STUDIA PRAWA PUBLICZNEGO
STUDIES IN PUBLIC LAW
2020 • No. 2 (30)

ALEKSANDRA PYKA

Data protection impact assessment

Summary

This article deals with the issue of impact assessment for the protection of personal data. This is a new obligation for the controller. The article presents the essence of impact assessment (DPIA), exclusion from the obligation to carry it out, the prerequisite for mandatory DPIA, the role of the data protection officer and the powers of the supervisory authority. The analysis of legal provisions related to the impact assessment presented here does not refer to specific situations, due to the wide scope for interpreting specific phrases contained in the General Regulation. Nevertheless, the article discusses the issue of conducting data protection impact assessments as one of the most problematic obligations incumbent on the controller, who in practice raises many doubts. The DPIA has been imprecisely regulated by the EU legislator, thus leaving controllers plenty of leeway to interpret the terms used in the General Regulation. In addition, carrying out a DPIA in practice (as a new obligation on entities setting the purposes and means of data processing) can be problematic due to the lack of harmonized methods for conducting a data protection impact assessment. However, controllers cannot assign DPIA implementation to other entities involved in data processing, such as an entity processing personal data on behalf of another. Entities setting the purposes and methods of data processing should not only take into account the provisions of the General Regulation but also a list of data processing operations that are obligatorily subject to DPIA. Controllers fulfilling the obligation to carry out a data protection impact assessment will be obliged by the supervisory authority to demonstrate how to carry out a data protection impact assessment.

Keywords: data protection impact assessment – DPIA – data controller – risk – personal data