Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

A risk to a right? Beyond data protection risk assessments

Niels van Dijk [a,*], *Raphaël Gellert* [a], *Kjetil Rommetveit* [b]

[a] *Research Group on Law, Science, Technology & Society, Vrije Universiteit, Brussels, Belgium*
[b] *Centre for the Study of the Sciences and the Humanities, University of Bergen, Bergen, Norway*

Keywords:
Data protection impact assessment
Privacy impact assessment
Risk assessment
Risk management
Risk
Rights
Data protection
Privacy
Public participation
Legal expertise

A B S T R A C T

The proposal for a new European Data Protection Regulation introduces the novel obligation of performing data protection assessments. Since these assessments will become a mandatory exercise for those in control of data processing systems, they will become an important apparatus for the governance of new and emerging information technologies. This tool, and in particular the notion of "risks to the rights and freedoms of data subjects" which is at its core, epitomises the shift from classical legal practice to more risk-based approaches. Merging risks and rights in the proposed fashion could change their meanings into something hardly predictable. This contribution proposes to explore the nature of the relation between both concepts within the assessment of a "risk to a right". It will start by mapping out the various relations that exist between risks and rights in different practices. This should serve to identify gaps in the way DPIAs are currently operationalised and might well determine whether the introduction of this methodology in its current form might itself pose a risk to the rights of privacy and data protection. In turn however, it can provide opportunities for improvement and for lessons to be drawn from other practices and expertise that strike different relations between risks and rights, like the ones found in environmental governance and courts.

1. Introduction

In January 2012 the European Commission (EC) initiated the reform process of the European Union (EU) personal data protection legislation by tabling a proposal for a so-called General Data Protection Regulation (GDPR), which is meant to replace the existing Data Protection Directive created in 1995.[1] In March 2014 the European Parliament formally adopted a compromise text of this Regulation. In June 2015 the Council of the European Union approved its own draft and in December 2015 the Commission, Parliament and the Council agreed on a

Niels van Dijk and Raphaël Gellert are members of the Research Group on Law, Science, Technology & Society, Law & Criminology Department, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium.

Kjetil Rommetveit is associate professor at the Centre for the Study of the Sciences and the Humanities, Postboks 7805, 5020 Bergen, Norway.

* *Corresponding author.* Research Group on Law, Science, Technology & Society, Law & Criminology Department, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium. Tel.: +32488579011.

E-mail address: nvdijk@vub.ac.be (N. van Dijk).

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050. (Hereafter: "the Data Protection Directive of 1995").

http://dx.doi.org/10.1016/j.clsr.2015.12.017

common (inofficial) version, which will probably be approved early 2016.[2] Among its many novelties, the proposed Regulation introduces the notion of data protection impact assessments (DPIAs).[3]

In this introductory section we will describe the risk-based nature of the data protection impact assessment and set out the conceptual and institutional challenges it represents. These challenges revolve around the central notion of assessing the risks to the rights of data subjects. What changes does the introduction of risk-based tools bring about in comparison to legal definitions of risks and rights? Who will get to decide what such a "risk to a right" means and according to which methodologies and principles? What kind of knowledge should be drawn upon, and who should be included in such processes? What lessons can be drawn from other practices with experience in striking a relation between risks and rights?

The article is the result of interdisciplinary research into different forms of technology and impact assessments, against which DPIAs will be situated.[4] Drawing upon historical sources, legal scholarship, sociology of science and risk studies, we will outline a typology of risk–right relations and the different institutional settings in which they are embedded: governments, large organisations and corporations, courts, and civil society. We use these to draw lessons about the role for public participation and legal practice in these new and emerging assessments.

1.1. *Data protection impact assessments and privacy impact assessments*

The DPIA is inscribed in article 33 of the Regulation, which states that:

> "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk for the rights and freedoms of individuals, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (EP & CEU 2015)".

The proposed Regulation introduces the DPIA in very general terms for several data processing technologies. DPIAs shall be mandatory for the data controller in certain stipulated circumstances that are likely to present specific risks. The Regulation further prescribes the minimal set of elements that a DPIA should contain (i.e., description of the processing operation, assessment of the risks, remedial measures taken). The provision thus lays the legal ground for DPIAs, but does not provide further guidance.

In parallel, two sector-specific documents have already concretised the assessment processes for two concrete technologies. The first is the industry-proposed Privacy Impact Assessment and Data Protection Impact Assessment Framework (DPIAF) for RFID applications (2010),[5] the second is the DPIA template for smart grid and smart metering systems proposed by the Expert Group (EG2) from the EC's Smart Grids Task Force (2013).[6] Both documents have been commented upon by the article 29 Working Party,[7] which in turn led to revisions. Important points of reference in these documents are the ENISA Position paper on the RFID (D)PIAF and the CNIL Methodology for Privacy Risk Management.[8] All these instruments consider the same elements of the Data Protection Directive of 1995, yet the manner in which the relevant threats are operationalised within the actual impact assessment varies from one document to another.

The data protection impact assessment (DPIA) to be introduced by the new Regulation is a newcomer in the impact assessment vocabulary. On the one hand, it has no direct previous historical lineage and in this sense refers to aspects that are specific to the EU context. On the other hand, it could be argued that it shares many similarities with the field of privacy impact assessment (PIA), which progressively developed from the 1990s onwards, predominantly in Anglo-Saxon countries.[9] These assessments, in turn, had important historical precursors in technology assessments (TA) and environmental impact assessments (EIA) (Clarke, 2009). There is a consolidated and growing literature on privacy impact assessments,[10] including manuals and guidance documents by expert authors, DPAs and other bodies,[11] which seems to constitute an obligatory reference point for DPIAs.

A privacy impact assessment (PIA) can be defined in different ways, depending on different legislatures, organisational

[2] Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Inofficial version, 15 December 2015, Hereafter: "Regulation (EP & CEU 2015)".

[3] The current EU legal regime (the Data Protection Directive) contains no provisions on impact assessments. The directive does however provide for prior checking (which some have qualified as forerunners of DPIAs), and some have argued that a broad interpretation of Art. 17 could provide a legal basis for (D)PIAs.

[4] The research is based on the European (FP 7) project EPINET, at: http://www.epinet.no

[5] Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011.

[6] European Commission, Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, 2014/724/EU, OJ L 300, 18.10.2014, pp. 63–68.

[7] Article 29 Working Party (2010; Article 29 Working Party (2013).

[8] ENISA (2010) and CNIL (2012). These include the principles concerning the data processing as such (purpose specification, data quality, minimisation, etc.), the data subjects' rights (access, objection, transparency. . .), technical and organisational measures, etc.

[9] It must be noted however that the drawing of such similarities and differences between these two different tools is itself a hot topic of current debate with regard to determining and demarcating the topic and scope of the assessments at stake. According to De Hert, the DPIA for instance seems like a mere compliance check of legal requirements (De Hert, 2012), whereas a PIA investigates broader privacy implications like "how information flows affect individuals' choices, the degree of intrusiveness into individuals' lives, how the project fits into community expectations" (Wright and De Hert, 2012, p. 6).

[10] See: Clarke (2009, 2011); (Linden Consulting, Xama Consultancy, University of Bristol, 2007); Wright (2012); Wright and De Hert (2012).

[11] Like ICO, ENISA, CNIL and ISO 27005.