Technology and Regulation

What could possibly go wrong?

On risks to the rights and freedoms of natural persons in EU data protection law, their typologies and their identification

Author(s)	Dariusz Kloza, Thibaut D'hulst and Malik Aouadi
Contact	dariusz.kloza@uclouvain.be, tdhulst@vbb.com, maouadi@vbb.com
Affiliation(s)	D. Kloza, UCLouvain Saint-Louis Bruxelles (chargé de recherche FNRS), Van Bael & Bellis (VBB); T. D'hulst, VBB; M. Aouadi, VBB

Keywords	data protection, risk-based approach, risk to the rights, data protection impact assessment		
Published	**Received**: 21 Aug. 2024	**Accepted**: 12 Dec. 2024	**Published**: 20 Jan. 2025
Citation	Dariusz Kloza, Thibaut D'hulst and Malik Aouadi, What could possibly go wrong? On risks to the rights and freedoms of natural persons in EU data protection law, their typologies and their identification, Technology and Regulation, 2024, 309-329 • https://doi.org/10.26116/techreg.2024.022 • ISSN: 2666-139X		

Abstract

The risk-based approach is a pillar of EU data protection law, mandating data controllers and processors to adapt their obligations to reflect the level of risk to the rights and freedoms of natural persons. Despite clear aims of strengthening data protection, accommodating diverse interests and providing greater flexibility in complying with the law, understanding and assessing this risk presents particular conceptual and practical challenges. This paper seeks to clarify these issues to improve legal compliance and safeguard fundamental rights. First, it scrutinizes the nature of such risk and its assessment, examines related concepts, like damage, and explores inherent problems. Next, it expands the understanding of such risk by introducing a broader, more comprehensive construct of 'negative consequences', provides concrete, precise examples and proposes their typology. Subsequently, it presents a method for efficiently identifying these consequences, i.e., an inventory with complementary classification criteria. It concludes by discussing the applicability of our findings in sister domains of law and suggesting further research.

1. Introduction

The risk-based approach (RBA) is a pillar of European Union (EU) data protection law, requiring data controllers and data processors to adapt their obligations to the level of risk to the rights and freedoms of natural persons that their processing operations might present. Aiming to strengthen the protection of personal data, accommodate diverse interests and provide greater flexibility in legal compliance, the RBA nonetheless presents conceptual and practical challenges, starting with understanding and assessing such risk. In other words, one of the key challenges is that of insufficient clarity as to what exactly risk is and how to identify the risks that are relevant for a given intended processing operation. The implications for fundamental rights, coupled with the significance of the RBA in the General Data Protection Regulation (GDPR, the Regulation),[1] underline the importance of addressing these problems. Despite existing extensive theoretical literature on risk in EU data protection law, there is a noticeable gap concerning the practice of risk and its identification as only very few attempts have been thus far made to, e.g., comprehensively enumerate such risks.

This paper aims to fill this knowledge gap. It clarifies the concept of risk in EU data protection law and – more specifically, in the GDPR terminology – the risk to the rights and freedoms of natural persons (*hereafter*: risk to the rights). It further proposes a typology and a method for an efficient identification of such risks.

This paper is structured as follows: after this introduction, in Section 2, for background information, we synthesise what is already known about risk to the rights and its assessment in EU data protection law. While the GDPR does not specifically define it, textual analysis of the Regulation nonetheless provides some indication of its parameters and assessment methods. As the GDPR also uses several related concepts, such as damage and infringement, we relate these to that of risk. Finally, we provide an overview of some problems related to risk and its identification, such as the relationship between compliance risk and the risk to the rights, and whether risk identification is an obligation of means or an obligation of result (i.e., fault-based liability or strict liability).

In Section 3, we elaborate on the understanding of risk to the rights through the identification of its examples and through its classifications (e.g., typologies). Since what could possibly go wrong with the processing of personal data extends beyond the scope of a risk to the rights, we introduce a broader construct of 'negative consequences'. Furthermore, since these consequences need to be defined and described in sufficient detail to be appropriately assessed, we seek out precise, concrete examples in relevant academic and professional literature as well as legislation and the jurisprudence of the Court of Justice of the EU (CJEU, the Court). We then review the many attempts to classify these consequences, suggesting a synthesised typology.

In Section 4, we turn to practical application and lay the foundation for a method to efficiently identify negative consequences that may be caused by the processing of personal data. Acknowledging the shortcomings of risk identification with the aid of the typologies mentioned above, we propose developing an inventory (database) with a complementary classification method. This database would be updated as technology, economy and society develop. We propose to classify (tag) each entry in the database with multiple descriptors of certain characteristics, e.g., the type of data subject (if vulnerable, the type of vulnerability). This allows – for example, during a data protection impact assessment (DPIA) process – for easy filtering for negative consequences that an intended processing operation might pose.

Finally, in Section 5, we offer some suggestions for the application of our method in sister domains of law as well as for further research.

This paper contributes to a more complete understanding of risks to the rights – or, more broadly, of negative consequences – and to the efficiency of their identification, leading to potential improvements in legal compliance and in the level of fundamental rights protection. Consequently, it is addressed predominantly to data protection lawyers and other practitioners in the field, and to policymakers to facilitate their work on the protection of personal data and legal compliance. Practitioners could use it as a manual to help them identify what could possibly go wrong with their envisaged data processing operations. In parallel, policymakers could use it to evaluate the functioning of the RBA.

This paper reflects the law as it stood on 31 July 2024. Legal references and the jurisprudence quoted without any further specification relate to the GDPR and the CJEU, respectively.

[1] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1. The GDPR is directly applicable in the EU and – by virtue of the European Economic Area (EEA) Agreement – also in Norway, Iceland and Liechtenstein. The United Kingdom (UK) after Brexit has retained, with necessary adaptations, the GDPR – as the 'UK GDPR' – until its own reform of data protection law takes place; cf. <https://www.legislation.gov.uk/eur/2016/679>. Unless explicitly mentioned otherwise, any reference to the EU shall be understood also as a reference to the EEA, possibly also covering the UK.

2. Key characteristic features of risk under EU data protection law

2.1 Context: risk, risk-based approach and DPIA

The RBA serves as a central pillar of EU data protection law. In a nutshell, the RBA requires both data controllers and data processors to calibrate their legal obligations to the level of risk that their data processing operations might pose to the rights and freedoms of natural persons. The RBA functions on the premise that the higher the level of risk, the more stringent the measures controllers and processors need to take to appropriately address it.

This innovative approach was introduced by the first reform of EU data protection law (2010),[2] which approached risk regulation, introducing the concept of risk to the rights as a sub-category of risk in general.[3] By way of background, risk regulation aims to "channel technological development and uses as they occur rather than responding to harms after the fact. [...] That is, we *choose* to take risks (albeit preferably minimized ones); we choose, by contrast, to *avoid* harms".[4] The aim was to enhance the overall level of protection of personal data while simultaneously allowing greater flexibility to controllers and processors to meet their legal obligations, all while adapting to technological, economic and societal shifts. From a society perspective, the RBA was introduced to appropriately balance various societal interests, such as innovation and the protection of fundamental rights.[5] However, the RBA carries several difficulties, both conceptual and practical, ranging from the understanding of the basic concepts (e.g., what *exactly* is risk?) to methodological challenges (e.g., how *exactly* to identify and assess risk?).[6] Particularly with regard to these two challenges, we have observed that there is insufficient clarity as to what exactly risk is and how to identify those risks that are relevant for a given envisaged processing operation. This is largely due to the novelty of the RBA in EU data protection law, coupled with the shortage of experience[7] in dealing with risks to the rights, and limited professional commentary,[8] authoritative guidance[9] and oversight.

[2] European Commission, 'A comprehensive approach on personal data protection in the European Union', Brussels, 04.11.2010, COM(2010) 609 final.

[3] Claudia Quelle, 'The "Risk Revolution" in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too' in Ronald Leenes and others (eds), *Data Protection and Privacy: The Age of Intelligent Machines* (Hart 2017) 33 <http://ssrn.com/abstract=3000382> accessed 3 September 2024.

[4] Margot E. Kaminski, 'The Developing Law of AI: A Turn to Risk Regulation' (2023) *The Digital Social Contract: A Lawfare Paper Series* (2) <https://www.lawfaremedia.org/article/the-developing-law-of-ai-regulation-a-turn-to-risk-regulation> accessed 3 September 2024. Cf. also Christopher C. Hood, Henry Rothstein and Robert Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes* (Oxford University Press 2001) 3.

[5] Giovanni De Gregorio and Pietro Dunn, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (2022) 59(2) *Common Market Law Review* 473.

[6] Controllers and processors equally encounter such difficulties when they fulfil other risk-based obligations stemming from EU data protection law. In the GDPR, beyond the DPIA, these comprise, for the sake of comprehensiveness, from the viewpoint of a controller and/or processor: general responsibilities of data controllers (Article 24), data protection by design and default (Article 25), conditions for the appointment of a representative of a controller (Article 27), data security (Article 32), data breach notifications (Articles 33-34), tasks of a data protection officer (DPO; Article 39), consent as a derogation for international personal data transfers (Article 49(1)(a)) as well as with regard to the small and medium enterprises (SME) exemption in the records of processing operations (Article 30(5)). Furthermore, the legislature (EU or Member State) shall consider risk when restricting data subject rights (Article 23(2)(g)) and data protection authorities (DPAs) need to assess risk when they raise a relevant and reasoned objection (RRO) (Article 4(24)). In addition, both national DPAs and the European Data Protection Board (EDPB) are empowered to, broadly speaking, inform about the risk (Articles 57(1)(b) and 70(1)(h), respectively).

[7] Jennifer Stoddart, 'Auditing Privacy Impact Assessments: The Canadian Experience' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer 2012) 419–436; Dariusz Kloza and others, 'The Concept of Impact Assessment' in J. Peter Burgess and Dariusz Kloza (eds), *Border Control and New Technologies* (Academic & Scientific Publishers 2021) 35-36 <https://doi.org/10.5281/zenodo.5121680> accessed 1 September 2024.

[8] E.g. Dariusz Kloza and others, 'Towards a Method for Data Protection Impact Assessment: Making Sense of GDPR Requirements' (VUB 2019) <https://cris.vub.be/files/48091346/dpialab_pb2019_1_final.pdf> accessed 1 September 2024; Dariusz Kloza and others, 'Data Protection Impact Assessment in the European Union: Developing a Template for a Report from the Assessment Process' (VUB 2020) <https://cris.vub.be/files/53602836/dpialab_pb2020_1_final.pdf> accessed 1 September 2024; Nicholas Martin and others, *Die Datenschutz-Folgenabschätzung Nach Art. 35 DSGVO: Ein Handbuch für die Praxis* (Fraunhofer Verlag 2020) <http://publica.fraunhofer.de/documents/N-586394.html> accessed 1 September 2024.

[9] E.g., Article 29 Working Party (WP29), 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' (2017) <https://ec.europa.eu/newsroom/article29/items/611236> accessed 7 September 2024; European Union Cybersecurity Agency (ENISA), 'Interoperable EU Risk Management Toolbox' (2023) <https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox> accessed

The first challenge of the RBA is the very understanding of the concept on which the entire approach is constructed, namely, risk. Despite its long history, contemporary importance and ubiquity, risk is not a clear-cut concept. On the contrary, it remains an essentially contested concept, to the extent that some commentators even suggest that it suffers from 'identity crisis' as in each of its domains of practice it can have a (slightly) different yet equally legitimate meaning.[10] Nonetheless, extensive scholarly discourse has been dedicated to it,[11] spanning from its historical roots[12] to social approaches to risk (e.g., risk society),[13] to various aspects of risk governance,[14] including its contemporary significance – most recently – in the realm of data protection law[15] and nascent artificial intelligence (AI) law.[16]

Despite many diverse definitions,[17] risk is frequently understood as an "effect of uncertainty on objectives" and expressed in terms of a cause (i.e., risk source), event or situation, consequence and its likelihood or probability.[18] Risk and its management are tools used to, *inter alia,* improve decision-making.[19] To bear fruit, risk is managed – i.e., identified, analysed, evaluated and treated[20] – and – in parallel – communicated[21] in formal, systematic and rational processes, to anticipate and address consequences that might or might not occur in the future. Risk and its management have become crucial for the functioning of many domains of contemporary life, both individual and collective. These include business management, finance and insurance, environment, toxicology, nuclear safety, national security, ethics and privacy and personal data protection.

However, the challenge that this paper is preoccupied with is understanding and assessing risk in the context of data protection law. We have observed – especially in the context of a DPIA process – that many flaws in risk assessment persist, including inadequate risk identification (e.g., imprecision), faulty evaluation, omission, confusion of key concepts, and – more broadly – assessment of risk in an *ad hoc* manner alongside difficulties in accommodating the diverging interests of controllers, processors and data

7 September 2024; Agencia Española de Protección de Datos (AEPD), 'Guidelines for conducting a data protection impact assessment in regulatory development' (2023) <https://www.aepd.es/es/documento/guidelines-conducting-data-protection-impact-assessment-regulatory-development.pdf> accessed 7 September 2024; Agencia Española de Protección de Datos (AEPD), 'Risk Management and Impact Assessment in the Processing of Personal Data' (2021) <https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf> accessed 7 September 2024. Cf. also *infra* (n 25).

[10] Walter B. Gallie, 'Essentially Contested Concepts' (1956) 56 *Proceedings of the Aristotelian Society* 167 <https://doi.org/10.1093/aristotelian/56.1.167> accessed 7 September 2024.

[11] Adam Burgess, Alberto Alemanno and Jens Zinn (eds), *Routledge Handbook of Risk Studies* (Routledge 2016) <https://www.taylorfrancis.com/books/9781317691662> accessed 7 September 2024.

[12] E.g., Peter L. Bernstein, *Against the Gods: The Remarkable Story of Risk* (Wiley 1996); Terje Aven, 'The Risk Concept—Historical and Recent Development Trends' (2012) 99 *Reliability Engineering & System Safety* 33 <http://dx.doi.org/10.1016/j.ress.2011.11.006> accessed 7 September 2024; Mary Douglas, 'Risk as a Forensic Resource' (1990) 119 *Daedalus* 1 <https://www.jstor.org/stable/20025335> accessed 7 September 2024.

[13] Risk society is a "society increasingly preoccupied with the future (and also with safety), which generates the notion of risk". Anthony Giddens and Christopher Pierson, *Conversations with Anthony Giddens: Making Sense of Modernity* (Stanford University Press 1998) 209.

[14] E.g., Julia Black, 'The Role of Risk in Regulatory Processes', in Robert Baldwin, Martin Cave, and Martin Lodge (eds), *The Oxford Handbook of Regulation* (Oxford University Press 2010) 302-348.

[15] Alessandro Spina, 'A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics' (2017) 8 *European Journal of Risk Regulation* 88; Milda Macenaite, 'The "Riskification" of European Data Protection Law through a Two-Fold Shift' (2017) 8 *European Journal of Risk Regulation* 506.

[16] Margot E. Kaminski, 'Regulating the Risks of AI' (2023) 103 *Boston University Law Review* 1347 <https://www.bu.edu/bulawreview/files/2023/11/KAMINSKI.pdf> accessed 7 September 2024; Jonas Schuett, 'Risk Management in the Artificial Intelligence Act' (2023) 2017 *European Journal of Risk Regulation* 1 <http://doi.org/10.1017/err.2023.1> 7 September 2024.

[17] E.g., Terje Aven, 'On How to Define, Understand and Describe Risk' (2010) 95 *Reliability Engineering and System Safety* 623, <http://dx.doi.org/10.1016/j.ress.2010.01.011> accessed 8 September 2024; Terje Aven, Ortwin Renn and Eugene A Rosa, 'On the Ontological Status of the Concept of Risk' (2011) 49 *Safety Science* 1074, <http://dx.doi.org/10.1016/j.ssci.2011.04.015> accessed 8 September 2024; Ortwin Renn, 'Concepts of Risk: A Classification' (1992) 53; David Garland, 'The Rise of Risk' in Aaron Doyle and Diana Ericson (eds), *Risk and Morality* (University of Toronto Press 2003); Terje Aven and Ortwin Renn, 'On Risk Defined as an Event Where the Outcome Is Uncertain' (2009) 12 *Journal of Risk Research* 1 <https://doi.org/10.1080/13669870802488883> accessed 8 September 2024.

[18] International Organization for Standardization (ISO), *ISO 31000:2018: Risk management – Guidelines*, § 3.1 <https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en> accessed 8 September 2024.

[19] 'Tool' in Hood's sense, i.e., tools like those "for carpentry and gardening" that someone has at their disposal to use them for a given purpose such as governance or management. Cf. Christopher C Hood, *The Tools of Government* (Macmillan 1983).

[20] E.g., ISO 31000:2018 *Risk management – Guidelines*, <https://www.iso.org/standard/65694.html> accessed 8 September 2024.

[21] Hyunyi Cho, Torsten Reimer, and Katherine A. McComas (eds), *The SAGE Handbook of Risk Communication* (SAGE Publications 2014).

subjects. Furthermore, given the complexity of contemporary processing operations, the elusive nature of risk often makes it difficult for data subjects and for controllers and processors alike to have a clear and comprehensive understanding of what could possibly go wrong.[22]

By way of background, under the GDPR and its sister instruments (i.e., the Data Protection and Law Enforcement Directive[23] and Regulation 2018/1795),[24] the DPIA process is a prime example of an RBA tool. In a nutshell, the DPIA is a techno-legal process to identify, analyse and evaluate possible future consequences of the intended processing operations, and to recommend the course of action to appropriately address the negative consequences, with a view to helping make decisions on how to protect personal data and to comply with the law.[25] A DPIA process is triggered when there may be a high risk to the rights and a central element of this process is risk assessment. In other words, the identification and assessment of risks, coupled with the assessment of the necessity and proportionality of the processing operations in relation to their purposes, constitute the key elements of the DPIA process.

These challenges have significant implications for the protection of fundamental rights. From the standpoint of data subjects, these difficulties particularly undermine rights to private life and to the protection of personal data. From the perspective of controllers and processors, especially in the private sector, these difficulties undermine their freedom to conduct a business or their rights to good administration, to an effective remedy or the presumption of innocence (e.g., through the reversal of the burden of proof).[26] Not only are compliance efforts likely to be adversely affected, but these difficulties also negatively impact legal certainty – a key component of the rule of law (*Rechtsstaat)*.[27] All in all, these difficulties run counter to the GDPR's stated aim of creating the "trust that allows the digital economy to develop across the internal market" in the EU and to enhance "[l]egal and practical certainty for economic operators and public authorities" (Recital 7).

In parallel, many data protection authorities (DPAs) in the EU are increasingly relying on RBA tools in their enforcement activities. Accordingly, the importance of DPIAs has grown in recent years and fines for non-compliance or malpractice are not uncommon. For instance, in 2022, two Belgian airports received fines due to the inadequate quality of their DPIA processes,[28] while in 2023, a Dutch financial services provider

[22] Cf. Jan Van Leeuwen, 'On Floridi's Method of Levels of Abstraction' (2014) 24 *Minds and Machines* 5.

[23] Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89; for its applicability to Norway, Iceland, Liechtenstein and Switzerland, cf. its Recitals 101-103.

[24] Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L295/39.

[25] Kloza and others, 'The Concept of Impact Assessment' (n 8) 32; Thibaut D'hulst and Dariusz Kloza, 'Data Protection Impact Assessment: More than Just a Compliance Tool' (Van Bael & Bellis 2022) 2, <https://www.vbb.com/media/Insights_Articles/VBB_QA_DPIA_2022_final.pdf> accessed 8 September 2024; Eleni Kosta, 'Article 35. Data Protection Impact Assessment' in Christopher Kuner, Lee A Bygrave, and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020); Jens Ambrock and Moritz Karg, 'Art. 35 Data Protection Impact Assessment' in Indra Spiecker gen. Döhmann and others (eds), *General Data Protection Regulation, Article-by-Article Commentary* (Nomos/CH Beck/Hart 2023).

[26] Cf. Articles 7-8 and 16, 47 and 48, respectively, Charter of Fundamental Rights of the European Union [2016] OJ C 202/391 (*hereafter*: CFR).

[27] Both the rule of law and *Rechtsstaat* doctrines serve multiple purposes in a polity and one of them is to channel the exercise of public power through law. They achieve their goals in different manners and hence function differently while sharing some common characteristics. Cf. further, e.g., Geranne Lautenbach, *The Concept of the Rule of Law and the European Court of Human Rights* (Oxford University Press 2013) <https://academic.oup.com/book/6558> accessed 8 September 2024; James R. Silkenat, James E. Hickey and Peter D. Barenboim (eds), *The Legal Doctrines of the Rule of Law and the Legal State (Rechtsstaat)* (Springer 2014) <http://link.springer.com/10.1007/978-3-319-05585-5> accessed 8 September 2024.

[28] Autorité de protection des données (APD), *Décision 47/2022* (4 April 2022) <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-47-2022.pdf> accessed 8 September 2024; Cour des marchés, *Arrêt AR/556* (7 December 2022) <https://www.autoriteprotectiondonnees.be/publications/arret-du-7-decembre-2022-de-la-cour-des-marches-ar-556.pdf> accessed 8 September 2024; Autorité de protection des données (APD), *Décision 48/2022* (4 April 2022) <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-48-2022.pdf> accessed 8 September 2024; Cour des marchés, *Arrêt AR/560* (7 December 2022).

was fined for failing to appropriately conduct a DPIA before processing special categories of personal data on a large scale.[29] Similarly, in January 2024, the Danish DPA fined a controller operating a secure document platform for failure to conduct a DPIA.[30] In 2022, the Dutch DPA also used powers derived from the Data Protection and Law Enforcement Directive (Article 27)[31] to fine the national police for not conducting a DPIA before deploying camera cars in Rotterdam to detect people infringing sanitary measures then in force (i.e., social distancing).[32]

Consistent with the foregoing, clarifications as to the concept of risk to the rights in EU data protection law are warranted and necessary.

2.2 Risk under the GDPR

To refer to the particular type of risk within its scope, the GDPR uses the term 'risk to the rights and freedoms of natural persons' or of 'data subjects'[33] (we refer thereto as: risk to the rights).[34] The GDPR does not contain any definition of what constitutes risk to the rights.[35] Instead, the Regulation refers to certain parameters and elements that constitute this risk. Moreover, as the Regulation makes no reference to national law for the meaning of that concept, CJEU jurisprudence suggests it must be an autonomous concept of EU law, interpreted uniformly throughout the EU, taking into account the context of the provisions referring to it and the purpose of the GDPR.[36]

At the most basic level, reading from the text of the GDPR, it is apparent that this risk relates to a negative consequence of data processing operations that might or might not occur in the future. The GDPR ignores any positive consequences and instead approaches "risk as something to overcome, an experience whose time can and should be put to an end".[37] (This interpretation largely aligns with most of the contemporary understandings of risk and a number of DPAs have offered a similar view, e.g., the Article 29 Working Party (WP29)[38] and the French DPA.)[39] Necessarily, there must be a sufficient link between a processing operation and such a consequence. The scope of such a risk concerns "all fundamental rights" – as enshrined in the CFR and in the laws of EU Member States; the latter as long as the "primacy, unity, and effectiveness of EU

[29] At the time of writing, the decision may still be appealed. Cf. *Autoriteit Persoonsgegevens* (AP), Decision of 18 December 2023, <https://www.autoriteitpersoonsgegevens.nl/uploads/2024-01/Besluit%20boete%20ICS.pdf> accessed 8 September 2024.

[30] Datatilsynet, *Netcompany indstilles til bøde* (12 January 2024) <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/netcompany-indstilles-til-boede> accessed 8 September 2024.

[31] *Supra* (n 23).

[32] Autoriteit Persoonsgegevens, *Decision No. z2021-17798* (17 November 2022) <https://www.autoriteitpersoonsgegevens.nl/uploads/imported/besluit_boete_mobiele_camera-autos_rotterdam.pdf> accessed 8 September 2024.

[33] The terminology seems to be inconsistent; cf. e.g., Articles 35(1) and 35(9).

[34] Niels van Dijk, Raphaël Gellert and Kjetil Rommetveit, 'A Risk to a Right? Beyond Data Protection Risk Assessments' (2016) 32 *Computer Law & Security Review* 286 <http://dx.doi.org/10.1016/j.clsr.2015.12.017> accessed 9 September 2024; Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 *Computer Law & Security Review* 279 <https://doi.org/10.1016/j.clsr.2017.12.003> accessed 9 September 2024; Katerina Demetzou, 'Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of "High Risk" in the General Data Protection Regulation' (2019) 35 *Computer Law & Security Review* 105342 <https://doi.org/10.1016/j.clsr.2019.105342> accessed 9 September 2024; Katerina Demetzou, 'Risk to the "Rights and Freedoms": A Legal Interpretation of the Scope of Risk under the GDPR', Dara Hallinan, Ronald Leenes, Paul De Hert and Serge Gutwirth (eds.), *Data Protection and Privacy, Volume 12: Data Protection and Democracy* (Hart 2020). Cf. also WP29, 'Statement on the role of a risk-based approach in data protection legal frameworks' (2014).

[35] By contrast, e.g., the EU AI Act defines 'risk' as the "combination of the probability of an occurrence of harm and the severity of that harm" (Article 3(2)) and 'significant risk' as a "risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact [...] due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain" (Article 3(65)).

[36] Cf. e.g., *Engie Cartagena SL*, C–523/18, § 34; *IB v FA*, C-289/20, § 39.

[37] J Peter Burgess, 'The Ethos of Risk' (2014) 4.

[38] Cf. e.g., risk is a "scenario describing an event and its consequences, estimated in terms of severity and likelihood". WP29, 'Guidelines on Data Protection Impact Assessment', *supra* (n 9).

[39] Cf. e.g., risk is a "hypothetical scenario that describes a feared event and all the threats that would allow this to occur" to be "estimated in terms of severity and likelihood". Commission nationale de l'informatique et des libertés (CNIL), 'Privacy impact assessment (PIA) – methodology' (2018) 6 <https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-1-en-methodology.pdf> accessed 9 September 2024.

law would not be affected"[40] – whenever a right is interfered with by the processing of personal data, and "in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity" (Recital 4). Such a consequence – e.g., "discrimination, identity theft or fraud, financial loss, damage to the reputation" etc. (Recital 75) – if materialised, could produce physical, material, or non-material damage – of varying severity – to natural persons (largely, data subjects) and not – at least, not directly – to organisations (largely, controllers or processors). In other words, these consequences pertain to individuals and not to controllers or processors, at least not directly.[41] In turn, the consequences for controllers or processors for failure to comply with EU data protection law – such as administrative fines (Article 83), criminal sanctions (Article 84), reparation for damages to third parties (Article 82) or loss of reputation – constitute a different sort of risk (e.g., compliance risk), with which the GDPR is not directly concerned and the management of which belongs to a separate process.

2.3 Related concepts

What could possibly go wrong with the processing of personal data has been so far described in diverse ways, including privacy (or: data protection) risk, harm, damage, loss, tort (or: delict), interference, violation or infringement of law. The GDPR uses concepts such as 'damage', 'violation', 'loss' or 'infringement'. Often these terms are different but related, and although they are often used interchangeably, these concepts are not equivalents and not all of them fall within the scope of what can be understood as a risk to the rights within the meaning of the GDPR. The theoretical aspects of these related concepts have already been discussed extensively.[42] This paper analyses only some ways in which they relate to risk and to risk to the rights.

First, risk and risks to the right concern the future and hence they refer to known (even if only to some degree) negative outcomes that have not yet materialised or may never materialise (i.e., the consequence is only potential), and are terms employed before these (potential) consequences occur (i.e., *ex ante*). By contrast, concepts such as 'damage', 'violation', 'loss' or 'infringement' denote a realized negative consequence and are employed after consequences occurred (i.e., *ex post*). (The severity and likelihood of such damage etc. – that might or might not materialise in the future – are typically factors in risk assessment.)

Second, risk and risk to the rights also differ from 'harm', even if the latter term is not explicitly used in the English language version of the GDPR.[43] In theory, 'harm' generally refers to any physical, mental or other negative outcome of an event or a situation – e.g., as a setback to the legitimate interests of or a wrong inflicted on an individual or a group.[44] Black's Dictionary defines harm as "[i]njury, loss, damage; material or tangible detriment", also identifying several sub-categories, e.g., bodily harm as "[p]hysical pain, illness

[40] Paul Craig and Gráinne de Búrca, *EU Law: Text, Cases, and Materials* (7th edn, Oxford University Press 2020) 433 <https://doi.org/10.1093/he/9780198856641.001.0001> accessed 8 September 2024; Cf. also C-399/11, *Melloni*, §§ 58-60 and Filippo Fontanelli, 'Implementation of EU Law through Domestic Measures after Fransson: The Court of Justice Buys Time and "Non-Preclusion" Troubles Loom Large' (2014) 39 *European Law Review* 682.

[41] This is not uncommon in EU law as e.g., the process of assessing the potential environmental consequences of a project requires to include "a description of the likely significant effects of the project on the *environment*" (and not relating to the "developer") (Article 5(1)(a), Directive 2014/52/EU). The REACH Regulation concerns the "risk to human health or the environment" (not just the "manufacturer" of a chemical substance) (Article 7(5)(b)(ii), Regulation 1907/2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency... [2006] OJ L396/1).

[42] Ignacio N. Cofone and Adriana Z Robertson, 'Privacy Harms' (2018) 69 *Hastings Law Journal* 1039 <https://www.hastingslawjournal.org/wp-content/uploads/Cofone-69.4.pdf> accessed 9 September 2024; Sourya Joyee De and Daniel Le Métayer, 'Privacy Risk Analysis to Enable Informed Privacy Settings' (2018) <https://hal.inria.fr/hal-01660045> accessed 9 September 2024; Bart van der Sloot, 'Where Is the Harm in a Privacy Violation : Calculating the Damages Afforded in Privacy Cases by the European Court of Human Rights' (2017) 8 *Journal of Intellectual Property, Information Technology and E-Commerce Law: JIPITEC* 322 <https://www.jipitec.eu/archive/issues/jipitec-8-4-2017/4641> accessed 9 September 2024.

[43] In French, the GDPR uses the terms '*dommage*' and '*préjudice*'; the latter is a consequence of the former (Gerard Cornu, *Vocabulaire Juridique* (PUF 1987) 617). In Dutch, the Regulation employs the term '*schade*'.

[44] Joel Feinberg, 'Harms as Setbacks to Interest', *The Moral Limits of the Criminal Law Volume 1: Harm to Others* (Oxford University Press 1987) <https://academic.oup.com/book/1573/chapter/141067016> accessed 9 September 2024.

or impairment of the body" or social harm as an "adverse effect on any societal interest".[45] While the GDPR uses the term 'damage' as one way to refer to negative outcomes, it does not define it. The Regulation only stipulates that a processing operation may cause physical, material or non-material damage to a data subject and subsequently offers a non-exhaustive list of possible damage (Recital 75). In theory, 'damage' often denotes more severe, or at least more concrete, manifestations of harm. Black's Dictionary defines damage as a "[l]oss or injury to a person or property" and distinguishes it from damages (plural), which are the "money claimed by, or ordered to be paid to, a person as a compensation for loss or injury".[46] Ultimately, the CJEU jurisprudence suggests that – as with risk – damage should be attributed an autonomous meaning. However, the calculation of damages, in the absence of relevant rules at the EU level, is determined by the law of a Member State. Overall, it seems that the term 'harm' is broader than 'damage'. Sister domains of EU law, such as competition law, also understand 'harm' somewhat broadly.[47] Harm or damage are not a necessary condition for the existence of a risk to a right.

Third, the GDPR empowers anybody to seek 'compensation' from controllers and processors for any damage, both material and non-material, that they suffer as a result of an "infringement" of the Regulation (Article 82). In principle, 'infringement' denotes a breach of law, regardless of whether or not it causes any harm or damage. Black's Dictionary defines compensation as a "[p]ayment of damages, or any other act that a court orders to be done by a person who has caused injury to another. In theory, compensation makes the injured person whole".[48] The liability of the controller and processor is fault-based: they can escape liability if they prove that they were "not in any way responsible for the event giving rise to the damage" (Article 82(3)). However, the mere infringement of the GDPR is not, in and of itself, sufficient to establish a right to compensation for data subjects; individuals must have suffered actual damage from such an infringement.[49]

2.4 Risk assessment under the GDPR

As with the concept of risk, the text of the GDPR gives only a few hints as to how to assess it. Given the existence of numerous risk assessment methods, the Regulation suggests only that assessment is based on the combination of likelihood or probability of occurrence[50] and severity of consequence, should it materialise (Recital 76). The Regulation further suggests that risk assessment should be objective (Recital 76) and thus free from personal opinions, bias, etc.

Risk management is typically a four-part process, consisting of risk identification, analysis, evaluation and – eventually – risk treatment.[51] In the DPIA process, the GDPR requires risk to the rights to be *assessed* (i.e., the first three steps of risk management) and not *managed* – at least not explicitly – as the *treatment* of risk belongs to a separate process. The GDPR does not contain any general obligation to treat the risk;[52] the Regulation only suggests that the "outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data" complies with the law (Recital 84) and the GDPR obligates a controller to implement "appropriate technical and organisational measures" to protect personal data, such as data protection by design and by default (Article 25(1)).

Specifically, in the DPIA process, in parallel to the assessment of risks to the rights (Article 35(7)(c)), assessors must also assess the necessity and proportionality of processing operations in relation to their purposes (Article 35(7)(b)). Furthermore, the GDPR also requires that the "views of data subjects or their representatives on the intended processing" are sought. This is, however, only required "[w]here appropriate"

[45] *Black's Law Dictionary* (Bryan A Garner ed, 9th edn, West 2010) 616.

[46] Ibid, 355.

[47] Directive 2014/104 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union [2014] OJ L349/1.

[48] *Black's Law Dictionary* (Bryan A Garner ed, 9th edn, West 2010) 259.

[49] *Österreichische Post*, C-300/21; *MediaMarktSaturn*, C-687/21 and *juris GmbH*, C-741/21. Cf. e.g., Thibaut D'hulst, Dariusz Kloza and Orla Murnaghan, 'GDPR Case Sheds Light On Threshold For Individual Damages' *Law360* (2023).

[50] In English, probability (e.g., '85%') is often interpreted as the mathematical expression of likelihood (e.g., 'highly likely').

[51] ISO, §§ 6.4-6.5, *supra* (n 18).

[52] Quelle (n 3) 50.

and, in any case, "without prejudice to the protection of commercial or public interests or the security of processing operations" (Article 35(9)). If the DPIA process concludes that there would be residual high risk despite mitigation measures, a consultation with a competent DPA is required (Article 36). High risk is not defined, although Article 35(3) lists some examples of high-risk processing operations, e.g., the "processing on a large scale of special categories of data"; additionally, the European Data Protection Board (EDPB) offers some guidance on that matter[53] and national DPAs can determine, for their own jurisdiction, what further types of processing operations are deemed highly risky and hence require a DPIA (Article 35(4)). Upon such a consultation, a DPA can use all investigatory, corrective or authorisation and advisory powers at its disposal, including administrative fines (Article 58(2)(i)) and a ban on processing operations (Article 58(2)(f)).

2.5 Discussion

Perhaps due to its new role under EU data protection law, the concept of risk to the rights suffers from several problems, which adversely affect legal compliance and fundamental rights protection.

First, risk to the rights is frequently confused with non-compliance risk. Scholars have argued that limiting the scope of risk to the rights to 'non-compliance risk', i.e., the "chances that a given processing operation will not comply with the GDPR" would go "against both the wording and the role of the concept in the GDPR".[54] Similarly, the relationship between the rights-based elements of the GDPR and the risk-based ones (e.g., the data subject rights that are not calibrated in terms of risk) are frequently confused.[55]

Second, the nature of risk identification – and, more broadly, risk management – is frequently understood as an obligation of result and not as an obligation of means. While obligations of result require some predetermined results to be attained and are judged by strict liability rules (i.e., a result achieved or not), obligations of means require best efforts to be given to attain such a result and typically require proof of fault or negligence for liability to arise (i.e., best-efforts obligation, due diligence).[56] Under the GDPR, risk assessment takes place in the context of the accountability principle (Article 5(2))[57] and within the requirement to "implement appropriate technical and organisational measures" (Article 24). However, given its inherent limitations, risk identification is an obligation of means, and the means that can be required to identify risks should be reasonable. To determine these means, Article 24 indicates that "the nature, scope, context and purposes of processing" should be considered. In the context of a DPIA, the process is required for processing operations that are likely to result in a high risk (Article 35(1)) and the effort in identifying risk should reflect this. Risk identification cannot be regarded as an obligation of result and organisations cannot be held liable merely because the outcome of the risk assessment process failed to take account of specific events or situations that materialised after the assessment, e.g., despite best efforts, risks identified were incomplete. The accountability principle requires controllers to demonstrate that they have taken all necessary steps to ensure compliance with the GDPR and to document this for DPAs, who may review documentation with the benefit of hindsight.

In parallel, given the very nature of risk and its inherent limitations, the desired, *objective* assessment – as hinted in Recital 76 – is not fully attainable in practice, due to ambiguities about assignable likelihood and severity of the negative outcome, scarce knowledge (e.g., 'unknown unknowns' or 'black swans'),[58] risk

[53] WP29, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (2017).

[54] Gellert (n 34); Demetzou, 'Risk to the "Rights and Freedoms": A Legal Interpretation of the Scope of Risk under the GDPR' (n 34).

[55] Quelle (n 3) 42.

[56] From French: *obligation de moyen* and *obligation de résultat*. René Demogue, *Traité des Obligations en général: Analyse des Principes – Comparaison des Législations* vol 6 (A Rousseau, Paris 1925) 538.

[57] The principle of accountability is yet another of the cornerstones of EU data protection law. It stipulates that a "controller shall be responsible for, and be able to demonstrate compliance with" data protection principles (Articles 5(2)). Cf. e.g., Joseph Alhadeff, Brendan van Alsenoy and Jos Dumortier, 'The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions' in Daniel Guagnin and others (eds), *Managing Privacy through Accountability* (Palgrave Macmillan 2012) <http://link.springer.com/10.1057/9781137032225_4> accessed 10 September 2024.

[58] Terje Aven, 'On the Meaning of a Black Swan in a Risk Context' (2013) 57 *Safety Science* 44 <http://dx.doi.org/10.1016/j.ssci.2013.01.016> accessed 10 September 2024.

perception and attitudes (e.g., risk-prone or risk-averse approach)[59] or confirmation bias (e.g., concluding that risks have sufficiently been mitigated).[60] As a result, there are risks that may never be fully identifiable and manageable, which further underlines that these processes are necessarily obligations of means.

Third, the practice of risk assessment frequently suffers from many flaws, such as inadequate risk identification, omission or confusion of key concepts. For example, risk is often imprecisely described (e.g., not sufficiently detailed). At times, events are confused with their consequences or consequences that are certain to happen are incorrectly described in terms of risk. Further difficulties include faulty evaluation such as assessing risk in an *ad hoc* manner,[61] in a formalistic fashion, such as ticking the boxes of a pre-populated form, or assessing them partially, e.g., only the severity of risk, while ignoring its likelihood. Accommodating diverging interests of controllers, processors and data subjects presents additional challenges. In the context of a DPIA process, these problems are magnified by freely available – yet often poor quality – methods, forms and templates. This runs counter to the objective of protecting fundamental rights and ensuring legal certainty.

3 Examples and classification of negative consequences

3.1 Broadening the scope: from risk to the rights to negative consequences

Risk to the rights under the GDPR has a specific meaning: it concerns solely those consequences that pertain to data subjects in the context of the processing of personal data. While the scope of the concept is relatively broad, it may not contribute to a full understanding of what could possibly go wrong while processing personal data. As we aim to provide the most comprehensive picture, while acknowledging that exhaustiveness is elusive, we suggest using a broader term: looking at any possible ‘negative consequences’ stemming from the processing of personal data (*hereafter*: negative consequences) as an answer to the plain language question of ‘what could possibly go wrong?’.

Use of a broader term is advantageous at two levels. First, it allows us to go beyond the strict boundaries of data protection law. Relying only on negative consequences in the context of EU data protection law might not always convey a sufficiently complete picture. Some negative consequences may fall into the scope of protection offered by other legal instruments, e.g., damage to the integrity of elections.[62] Moreover, considerations such as applied ethics, corporate social responsibility (CSR) or environmental, social, and governance (ESG) aspects may necessitate a broader understanding. In addition, from a practical viewpoint, assessors may wish to include such broader consequences in their assessment for efficiency reasons, to integrate multiple assessments in an evolving regulatory landscape, e.g., the fundamental rights impact assessment (FRIA) under the AI Act[63] or risk assessment under the Digital Services Act (DSA).[64]

Second, while data protection laws typically offer protection only against those negative consequences that relate to data subjects (i.e., identified or identifiable natural person whose personal data are processed), other stakeholders may face different consequences. For example, controllers and processors often need to take into account their non-compliance risks. Moreover, data protection law does not protect natural persons who are as yet unidentifiable (e.g., anonymous data) and who may suffer some negative consequences; similarly, it does not protect societal groups.

[59] Nikolaos Ioannidis and others, ‘A Tailored Method for the Process of Integrated Impact Assessment on Border Control Technologies in the European Union and the Schengen Area’ in J.Peter Burgess and Dariusz Kloza (eds), *Border Control and New Technologies* (Academic & Scientific Publishers 2021) 152.

[60] Cf. J. Peter Burgess, *Data protection and ethics. Does more ethics imply more duties for controllers?*, Brussels Privacy Hub (2017) <https://soundcloud.com/user-845197532/burgess-ethics-and-data-protection> accessed 11 September 2024.

[61] R. Jason Cronk, *Strategic Privacy by Design* (International Association of Privacy Professionals 2022) 49.

[62] About the damage to electoral process, e.g., Regulation (EU) 2024/900 of the European Parliament and of the Council of 19 March 2024 on the transparency and targeting of political advertising.

[63] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 11 July 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L202/1.

[64] Articles 34–35, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) [2022].

3.2 Categories of negative consequences: examples from the conceptualisations of privacy

Examples of negative consequences are plentiful and they can be identified in several ways.

One way to do so is *via* a 'reverse' reading of the many conceptualisations of privacy. The concept of personal data protection is closely related to that of privacy.[65] As a result, negative consequences of the processing of personal data are closely related to those of privacy infringements. As privacy is an abstract concept, making it difficult to grasp, various authors have attempted to make it more concrete by distinguishing various conceptualisations of privacy (its scope, types or dimensions). Broadly speaking, infringements or interferences with such dimensions of privacy would constitute negative consequences, or at least categories thereof.

For example, Clarke identified four dimensions, namely: privacy of the person, of personal behaviour, of communications and of personal data, to which he later added a fifth: privacy of personal experience.[66] Finn *et al*. have listed seven dimensions, extending Clarke's by the privacy of thoughts and feelings, of location and space, and of association.[67] Most recently, Koops *et al*. have structured the "types of privacy in a two-dimensional model, consisting of eight basic types of privacy (bodily, intellectual, spatial, decisional, communicational, associational, proprietary, and behavioral privacy), with an overlay of a ninth type (informational privacy) that overlaps, but does not coincide, with the eight basic types".[68]

From a slightly different perspective, Nissenbaum identified several fundamental values likely to be affected by informational flows, discussing (1) "information-based harm, (2) informational inequality, (3) autonomy, (4) freedom, (5) [...] important human relationships, and (6) democracy and other social values".[69] Clarke, who introduced the concept of dataveillance, identified three broad categories of dangers stemming therefrom, e.g., wrong identification as an instance of dangers of personal dataveillance.[70] Mulligan *et al*. mapped 14 "claims for, criticisms of, and contests over privacy", some of which directly identify "archetypal threat[s]" thereto, e.g., "identity theft; intrusive surveillance; gossiping neighbours" or "action[s] against privacy", e.g., "act or behaviour that initiates or constitutes a privacy harm, i.e. staring at him while he was dressing in the locker room violated his privacy".[71] Furthermore, Hartzog has identified obscurity, trust and autonomy as three primary enabling values for his privacy blueprint.[72] From a broader perspective, Sartor identified nine information and communications technologies (ICT) risks, colourfully relating them to some well-known literary works, such as the use of technology for surveillance ("Orwell's nightmare"), covering control and judgement ("Kafka's nightmare") or discriminating and excluding ("Huxley's nightmare").[73]

In international human rights law and constitutional law, privacy is typically understood as a multi-dimensional concept, comprising the right to private life, family life, home and correspondence[74] as well as the protection against "attacks upon [an individual's] honour and reputation".[75] Therefore, privacy can

[65] Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Erik Claes, Anthony Duff and Serge Gutwirth (eds), *Privacy and the criminal law* (Intersentia 2006) <http://works.bepress.com/serge_gutwirth/5> accessed 11 September 2024.

[66] Roger Clarke, 'What's "Privacy"?' (2006) <http://www.rogerclarke.com/DV/Privacy.html> accessed 11 September 2024.

[67] Rachel L. Finn, David Wright and Michael Friedewald, 'Seven Types of Privacy' in Serge Gutwirth and others (eds), *European Data Protection: Coming of Age* (Springer 2013) <http://dx.doi.org/10.1007/978-94-007-5170-5_1> accessed 11 September 2024.

[68] Bert-Jaap Koops and others, 'A Typology of Privacy' (2017) 38 *University of Pennsylvania Journal of International Law* 483, 483–575 <https://scholarship.law.upenn.edu/jil/vol38/iss2/4/> accessed 11 September 2024.

[69] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 *Washington Law Review* 119 <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10> accessed 12 September 2024.

[70] Roger Clarke, 'Information technology and dataveillance' (1988) 31(5) *Communications of the ACM* 498 <https://doi.org/10.1145/42411.42413> accessed 12 September 2024.

[71] Deirdre K. Mulligan, Colin Koopman and Nick Doty, 'Privacy Is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy' (2016) 374 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 20160118 <http://rsta.royalsocietypublishing.org/lookup/doi/10.1098/rsta.2016.0118> accessed 12 September 2024.

[72] Woodrow Hartzog, *Privacy's Blueprint. The Battle to Control the Design of New Technologies* (Harvard University Press 2018) 234.

[73] Giovanni Sartor, 'Human Rights in the Information Society' (2010) *SSRN* <http://dx.doi.org/10.2139/ssrn.1707724> accessed 15 September 2024.

[74] Article 8, European Convention on Human Rights (ECHR), opened for signature 4 November 1950, ETS 5 (entered into force 3 September 1953); Article 7, Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

[75] Article 12, Universal Declaration of Human Rights (UDHR), adopted 10 December 1948, UNGA Res 217 A (III).

typically cover a wide range of issues such as bodily integrity, access to public information, secrecy of communications, protection of the domicile, protection of personal data, identity, making essential personal choices (e.g., name or sexual orientation) or the protection against environmental nuisance.[76]

Finally, some authors directly focus on listing the negative consequences (or categories of them) arising from specific technologies or practices, such as algorithms and automated decision-making (e.g., discrimination in school admission, recruitment or access to financial services)[77] or AI (e.g., 'hallucinations');[78] some of them relating to privacy and personal data protection.

3.3 Concrete and precise illustrations of negative consequences: examples from data protection law and sister domains

Our exercise has revealed the *categories* of negative consequences, but not described them with a sufficient level of detail. Since these consequences need to be defined and accurately described to be appropriately assessed, we sought out *concrete, precise examples* of them. To that end, we turned to scholarly and professional writing, and legislation as well as jurisprudence and decisions of courts and DPAs.

First, the early enumerations of privacy torts in American legal doctrine can be illustrative of negative consequences. In their classic text, Warren and Brandeis identified several such negative consequences and argued for them to be remediable, possibly with an injunction "in a very limited class of cases".[79] When they proposed a 'right to be let alone', Warren and Brandeis were motivated by the intrusion into one's private matters by yellow journalism, amplified by the emergence of affordable – and, with time, ubiquitous – photography.[80] Based on their work, Prosser proposed four privacy torts, namely: "[i]ntrusion upon the plaintiff's seclusion or solitude, or into his private affairs", "[p]ublic disclosure of embarrassing private facts about the plaintiff", "[p]ublicity which places the plaintiff in a false light in the public eye" and "[a]ppropriation, for the defendant's advantage, of the plaintiff's name or likeness".[81] Next, Westin distinguished three types of intrusions on privacy, namely self-revelation, curiosity and surveillance.[82]

Second, amongst scholarly and professional writings, Wright and Raab attempted to match privacy principles with examples of harm;[83] as did, amongst public authorities, the New Zealand DPA in its own enumeration of privacy risks.[84] Moreover, the World Economic Forum (WEF) has recently offered an equally broad typology of online harms, distinguishing between threats to personal and community safety (e.g. child sexual abuse material (CSAM), incitement to violence, grooming), harm to health and well-being (e.g., promotion of self-harm), hate and discrimination (e.g., hate speech), violation of dignity (e.g., bullying, harassment), invasion of privacy (e.g., doxing), and deception and manipulation (e.g., phishing, catfishing).[85]

[76] Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 *International Data Privacy Law* 222 <https://doi.org/10.1093/idpl/ipt017> accessed 22 September 2024; Raphaël Gellert and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection' (2013) 29 *Computer Law & Security Review* 522 <https://doi.org/10.1016/j.clsr.2013.07.005> accessed 22 September 2024.

[77] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown 2016).

[78] Organisation for Economic Co-operation and Development (OECD), *Framework for the Classification of AI Systems* (12 September 2022) <https://doi.org/10.1787/cb6d9eca-en> accessed 22 September 2024; Schuett (n 16); US Department of State, Bureau of Cyberspace and Digital Policy, *Risk Management Profile for Artificial Intelligence and Human Rights* (2024) <https://www.state.gov/risk-management-profile-for-ai-and-human-rights> accessed 22 September 2024; Peter Slattery and others, 'The AI Risk Repository: A Comprehensive Meta-Review, Database, and Taxonomy of Risks From Artificial Intelligence' (2024) <https://airisk.mit.edu> accessed 22 September 2024. Cf. also: AI Incident Database <https://incidentdatabase.ai> accessed 22 September 2024.

[79] Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

[80] Sarah E. Igo, *The Known Citizen. A History of Privacy in Modern America* (Harvard University Press 2018).

[81] William L. Prosser, 'Privacy' (1960) 48 *California Law Review* 389.

[82] Alan F. Westin, *Privacy and Freedom* (Atheneum 1967).

[83] David Wright and Charles Raab, 'Privacy Principles, Risks and Harms' (2014) 28 *International Review of Law, Computers and Technology* 277.

[84] Office of the Privacy Commissioner [New Zealand], 'Privacy Principles & Examples of Risks and Mitigations' (n.d.) <https://privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/PIA/2023-PIA-toolkit-files/PIA-Toolkit-The-privacy-principles-and-examples-of-risks-and-mitigations.pdf> accessed 14 September 2024.

[85] World Economic Forum, 'Toolkit for Digital Safety Design Interventions and Innovations: Typology of Online Harms' (2023) <https://www3.weforum.org/docs/WEF_Typology_of_Online_Harms_2023.pdf> accessed 14 September 2024.

Third, legislation too can be a source for examples of negative consequences. For instance, the GDPR offers a few examples of negative consequences, or events or causes leading to them, such as "discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage" (Recital 75). In turn, the anti-money laundering (AML) directive, which establishes a register of ultimate beneficial owners (UBO), lists possible negative consequences from processing personal data in such a register as "fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation" (Article 30(9)).[86]

Fourth, authoritative interpretation of what constitutes risk to the rights comes from the vast jurisprudence of the CJEU, making it a significant source of examples of negative consequences. To date, this Court has handed down 181 judgments in data protection matters, of which 90 cases explicitly mention the concept of risk, 63 mention damage and 38 mention both terms, yet in various contexts.

The Court has frequently mentioned a risk of "abuse" or "misuse" of personal data. For example, in *Schufa* (2023), the Court – at the most general level – ruled that risks stemming from automated decision-making, which includes profiling, are "likely to weigh on the legitimate interests and rights of the data subject, in particular taking account of discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation".[87] In *Digital Rights Ireland* (2014), the CJEU considered the retention of personal data for the purpose of the investigation, detection and prosecution of serious crime, and found that "data must be protected against the risk of abuse and against any unlawful access and use of that data".[88]

In *Österreichischer Rundfunk* (2003), the Court offered a more detailed description of negative consequences. The CJEU considered the "obligation of public bodies subject to control by the Rechnungshof to communicate to it the salaries and pensions exceeding a certain level [...] together with the names of the recipients, for the purpose of drawing up an annual report [...] and made available to the general public". The CJEU found that data subjects "may suffer harm as a result of the negative effects of the publicity attached to their income from employment, in particular on their prospects of being given employment by other undertakings".[89]

More recently, in *Puskar* (2017), the Court considered whether national tax authorities were "permitted to keep a confidential list of natural persons who purport to act as company directors of specific legal persons" for the purpose of collecting tax and combating tax fraud. The Court found that the "inclusion in that list could harm [an individual's] reputation and affect his relations with the tax authorities.[90] In *Latvijas Republikas Saeima* (2021), the CJEU decided that the "public disclosure of personal data relating to road traffic offences, including data relating to the penalty points imposed for committing them [...] may give rise to social disapproval and result in stigmatization of the data subject";[91] the Court subsequently struck a similar chord in *Endemol Shine Finland* (2024).[92] In *FT* (*Copies du dossier médical*) (2023), the Court considered the right to access one's health records and held that a "simple summary or a compilation of [highly technical health data] by the medical practitioner, in order to present them in an aggregated form, could create the risk of some relevant data being omitted or incorrectly reproduced, or, in any event, of it being made harder for the patient to verify how accurate and exhaustive those data are and to understand those data".[93]

[86] Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing... [2015] OJ L141/73. Cf. *WA & Sovim SA*, C-37/20 and C-601/20, § 79.

[87] C-634/21, § 59.

[88] C-293/12 and C-594/12, § 54.

[89] C-465/00, C-138/01 and C-139/01, §§ 2 and 89.

[90] C-73/16, § 114.

[91] C-439/19, §§ 74, 75 and 112.

[92] C-740/22, § 54.

[93] C-307/22, § 78.

3.4 Typologies of negative consequences

Given the abundance of possible negative consequences, numerous efforts have been made to catalogue them systematically, i.e., to classify them.

For the sake of clarity, classification is the "ordering of entities into groups or classes on the basis of their similarity", e.g., on a basis of some "key or fundamental characteristics". Classification is "both a process and an end result".[94] Of the two main types of classification, typology is primarily conceptual, while taxonomy is empirical. To be useful, classifications should, as a minimum, be sufficiently clear, comprehensive, fit-for-purpose and accurate. Typologies and taxonomies are tools to facilitate comprehension of abstract concepts and are frequent in many domains of life, such as biology (e.g., Linnaeus' scientific names of species), and their usage in other fields of (technology) law are nothing new *per se*, e.g., in cybercrime[95] or AI risk.[96]

Concerning classifications of privacy harms, in academia, Solove was perhaps the first to offer a four-partite typology of information privacy harms, consisting of information collection, its processing and dissemination, as well as "impingements directly on the individual".[97] Citron and Solove subsequently advocated what is – thus far – the most comprehensive typology thereof, i.e. "(1) physical harms; (2) economic harms; (3) reputational harms; (4) psychological harms; (5) autonomy harms; (6) discrimination harms; and (7) relationship harms".[98] In parallel, Calo categorised harms as "distinct but not entirely separate" objective harms (i.e., external to the person harmed, e.g., identity theft) and subjective ones (i.e., internal thereto, e.g., fear or discomfort).[99] Cofone distinguished five groups of harm: reputational, financial, physical harm, discrimination and harms to democracy.[100] Cronk further categorised harms as psychological and behavioural harms, lost opportunity, economic loss, loss of liberty and social detriment.[101]

Amongst public authorities, the Information Commissioner's Office (ICO), the British DPA, has issued its own typology,[102] based on a synthesis of the literature to date. The ICO distinguishes between individual and societal harms; examples of the former include financial harm or chilling effects and an example of the latter is damage to the environment (e.g., "[h]igh energy use associated with data mining, storage and sharing").[103]

3.5 Towards a comprehensive typology

Each of these classifications provides useful perspectives on negative consequences. However, we believe that only a combination of all these viewpoints can present a comprehensive understanding, and provide a useful tool to assist assessors in identifying such consequences.

Hence, in Exhibit 1, we propose – based on the sources mentioned above – a comprehensive albeit non-exhaustive typology of possible negative consequences stemming from the processing of personal data, inspired by and based on both the examples of such consequences and a synthesis of earlier attempts to classify them. We distinguish between three broad categories of such consequences: those pertaining to

[94] Kenneth D. Bailey, *Typologies and Taxonomies: An Introduction to Classification Techniques* (Sage 1994) 1.

[95] Jan-Jaap Oerlemans and Wytske Van Der Wagen, 'Types of Cybercrime and Their Criminalisation' in Wytske Van Der Wagen, Jan-Jaap Oerlemans and Marleen Weulen Kranenbarg (eds), *Essentials in cybercrime: A criminological overview for education and practice* (Eleven 2022); David Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press 2007).

[96] *Supra* (n 78).

[97] Daniel J. Solove, 'A Taxonomy of Privacy' (2006) 154 *University of Pennsylvania Law Review* 477 <https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1/> accessed 14 September 2024; Daniel J. Solove, *Understanding Privacy* (Harvard University Press 2008).

[98] Danielle Keats Citron and Daniel J. Solove, 'Privacy Harms' (2022) 102 *Boston University Law Review* 793 <https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf> accessed 15 September 2024.

[99] Ryan Calo, 'The Boundaries of Privacy Harm' (2011) 86 *Indiana Law Journal* <http://ilj.law.indiana.edu/articles/86/86_3_Calo.pdf> accessed 15 September 2024.

[100] Ignacio N. Cofone, *The Privacy Fallacy* (Cambridge University Press 2023) 112 <https://www.cambridge.org/core/product/identifier/9781108995825%23CN-bp-6/type/book_part> accessed 16 September 2024.

[101] Cronk (n 61) 93–95.

[102] ICO, 'Overview of Data Protection Harms and the ICO's Taxonomy' (2022) <https://ico.org.uk/media/about-the-ico/documents/4020144/overview-of-data-protection-harms-and-the-ico-taxonomy-v1-202204.pdf> accessed 16 September 2024.

[103] Sam Wood and others, 'Review of Literature Relevant to Data Protection Harms' (2022) <https://ico.org.uk/media/about-the-ico/documents/4020142/plum-review-of-literature-relevant-to-data-protection-harms-v1-202203.pdf> accessed 16 September 2024.

individuals (i.e., largely, data subjects), to society (i.e., group, collective, community, etc.)[104] and to those who process personal data of others (i.e., predominantly, controllers and processors).

In respect of negative consequences to individuals, we distinguish between substantive and formal consequences. Substantive consequences range from financial loss, discrimination to autonomy harm (e.g., manipulation, coercion) and chilling effects and from psychological harm (e.g., emotional distress, disturbance) through reputational harm (e.g., embarrassment, shame or ridicule) to physical damage (e.g., bodily injury or death). At the same time, some of these consequences may be classified as material or non-material, and others subjective or objective in their nature.

Formal consequences are mere infringements (violations, etc.) of data protection law that may not necessarily result in tangible or intangible harm or damage suffered by a natural person. In other words, harm or damage to an individual does not need to occur for such a formal consequence to materialise. Examples in this category include breaches of data protection principles, data subject rights or international transfer rules.

For consequences pertaining to a society, following the ICO, we distinguish between a group of negative consequences to democracy (i.e., damage to law and justice; to media, information and public discourse; and to electoral process) as well as negative consequences to public health, environment and the economy.[105]

Finally, for the negative consequences pertaining to those who process others' personal data – largely: controllers, processors, recipients and third parties – they can face negative consequences stemming from their failure to comply with data protection law or from otherwise damaging natural persons or society by their processing of personal data (e.g., non-compliance risk). Such consequences can be of civil, criminal or administrative nature, e.g., an administrative sanction (fine) imposed by a DPA or damages paid to compensate a data subject.

In addition, the cost of avoiding and/or repairing harm (e.g., time, money or workforce), should it occur, constitutes a 'meta' damage, relevant for all types of negative consequences.

Some of these negative consequences fall within the remit of the GDPR and others within sector-specific instruments, e.g., transparency and targeting of political advertising.[106] Both these substantive and formal consequences can be conceptualised as risks to the rights under EU data protection law. A single processing operation could cause more than one negative consequence (e.g., an event leading to both psychological harm and financial loss). As a result of using this synthesised typology, a consequence is described using four dimensions: stakeholders, formal/substantive, material/non-material and subjective/objective.

[104] Cf. Linnet Taylor, Luciano Floridi and Bart van der Sloot, *Group Privacy. New Challenges of Data Technologies* (Springer 2017).
[105] ICO (n 102).
[106] Cf. Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising.

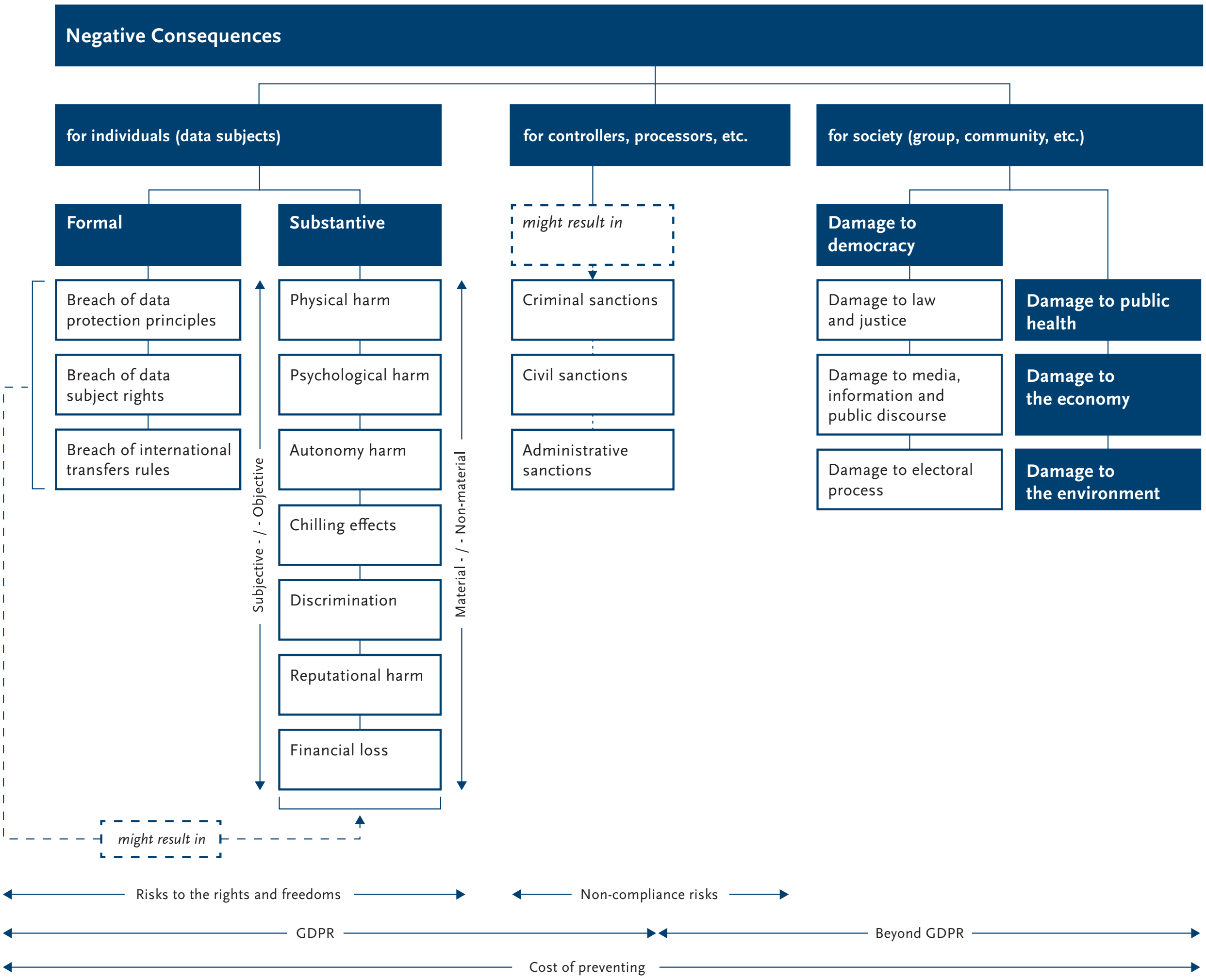
Negative Consequences
for individuals (data subjects)
for controllers, processors, etc.
for society (group, community, etc.)
Formal
Substantive
might result in
Damage to democracy
Breach of data protection principles
Breach of data subject rights
Breach of international transfers rules
Physical harm
Psychological harm
Autonomy harm
Chilling effects
Discrimination
Reputational harm
Financial loss
Subjective - / - Objective
Material - / - Non-material
Criminal sanctions
Civil sanctions
Administrative sanctions
Damage to law and justice
Damage to media, information and public discourse
Damage to electoral process
Damage to public health
Damage to the economy
Damage to the environment
might result in
Risks to the rights and freedoms
Non-compliance risks
GDPR
Beyond GDPR
Cost of preventing

Exhibit 1. A typology of possible negative consequences stemming from the processing of personal data.

3.6 Discussion

Identifying what could be a negative consequence is a continuous activity, and further categories and examples will be identified in the future. This is due, first and foremost, to the open-ended nature of the concept of personal data and the extent to which it overlaps with privacy, on the one hand, and with the objectives of the RBA (such as flexibility and accommodation of diverse interests), on the other. The right to privacy is perhaps the most malleable of all fundamental rights, to the extent that the European Court of Human Rights (ECtHR) once claimed that the “concept of ‘private life’ is a broad term not susceptible to exhaustive definition”.[107] As far as data protection is concerned, the CJEU jurisprudence on the concept of personal data – central to determining whether the GDPR applies – still leaves a lot of loose ends. The second reason relates to the lists of negative consequences and their typologies that will need to be updated as technology, economy and society develop.

[107] ECtHR, *Pretty v. UK*, 29 April 2002, 2346/02, § 61. Cf. also *supra* (n 76).

4 How to identify the negative consequences?

4.1 The deductive method: a typology

As mentioned earlier, risk assessment under the GDPR takes place in the context of the accountability principle. Therefore, particularly as risk assessment constitutes – we argue – an obligation of means, it is important that controllers and processors use a structured method for its various steps. To that end, we propose a two-phase method to efficiently identify the risks and – more broadly – negative consequences. Our method relies on both typologies and examples. The method combines a Phase 1 deductive, top-down approach, and a Phase 2 inductive, bottom-up approach whereby each phase complements the other.

Phase 1 relies on a typology of possible negative consequences: based on the many categories it offers, such a typology helps in further specifying what could possibly go wrong in the planned processing operations (i.e., through a top-down or *deductive* identification). While some typologies that are technology-neutral may provide versatility and broad applicability, others may be technology- or sector-specific. Such a method has many advantages, especially if the exercise takes place in a diverse and multidisciplinary group of assessors with adequate stakeholder representation (cf. Article 35(9)). Through human creativity and imagination, the method can identify novel or previously unknown negative consequences, especially in the context of new and emerging technologies.

However, the method also has its shortcomings. The analysed typologies are quite high level as they present categories of negative consequences rather than any detailed, concrete consequences. Some negative consequences could be overlooked, e.g., due to availability bias (i.e., giving more importance to things that easily come to mind) or limitations in experience or expertise. To address these shortcomings, a more comprehensive method for identifying negative consequences is necessary and warranted.

4.2 The inductive method: developing an inventory

To complement the deductive method described above, and remedy its shortcomings, we propose an *inductive* method using a 'living' inventory of known negative consequences, systematically classified under multiple criteria and regularly updated. The method is inductive (bottom-up) as assessors induce the listing of relevant negative consequences from examples thereof. Hence, in Phase 2, a database would be created and used to search for and/or filter relevant examples of negative consequences based on a description of the relevant processing operations. In practice, assessors would search for a set of relevant keywords (tags) that match their description of their envisaged processing operations.

The database would build upon existing typologies and examples, but – in addition – it would describe each negative consequence by further characteristics (keywords, tags), such as:

- Categories of personal data – in particular, if special categories are processed (e.g., health data or biometric data), data relating to criminal convictions and offences (Articles 9-10) or other highly personal categories of personal data (e.g., human resources management, neurological health data),
- Type(s) of processing activities – e.g., "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Article 4(3)) or re-use of personal data (Article 5(b) *in fine*),
- Categories of affected people – e.g., (specific) individuals such as schoolchildren, city residents, groups, society as a whole, etc.,
- Characteristics of a natural person (data subject) – i.e., if vulnerable, and if so, the type of vulnerability, such as being an employee, patient, child, elderly, migrant or belonging to a minority,[108]
- Sector of governance or economy – e.g., public administration, private or public-private partnership (PPP),
- Type of technology – e.g., information and communications technologies (ICT) (such as the Internet or AI), engineering, nanotechnology or biotechnology,

[108] Gianclaudio Malgieri, *Vulnerability and Data Protection Law* (Oxford University Press 2023). Cf. also: *International Observatory on Vulnerable People in Data Protection* (VULNERA), <https://brusselsprivacyhub.com/vulnera> accessed 30 September 2024.

- Context of the processing – e.g., fight against serious crime and terrorism, humanitarian action, special processing situations (Articles 90ff), such as the re-use of personal data for scientific research; journalism,
- Indicators of high risk – e.g., profiling (Article 35(3)(b)) or processing on a 'large scale', and risk parameters already attributed in prior occurrences, if any (e.g., highly probable, low severity, etc.),
- Technical characteristics of the data, such as their format (e.g., text, graphics, audio, video) or storage method (e.g., local, cloud),
- Relevant legislation regulating the processing – e.g., the GDPR, the Data Protection and Law Enforcement Directive, etc., or
- Source of the examples – e.g., law, literature, own experience, etc.

The database could be made available through a dedicated interface (software) to facilitate the work of assessors. To be user friendly, the interface should be simple, restricting the input that is required to the minimum necessary to return useful results. At the same time, a user should be guided to provide adequate information to return relevant results. First, users would be requested to provide a short summary of their processing operations. While this could be entered in free text, it should nevertheless include certain minimal necessary elements, such as contextual description (e.g., nature, scope, purposes) and technical description (e.g., categories of personal data) of their processing operations. In addition, users could apply additional filters based on the above-mentioned keywords (tags).

The search would return a report, containing a list of relevant negative consequence, each of them described in an 'item card'. For example, based on the negative consequences mentioned in the CJEU case of *Sovim,*[109] such an 'item card' could include the following information:

- Name of the negative consequence – abduction,
- Description – the data subject and "his family would be kidnapped while travelling or staying in Africa",
- Classification in a typology:
  - Consequence pertaining to an individual,
  - Objective consequence,
  - Substantive,
  - Material,
- Categories of personal data processed – surname(s), forename(s), nationality, date of birth, place of birth, country of residence, complete address (private or business), nature and extent of the beneficial interests held,
- Special categories of personal data – no,
- Types of processing activities – collection, storage, making available,
- Categories of affected people – specific individuals (business owners), family members,
- Vulnerable people – no,
- Sector of governance or economy – public administration,
- Type of technology – Internet,
- Context of the processing – fight against serious crime and terrorism,
- Indicators of high risk – serious interference with human rights,
- Technical characteristics of the data – plain text,
- Relevant legislation – Directive 2018/843,
- Source – *Sovim*, AG Opinion, § 30.

4.3 Sources

The proposed database is a 'living' instrument that is continuously fed with experience (e.g., with each DPIA process concluded), and adapts to developments in society, economy and technology. In addition to the sources identified earlier in this paper (legislation, jurisprudence, doctrine, etc.), we consider certain supplementary sources useful.

[109] *Supra* (n 86).

First, a database of negative consequences could be fed with the aid of future studies and foresight activities, which "encompass a range of activities centred around understanding new technology developments, and anticipate their potential effects and impacts";[110] these often identify possible harms or damage from new and emerging technologies.[111] Among the many roles they play,[112] several DPAs have already used technology foresight to engage in education, consultation and advice, e.g., the European Data Protection Supervisor (EDPS) regularly publishes its Tech Sonar.[113]

The second source could be their own experience, as organisations conduct DPIA processes and moreover frequently maintain their own risk registers. Similarly, a 'chronicle' of data protection news could serve as a third source as many organisations continuously monitor (legal) developments in the area of privacy and personal data protection. Professional press, newsletters and other media outlets often illustrate negative consequences, from data breaches[114] to the harm from peeping from an art gallery terrace into someone's home,[115] to infer some (intimate) details from someone's patterns of watching television on demand.[116]

Fourth, some negative consequences could be inspired or inferred from popular science books or from dystopian, speculative fiction dealing with (un)intended effects of science and technology. Their added value lies in their ability to capture the imagination and open wider horizons of understanding of what could possibly go wrong, often "in ways that conventional academic papers often cannot, or at least typically do not".[117] Our favourite examples,[118] amongst popular science writings, include Negroponte's *Being Digital*[119] or Naughton's *A Brief History of Tomorrow*.[120] Amongst dystopian fiction, these range from Shelley's *Frankenstein* (1818), Huxley's *Brave New World* (1931), Orwell's *1984* (1948), Bradbury's *Fahrenheit 451* (1953), Atwood's *The Handmaid's Tale* (1985) to Egger's *The Circle* (2013). Examples from cinema include (dramatized) documentaries, e.g. Bond's *Erasing David* (2010), Poitras' *Citizenfour* (2014) or Ajana and Albrechtslund's *Surveillance Culture* (2017)[121] as well as films such as Spielberg's adaptation of Dick's *Minority Report (*2002), Niccol's *Gattaca* (1997), Wimmer's *Equilibrium* (2002), Garland's *Ex Machina* (2014), Brooker's on-going television series *Black Mirror* (2011-) or Financial Times' *People You May Know* (2021).[122]

More broadly, to be as complete as possible, an inventory of negative consequences could benefit from (a degree of) crowdsourcing. A database could take the form of a 'wiki' that is continuously updated with the input from assessors upon conclusion of their DPIA processes, with the data protection community able to provide input and feedback on each negative consequence. Furthermore, the public at large could also provide their input. Contributions to the inventory would be reviewed and moderated, multi-lingual, and

[110] David Barnard-Wills, 'The Technology Foresight Activities of European Union Data Protection Authorities' (2017) 116 *Technological Forecasting and Social Change* 142 <http://dx.doi.org/10.1016/j.techfore.2016.08.032> accessed 3 September 2024.

[111] Alessandro Ortalda, Stefano Leucci and Gabriele Rizzo, 'Anticipating Compliance. An Exploration of Foresight Initiatives in Data Protection' (2024) <https://brusselsprivacyhub.com/wp-content/uploads/2024/04/Ortalda-et-al_Anticipating-compliance.pdf> accessed 3 September 2024.

[112] Colin J. Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press 2006) 107–16.

[113] Cf. European Data Protection Supervisor, 'TechSonar' <https://edps.europa.eu/data-protection/technology-monitoring/techsonar_en> accessed 30 September 2024.

[114] Cf. e.g., Wikipedia, 'List of Data Breaches' <https://en.wikipedia.org/wiki/List_of_data_breaches> accessed 30 September 2024.

[115] E.g., *Fearn & Ors v Board of Trustees of the Tate Gallery* [2023] UKSC 4 (01 February 2023). Cf. also: Ollie Pritchard-Jones, 'Tate Modern: Flat Owners Win Viewing Platform Privacy Case' (BBC News, 1 February 2023) <https://www.bbc.com/news/uk-england-london-64481260> accessed 30 September 2024.

[116] E.g., Matthew Gault, 'Netflix Has Saved Every Choice You've Ever Made in "Black Mirror: Bandersnatch"' (Vice, 12 February 2019) <https://www.vice.com/en/article/netflix-has-saved-every-choice-youve-ever-made-in-black-mirror-bandersnatch> accessed 30 September 2024.

[117] Susan Cahill and Bryce Newell, 'Surveillance Stories: Imagining Surveillance Futures' (2021) 19(4) *Surveillance & Society* 412-413 <https://doi.org/10.24908/ss.v19i4.15189> accessed 3 October 2024.

[118] We set aside their (artistic) evaluation.

[119] Nicholas Negroponte, *Being Digital* (1st edn, Knopf 1995).

[120] John Naughton, *A Brief History of the Future: Origins of the Internet* (Phoenix 1999).

[121] Cf. Anders Albrechtslund, *Surveillance Culture* (2017) <https://www.youtube.com/watch?v=arplOSR1NsY> accessed 3 October 2024.

[122] Cf. Financial Times, *People You May Know. An FT Film written by James Graham, FT Standpoint* (21 May 2021) <https://www.ft.com/video/0685a4ba-7b0b-442b-b38e-3f73101a6943> accessed 3 October 2024.

be made openly accessible, under an appropriate copyright licence (e.g., Creative Commons). Academia – through e.g., EU research funding – and/or the EDPS or the EDPB would be best placed to run such a database – or sector-specific databases – in the EU context.[123]

4.4 Discussion

The innovative character of our method lies in the combination of a deductive (top-down) approach, which relies on expertise, stakeholder input and human creativity using known typologies and enumerations, with an inductive (bottom-up) approach, which relies on a database of known possible negative consequences.

Our method enables identification of negative consequences in a cost-effective and more comprehensive way, covering many technologies and situations. Moreover, it contributes towards the objectivity of an assessment. It allows the spotting of emerging legal trends and therefore helps to anticipate consequences that may not be readily apparent. Our method also lays the foundation for the determination – in the subsequent stages – of the likelihood (probability) and severity of risks to the rights (e.g., if an event has occurred previously, the experience of dealing with it, especially if by a court or a DPA, will be relevant for the determination of likelihood and severity). An additional benefit of our method is that it assists in the choice of appropriate mitigation measures for risks, tailored to the complexity of a given processing operation, e.g., for a processing involving both vulnerable and non-vulnerable data subjects, different measures would be appropriate for different groups.

Consistent with best practice for impact assessment,[124] external assessors – being typically neutral and more critical – are best placed to identify negative consequences. Consultations with data subjects, their representatives (Article 35(9)) and – possibly – other stakeholders further add to the quality of the process.

5 Concluding remarks

In this paper, we contribute to the clarification of the concept of risk to the rights and its identification in EU data protection law.

Appropriately identifying risk – and, more broadly, negative consequences – in data protection practice is critical. It contributes to a high level of protection of fundamental rights. From the perspective of an organisation, failure to identify risks that a controller could or should have known can be costly, e.g., when a risk materialises or when a DPA or a court reviews the identified risks and determines that important risks have been omitted, imposing a fine and damaging reputation. Yet there always might be some negative consequences that the organisation 'should have known' and that could reflect poorly on controllers if a DPA or a court finds a lack of due diligence.

While focused on EU data protection law, our paper's findings are applicable *mutatis mutandis* to related domains, wherever the RBA underscores the (personal) data protection system. In particular, the nascent AI law and the newly introduced FRIA could benefit from the experience of the DPIA.[125] Under the AI Act, not only do both processes rely on the concept of risk, but also – if some obligations are already met through a DPIA – the FRIA is required to "complement" that DPIA.[126]

[123] It is not uncommon that public authorities offer such resource centres for various types and domains of impact assessment. E.g., in the US, the Environmental Protection Agency (EPA) offers the Environmental Impact Statement (EIS) Database; cf. US Environmental Protection Agency, *Environmental Impact Statement (EIS) Database* <https://cdxapps.epa.gov/cdx-enepa-II/public/action/eis/search> accessed 3 October 2024.

[124] Kloza and others, 'The Concept of Impact Assessment' (n 7).

[125] Article 27, AI Act. Cf. also Article 16, Draft Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (Council of Europe, Strasbourg, 18 December 2023) CAI(2023)28 <https://rm.coe.int/cai-2023-28-draft-framework-convention/1680ade043> accessed 1 October 2024; Point 6(l), *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*, United Nations, 11 March 2024, A/78/L.49.

[126] Article 27(3), AI Act.

Nonetheless, as the scope of our paper is limited to the concept of risk and its identification, further research on other key elements of risk in EU data protection law is indispensable.[127] These include its analysis and evaluation (e.g., likelihood (probability) and severity) and its treatment (i.e., a list of possible appropriate measures to address such risk, in order to minimise or even avoid negative consequences). Public participation in risk assessment (cf. Article 35(9)) requires further research too.

All in all, the effectiveness of the RBA – and, more broadly, the level of protection of fundamental rights and legal compliance – is highly dependent on an appropriate understanding of risk and its assessment.

Acknowledgements

For their useful comments, we thank Arian Birth, Jo Dishington, Guglielmo Finotti, César Augusto Fontanillo López, Lina Jasmontaitė-Zaniewicz, Mercedes Llano Areilza, Ross McKean, Órla Murnaghan, Kajetan Ostoja-Ciemny, Juraj Sajfert as well as three anonymous reviewers. We also gratefully acknowledge the feedback received from Thomas Haley and the participants of the Privacy Law Scholars Conference (PLSC) held at Georgetown University Law Center in Washington, DC on 30-31 May 2024. This article contains solely our personal views and not those of any organisation any of us may be affiliated with. Errors of fact, taste or judgement are, needless to say, ours.

[127] For a 'wish-list' for DPIA under the GDPR, cf. e.g., Section IV in: Dariusz Kloza and others, 'Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals' (VUB 2017) 4 <https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf> accessed 1 October 2024.