdp.bg
Bulgaria

Abstract: Technological changes and globalisation have dramatically changed the way personal data are processed. It takes time to understand the legal bases for data processing, auditing and confidentiality rules, and it cannot be easily verified that people's personal data are processed legally. Using a model for compliance with GDPR requirements turns data controllers from mere consumers of consultancy services into managers of the privacy protection system. ISO 27552 is the upgrade which gives the information security system a completely new status, transforming it into a privacy protection system.
Key words: GDPR, ISO 27552, model, PIMS, Business Analysis, Data Flow, Gap Analysis.

INTRODUCTION

The digital world we live in needs a strong set of rules to ensure that the traces we leave are not used in violation of the Charter of the fundamental rights and those of the European Union. This set of rules fosters citizens' trust and greatly affects the competitiveness of individual companies. Trust is a strategic competitive advantage in the battle for markets and clients. Technological changes and globalisation have dramatically changed the way personal data are processed and have turned them into a valuable asset for organisations.

The European Commission has made a fundamental reform of the EU data protection legal framework by adopting Regulation 2016/679 (General Data Protection Regulation) (GDPR) and Directive 2016/680 concerning police and judicial cooperation in criminal matters.

[1] The full paper is proposed for including in the IEEE Xplore Digital Library

The business diversity and the different ways of personal data processing prevent the standardisation of the protection system, where specific solutions are expected to be taken by the data controllers by analysing their business processes and taking into account potential risks.

With the abolition of the authorisation regime and the registration requirement, the initial confidence in the correct enforcement of the regulations was lost. The Regulation introduced a regime with defined regulatory constraints on data processing, but without a mechanism for the initial assessment of the measures taken by administrators for its correct implementation. At the same time, taking into account this uncertainty and realising the scale of the problem, organisations have incurred astronomical costs [1] in order to achieve compliance with GDPR, e.g. over $ 150 billion [2] for the US market. On the other hand, organisations are investing considerable resources in staff who are directly responsible for achieving compliance with the Regulation. According to a recent IAPP (International Association of Privacy Professionals) salary survey, a DPO's average salary in Europe is $ 88,000.

As Information Commissioner's Office (ICO) has acknowledged, this considerable financial resource is unbearable for small and medium-sized enterprises and they are forced to use the services of the hastily established market for consultancy services that lacks sufficient expertise. It takes time to understand the legal bases for data processing, auditing and confidentiality rules, and it cannot be easily verified that people's personal data are processed legally. It is considerably more difficult for sole proprietors. [3]

Developing a global, comprehensive model that organisations can use to implement GDPR would generally support the process and provide the missing confidence in the steps taken by data controllers. The idea was presented as a conceptual model at the IntoTech Conference in September, 2018. [4]

REFERENCES

[1] GDPR After One Year: Costs and Unintended Consequences, Alec Stapp — 24 May 2019, https://truthonthemarket.com/2019/05/24/ gdpr-after-one-year-costs-and-unintended-consequences/

[2] Fortune / Daniel Castro and Michael McLaughlin, https://fortune.com/2018/05/23/gdpr-compliant-privacy-facebook-google-analytics-policy-deadline/

[3] GDPR One year Later, Information Commissioner's Office (ICO), UK

[4] Implementation of the general data protection regulation in organizations based on ISO standards, Tzanko Tzolov, Communication & Cognition Vol. 52, Nr. 1 & 2 (2019), Belgaum

[5] BABOK, V3, A Guide to the Business Analysis Body of Knowledge, International Institute of Business Analysis

[6] ISO/IEC 27552 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines, Draft BS