Chapter 86
Erosion by Standardisation:
Is ISO/IEC 29134:2017 on Privacy Impact Assessment Up to (GDPR) Standard?

Athena Christofi
https://orcid.org/0000-0002-4506-6324
KU Leuven, Belgium

Pierre Dewitte
https://orcid.org/0000-0003-4204-7467
KU Leuven, Belgium

Charlotte Ducuing
https://orcid.org/0000-0003-1160-0637
KU Leuven, Belgium

Peggy Valcke
https://orcid.org/0000-0002-8456-430X
KU Leuven, Belgium

ABSTRACT

This chapter examines the interplay between the GDPR and parallel private regulation in the form of privacy-related standards adopted by the International Organisation for Standardisation (ISO). Focusing on the understanding of 'risks' in the GDPR and ISO respective ecosystems, it compares the GDPR requirement for Data Protection Impact Assessments (DPIAs) with ISO/IEC 29134:2017, a private standard on Privacy Impact Assessment explicitly referred to by EU Data Protection Authorities as relevant in the context of DPIA methods. The resulting gap analysis identifies and maps misalignments, critically reflecting on whether the parallel form of ISO regulation, in the context of DPIAs, could support or rather blurs GDPR's objective to protect fundamental rights by embracing a risks-based approach.

DOI: 10.4018/978-1-7998-8954-0.ch086

INTRODUCTION

In the era of relentless technological developments with an ambivalent potential to both advance the common good and undermine individuals' rights and freedoms, regulating the processing of personal data is by no means a simple task. Focusing on the European Union ('EU') legal order, this Chapter explores the interplay between the General Data Protection Regulation ('GDPR'),[1] including GDPR-based soft-law instruments, and 'private' regulatory instruments of data processing adopted over the past years, such as ISO standards in the field of privacy. At the centre of the analysis is the risks-based approach enshrined in the GDPR, which culminates with the obligation to conduct a Data Protection Impact Assessment ('DPIA') in cases of high-risk processing. At the same time, risks-based methodologies are also at the core of privacy-related standards adopted by the International Organization for Standardisation ('ISO'). The Chapter juxtaposes the two strands of regulation focusing on the provisions of the GDPR on DPIAs on the one hand, and ISO's counterpart ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment (hereinafter ISO/IEC 29134) on the other. By mapping misalignments, the aim is to assess and critically reflect on whether the parallel form of ISO regulation could support or rather blurs the GDPR's objective to protect fundamental rights by embracing a risks-based approach.

The Chapter falls into three main parts. The first part revolves around the GDPR's regulatory model for data protection, laying out regulatory challenges and the solutions envisaged by the EU legislator. It begins with what constitutes a major challenge for today's regulators: the pacing problem of the law in light of constant technological developments. In the authors' view, any critical analysis of the regulation of privacy and data protection should acknowledge this challenge and the fact that it can put to test the traditional 'command and control' regulatory model to favour 'new' regulation focused on risk and on a decentralised approach. Second, it lays down the key regulatory characteristics of the EU data protection legal framework, namely: (i) GDPR's omnibus nature and fundamental rights objective; (ii) the law's focus on general data processing principles that ought to be operationalised by regulated entities on a case by case basis and; (iii) the risks-based approach coupled with the accountability principle. It explains that, while those characteristics were devised with the desire to bring regulatory flexibility, they may impact legal certainty as regulated entities are faced with broad notions whose scope and incumbent obligations may be unclear. The Chapter then argues that the lack of legal certainty has been acknowledged by the EU legislator, even if perhaps only implicitly. The third section introduces the soft law tools foreseen under the GDPR, which are expected to supplement and consolidate the latter's objectives by providing guidance on how to achieve compliance. It sketches the characteristics of the GDPR's co-regulatory model and limitations of the envisaged soft law tools that one may already see three and a half years after the Regulation's adoption and one and a half year after its entry into force.

The second part explores the emergence and pitfalls of the parallel form of private regulation through ISO privacy-related standards, notably ISO/IEC 29134. With the GDPR co-regulatory model still in its infancy, it is indeed extra-GDPR soft law instruments that keep gaining traction. Because of their worldwide recognition and fast development, ISO standards can be particularly popular amongst companies as a means to demonstrate compliance with the GDPR. The sheer amount of work on privacy-related standards by ISO over the past few years echoes businesses' growing concern for data protection and need for tools to orient their compliance efforts. After a brief introduction to ISO and its standardisation work, the Chapter discusses ISO's willingness to play a role as a relevant actor in the regulation of privacy and data processing globally – more importantly in the EU market – as well as Article 29