Gdansk 10th November 2022.

SUMMARY OF THE DOCTORAL DISSERTATION

Legal instruments for assessing the correctness of personal data processing in the aspect of standardisation

Author of the thesis: Tomasz Soczyński, MA
Supervisor: Wojciech Wiewiórowski, Ph.D. habilitated

University of Gdansk
Faculty of Law and Administration

The pace of technological changes as well as the massive nature of personal data processing using information and communication technologies raise new challenges for ensuring data security in the course of their processing. Legislating in a manner that reconciles the obligatory nature of the legal standard (mandating the fulfilment of the legal provision wording) with voluntary application of the technical standard (choosing how to meet certain standardisation norms) is one way of reflecting technological progress in the legal order.

The main objective of the following dissertation is to demonstrate the need to take into account standardisation norms in the legal instruments used to assess the correctness and modelling of personal data processing. It is therefore expedient to relate the legal instruments introduced by the provisions of GDPR to the possibility as well as the need to refer to technical standards, to review the standards relevant to such instruments, to establish the relationship between the compliance requirements of the solutions provided for in the provisions of GDPR and the relevant technical standards. The main objective is supported by the legitimacy of the development with regards to technical standards-based conformity assessment tools (codes of conduct, personal data impact assessment, certification mechanisms and data protection by design), with particular emphasis being put on the role of personal data protection impact assessment (DPIA) and to show examples of exemplary DPIA use within the framework for assessment of regulatory effects with regards to the designed legal solutions.

The rationale for the choice of the dissertation topic, the purpose of the dissertation, the definition of the subject matter of the research, the presentation of the research hypothesis and

the research methods are contained in Chapter 1. The basic concepts of the legal instrument, privacy, personal data protection and the changing approach to such data are discussed in Chapter 2.

Chapter 3 is devoted to selected issues in the field of standardisation, including a reference to the definition of a standard, types of standards, the process of their creation, levels of standardisation, the importance of European and national standardisation and an overview of global standardisation organisations. This chapter considers the problem of how the legal system responds to technological changes, to the updating of technical standards and the issue of referencing standards in legislation.

In Chapter 4, the essence of the new approach to personal data protection is characterised on the basis of the GDPR provisions. Personal data protection is treated as one of the processes in an organisation, managed according to the technical standards of the ISO family, taking into account the level of quality and compliance management in the organisation and the level of risk management and data security.

Chapter 5 analyses the interplay between the application of legal data protection instruments and technical standards, highlighting the role of the personal data controller and processor, IT security criteria, the privacy framework, ensuring data security adequate to the risks involved, records of processing activities as a pre-control function and prior consultation with the supervisory authority.

Chapter 6 deals with the application of self-regulatory mechanisms using technical standards suitable for codes of conduct and certification as well as outlines the process for the implementation of such ones.

Chapter 7 discusses the use of DPIA based on standards and guidelines, how to mitigate risks in data processing, how to support the implementation of DPIA by supervisory authorities in the EU and their recommended tools to support DPIA.

Chapter 8 is devoted to better lawmaking at European and national level and the role of regulatory impact assessment (IA). The enforcement of the obligation to carry out DPIA as part of the preparation of IA for seven drafts of legislation in which provisions require the personal data processing is analysed. This practice has been contrasted with the experience of carrying out DPIA and regulatory IA in European countries.

Chapter 9 presents a solution to the research problem in the form of the author's proposal for a DPIA model for IA purposes to enforce the content of a legal standard based on international technical standards.

The deliberations end with remarks and conclusions in Chapter 10, summarising the results of considering the problem of legal instruments to assess the correctness of personal data processing in the aspect of standardisation, with particular emphasis on the need to carry out DPIA at the stage of designing legal solutions related to the personal data processing and protection.