THE DATA PROTECTION IMPACT ASSESSMENT

What can it contribute to data protection?

Claudia Quelle

Thesis for the Research Master in Law and the Master's program Law and Technology 2013-2015

THE DATA PROTECTION IMPACT ASSESSMENT: WHAT CAN IT CONTRIBUTE TO DATA PROTECTION?

Thesis for the Research Master in Law and the Master's program Law and Technology 2013-2015

Claudia Quelle

17 September 2015

Supervisors:

Prof. Dr. Ronald Leenes
Prof. Dr. Bert-Jaap Koops
Dr. Koen Van Aeken

TABLE OF CONTENTS

I Introduction

1.1 Background

The upcoming General Data Protection Regulation (**GDPR**) will bring about a number of changes in data protection law, hopefully bringing about better protection for individuals and providing a legal framework which is easier to comply with and to enforce. The current leading legal framework, The Data Protection Directive, entered into force in 1995. In the meantime, 'rapid technological developments' caused the European Commission concern about fragmentation between Member States, legal uncertainty, and the widespread perception that online activity is not without significant risks.[1] New technologies challenge the effectiveness of data protection law.[2] The General Data Protection Regulation, proposed by the European Commission and amended by the European Parliament in 2014 and by the Council in 2015, is meant to address these concerns by building a stronger and more coherent data protection framework.[3]

Recital 9 of the GDPR states that effective protection of personal data requires a strengthening and detailing of 1) data subject rights and 2) of the obligations of controllers, together with powers of monitoring and ensuring compliance. A useful distinction to briefly capture data protection law and its reform is indeed between provisions aimed at empowering the individuals whose data is being processed (**data subjects**), most notably consent and data subject rights, and rules aimed at increasing the responsibility of the entities responsible for the processing (**controllers**),[4] such as the principles of proportionality and accountability.[5] The consent of individuals is a frequently relied-on ground to legitimize the processing of personal information – and in many cases, it is the only available legal ground.[6] Individuals are further granted a number of rights, including the right to be informed of a number of categories of information,[7] to access, rectify or erase personal data,[8] and to object to certain automated processing operations, and the ability to withdraw your consent.[9] The General Data Protection Regulation extends the definition of consent and data subject rights.[10] It also adds a number of duties for the controller. Controllers are required to build compliance into the technology from

---

[1] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final, 1-2. **In the following, I shall refer to the GDPR when discussing the legal provisions of the proposal, mentioning the version under discussion if there are relevant differences between the versions which have currently been proposed.**

[2] Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union' COM(2010) 609 final.

[3] COM (2012) 11, 1-2.

[4] **Similarly, Borgesius distinguishes between rules that aim for control and rules that aim for protection.** F Borgesius, 'Improving privacy protection in the area of behavioural targeting' (PhD thesis, University of Amsterdam 2014) ch 4.5.

[5] e.g. GDPR, arts 5(1)(f) and 22 (removed and weakened in the Council version); Article 29 Working Party, 'Opinion 03/2010 on the principle of accountability'; C Tranberg, 'Proportionality and data protection in the case law of the European Court of Justice' (2011) 1(4) International Data Privacy Law 239.

[6] Data Protection Directive (DPD), arts 7(a) and 8(2)(a); ePrivacy Directive, arts 6, 9 and 13.

[7] DPD, art 10..

[8] DPD, art 12.

[9] DPD, art 15; Article 29 Working Party 'Opinion 15/2011 on the definition of consent'.

[10] GDPR, rec 25 and arts 4(8), 7, 17 and 19.

the start and make the default setting data protection friendly (privacy by design and privacy by default), appoint a data protection officer, and conduct a 'data protection impact assessment'.[11]

The provisions of user empowerment offer data subjects a very limited amount of control in practice. In the age of ubiquitous data collection, informed consent and data subject rights only enable individuals to review and influence data processing operations to a very limited extent. According to Koops, this is the death of data protection – a blow which the reform does not address.[12] Many authors explain that individuals do not have enough time to consider each processing operation because we engage with services which collect data so frequently, or that we at least lack the will to make time for this burden – and understandably so, considering how uneconomical it would be.[13] Moreover, individuals do not comprehend what it means to consent to the data processing and lack the rationality to base this decision on cost-benefit analyses. It is difficult, if not impossible, to make data processing operations transparent. This type of analysis may not even be explainable in human language.[14] The information could be presented in accessible ways, for example through logo's or seals, but this 'conflicts with fully informing people about the consequences of giving up data, which are quite complex if explained in sufficient detail to be meaningful'.[15] It is very difficult to adequately estimate the effect of the choice to share this one piece of information because these effects result from the totality of the information which is available to the controller; different sources are combined. Information can also be inferred from other available data, so that data shared by others can be used to infer things about you.[16] We cannot oversee what information has been shared or can be inferred, nor what it will be used for. Even if the information is informative and understandable, a number of cognitive limitations and biases are likely to skew the decision-making process. For example, individuals tend to go with the default setting and focus on short-term effects.[17]

Data subject rights cannot be of help if the data subject has no knowledge of the data processing or the resulting impact, or does not know who should be addressed to resolve this. Individuals (generally) have no knowledge of the profile that is used to analyse their data or when it is invoked.[18] As a result, only the most visible and directly harmful effects are likely to be addressed. Even if the exercise of the user empowerment provisions was not hindered by a lack of transparency, the normative argument can be made that data subjects should not be placed

[11] GDPR, arts 23, 33 and 35.
[12] B Koops, 'The trouble with European data protection law' (2014) International Data Privacy Law, 2-4.
[13] D Solove, 'Introduction Privacy self-management and the consent dilemma' (2013) 126 Harvard Law Review 1880, 1884; B Van Alsenoy, E Kosta and J Dumortier, 'Privacy notices versus informational self-determination: Minding the gap' (2014)28 International Review of Law, Computers & Technology 185, 189.
[14] T Zarsky, 'Transparent Predictions' (2013)4 University of Illinois Law Review 1503, 1503; Solove (2013) 1885.
[15] Solove (2013) 1885.
[16] M Hildebrandt, 'Who is Profiling Who? Invisible Visibility' in S Gutwirth, Y Poullet, P De Hert, C De Terwangne and S Nouwt (eds), *Reinventing Data Protection?* (Springer 2009) 243; D Le Métayer and J Le Clainche, 'From the Protection of Data to the Protection of Individuals: Extending the Application of Non-discrimination Principles' in S Gutwirth, R Leenes, P De Hert and S Poullet (eds), *European Data Protection: In Good Health?* (Springer 2012) 323; Solove (2013) 1889-1891.
[17] Solove (2013) 1891; Van Alsenoy, Kosta and Dumortier (2014) 190.
[18] R Leenes, 'Reply by Ronald Leenes (TILT): Addressing the obscurity of data clouds' (2009) TILT Law & Technology Working Paper No. 012/2009 17 April 2009, Version: 1.0 & Tilburg University Legal Studies Working Paper No. 008/2009, < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1393193> accessed 30 July 2015, 6; M van Otterlo, 'Automated Experimentation in Walden 3.0.: The Next Step in Profiling, Predicting, Control and Surveillance (2014)12(2) Surveillance and Society 255, 261.

under the burden of regulating data processing operations and preventing unwanted consequences thereof, as this task (partly) befalls to controllers and enforcement authorities.[19]

If anything, these limits of user empowerment increase the importance of the responsibilities of controllers. Data protection law does accord controllers some of the burden of overseeing their own processing operations. This thesis concerns one of the provisions which might place upon controllers a responsibility for the way in which they collect, infer, use and share personal data: the data protection impact assessment. This impact assessment has been developed and used in the Anglo-Saxon world under the heading of "Privacy Impact Assessment",[20] and is now to become mandatory in the EU. It is mandated by Article 33 of the Proposed Data Protection Regulation in certain risky cases, involving risks to the rights and freedoms of data subjects/individuals.[21] It requires controllers to assess the impact of the processing operations on (the right to) the protection of personal data before these operations are commenced. They also need to describe the measures which are envisaged to address the risks to the rights and freedoms of data subjects.[22] The data protection impact assessment seems to be an important nexus in the envisaged reform. Recital 71a of the Parliament's version of the GDPR even describes the impact assessment as 'the essential core of any sustainable data protection framework'. According to the International Working Group on Telecommunications, the impact assessment is an important tool to solve the challenges of big data and retain the confidence of data subjects.[23] The data protection impact assessment could potentially be a valuable addition to the responsibility of controllers for the way in which they process personal data and the impact thereof, possibly enabling compliance and enforcement and compensating for the limits of user empowerment described above. As such, it is a highly relevant topic of research.

1.2 Research problem and research objectives

However, while the Parliament and the International Working Group on Telecommunications see the data protection impact assessment as a valuable addition to data protection regulation, it is not yet clear what it adds to this body of law. A number of provisions already require controllers to assess the impact of their processing operations. If a controller wishes to process previously collected personal data for a purpose other than that for which it was collected, it must apply a test for compatible use, which contains considerations regarding the impact on the data subjects and the ways in which any undue impact is prevented through additional measures.[24] Moreover, the legal ground of Article 7(f) – often relied on if valid consent is not obtained - requires, amongst other things, an assessment of the impact of the processing on the data subject.[25] Furthermore, Article 30 requires controllers and processors to take measures to

[19] M Kightlinger, 'Twilight of the idols? EU internet privacy and the post enlightenment paradigm' (2007-2008) 14(1) Columbia Journal of European Law 62, 91; Le Métayer and Le Clainche (2012) 328; L Moerel, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof' (inaugural lecture, Tilburg University 2014) 59.
[20] R Clarke, 'Privacy impact assessment: Its origins and development' (2009) 25(2) Computer Law & Security Review 123, 127-129.
[21] GDPR, art 33; GDPR Parliament version, art 32a.
[22] GDPR, arts 33(1) and 33(3).
[23] International Working Group on Data Protection in Telecommunications, 'Working Paper on Big Data and Privacy' (55th Meeting, 2014) para 50-52.
[24] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' 25-27.
[25] Article 29 Working Party, 'Opinion 26/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' 36-41.

achieve a level of security, so as to address security risks.[26] In the UK interpretation of the requirement that data must be processed fairly, this principle includes the requirement that controllers do not 'use the data in ways that have unjustified adverse effects on the individuals concerned'.[27] A similar outcome is reached through a different route by the Dutch Supreme Court in its finding that the proportionality principle of Article 8 ECHR is directly applicable, so that all interferences with the interests of the data subject need to be proportionate to the purpose of the processing – a balancing test which is to be applied even if a legal ground is present.[28]

A preliminary analysis shows that the data protection impact assessment could have a number of forms and functions. The specificities of what the DPIA entails differs in each version of the General Data Protection Regulation. This thesis will therefore explore the various forms of the data protection impact assessment which have been proposed by the European institutions and analyse what they potentially entail and contribute. These different forms of the data protection impact assessment could have a number of functions. The DPIA could help controllers establish compliance with the provisions of substantive law, including those discussed above, and/or help the authorities hold them accountable for their decisions ex post. In other words, the data protection impact assessment could guide controllers to apply the complicated and fragmented set of rules that is data protection law so as to achieve compliance, or reduce the burden data protection authorities have in reviewing whether controllers are compliant**.** The hypothesis is that the DPIA functions to help establish and enforce compliance. But does the data protection impact assessment serve only to make data protection law easier to apply and enforce, or does it bring in new norms to be abided by? In its narrowest form, it concerns a data protection compliance checklist, to be checked before processing operations start,[29] but in a broader conception of the privacy impact assessment the level of data security, the privacy-friendliness, respect for the right to data protection, or generally the compatibility with human rights is also tested.[30] The privacy impact assessment may indeed be seen as going beyond compliance with data protection law.[31] As PIAF notes, risk mitigation is a crucial element of the privacy impact assessment, and it 'cannot be equalled to legal compliance check since the former is broader in scope than the latter. Risk management goes beyond merely assessing the risks of non-compliance with relevant laws and examines all possible risks to the protection of privacy and

---

[26] GDPR, art 30.

[27] Information Commissioner's Office, 'The Guide to Data Protection' (version 2.2.4, 31 March 2015) <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/> accessed 25 July 2015, 16.

[28] Hoge Raad 9 September 2011 ECLI:NL:HR:2011:BQ8097 para 3.3.

[29] **Oetzel and Spiekermann argue that compliance with data protection law sufficiently eliminates the privacy threats known to be caused by IT systems, so that in this context 'data protection law and privacy law are effectively the same'**. **This is not widely accepted**. M Oetzel and S Spiekermann, 'A systematic methodology for privacy impact assessments: a design science approach'(2014) 23 European Journal of Information Systems 126, 130-131.

[30] D Wright, M Friedewald, S Gutwirth and others, 'Sorting out smart surveillance' (2010) 26(4) Computer Law & Security Review 343, 353; P De Hert, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments', in D Wright and P De Hert (eds), Privacy Impact Assessment (Springer 2012) 72-74; R Finn, R Rodrigues and D Wright, 'A Compararive Analysis of Privacy Impact Assessment in Six Countries', (2013) 9(1) Journal of Contemporary European Research 160; K Wadhwa and R Rodrigues, 'Evaluating privacy impact assessments' (2013) 26 Innovation: The European Journal of Social Science Research 161, 168; Information Commissioner's Office, 'Conducting privacy impact assessments: code of practice' (2014) < https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/> accessed 15 August 2015, 6-8.

[31] Wright, Friedewald and Gutwirth (2010) 353; De Hert (2012) 38; Finn, Rodrigues and Wright (2013) 162. cf R Weber, 'Symposium on EU Data Protection Reform: Privacy management practices in the proposed EU regulation' (2014) 4(4) International Data Privacy Law 290, 294.

personal data'.[32] The "extra" has been argued to lie, for example, in an evaluation of privacy and security safeguards, or even of 'any potential consequences for the data subjects'.[33] The question is what the GDPR has made of risk mitigation. Perhaps the DPIA introduces an independent requirement to mitigate "risky" processing operations.

For all these different forms and functions, the contribution can also lie in the way in which the impact assessment regulates behaviour. Even if the data protection impact assessment makes no substantive additions to the rest of data protection law, it can still complement the rest of the regime from the perspective of regulatory studies. The contribution of the data protection impact assessment may (partly) lie in the way in which it achieves a certain regulatory outcome, for example by more effectively getting controllers to achieve compliance with the substantive norms of the GDPR. The ability of regulation to achieve a desired regulatory outcome is examined in a strand of literature which may be called the multi-disciplinary field of regulatory studies or regulation & governance.[34] Legal norms and regulatory goals can be formulated or put into regulation in different ways, using different modalities, and they can be enforced in different manners, possibly with different results.[35] In other words, the regulatory tools and techniques and the enforcement strategies which are employed may affect the capacity of the regulation to achieve a desired behavioural change. Several different categories of regulation have been proposed in the field of regulatory studies, e.g. command and control or incentive-based regimes, principles-based regulation, smart regulation, meta-regulation, responsive regulation, and risk-based regulation.[36]

While these types are oversimplifications, they can serve as heuristic devices to analyse the goals, strengths and weaknesses of the data protection impact assessment.[37] For example, an analysis of the impact assessment as a form of risk-based regulation will uncover that the impact assessment could function as a means for supervisory authorities to focus their efforts on risky conduct, but that this is not likely to form a successful contribution to data protection because the DPIA reports will not be uniform; there is no agreement on how to identify and score risks, which is a subjective exercise in any case. This approach will introduce an interdisciplinary perspective, which focuses on the way in which the impact assessment regulates behaviour. The perspective of regulatory studies is assumed to be helpful in uncovering the possible functions of the data protection impact assessment precisely because the DPIA may be (in part) a regulatory tool to establish compliance, enforce the law, or bring about respect for the right to personal data protection and other rights and freedoms. This thesis will therefore access the field of regulation and governance to explore the various ways in which the impact assessment can be categorised and what the strengths and weaknesses of these types of regulation are with a view to their ability to effectuate the regulatory outcome.

---

[32] PIAF 'Deliverable D3: Recommendations for a Privacy Impact Assessment Framework for the European Union' (2012), 21.
[33] International Working Group on Data Protection in Telecommunications (2014) para 52.
[34] Wiley Online Library, 'Regulation & Governance' <http://onlinelibrary.wiley.com/journal/10.1111/%28ISSN%291748-5991/homepage/ProductInformation.html> (accessed 17 August 2015); K Van Aeken, 'Regulation & governance-onderzoek in het rechtenonderwijs in Nederland: Sranger in a strange land?' 2015(2) RegelMaat 95, 98. cf B Morgan and K Yeung, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press 2007) ch 1; R Baldwin; M Cave and M Lodge, *Understanding Regulation: Theory, Strategy and Practice* (Oxford University Press 2012) 1-2.
[35] Morgan and Yeung (2007) ch 3; J Black, M Hopper and C Band, 'Making a success of Principles-based regulation' (2007) 1(3) Law and Financial Markets Review 191, 194; Baldwin, Cave and Lodge (2012) ch 7.
[36] Morgan and Yeung (2007) 80, 124 and 193; Baldwin, Cave and Lodge (2012) 105, 137, 259, 281 and 296.
[37] cf Morgan and Yeung (2007) 9.

In short, while the data protection impact assessment could potentially become a valuable contribution to data protection law, possibly as a potential compensation for the limits of user empowerment, there is a lack of clarity concerning what form it may take and what it can add to data protection. This research wishes to explore what the data protection impact assessment can contribute to data protection regulation by analysing what it may entail both legally and for regulatory compliance. It will be analysed what various forms and functions the data protection impact assessment of Article 33 GDPR can take. As argued above, a preliminary analysis shows that, because the impact assessment overlaps with other provisions, it may serve as a tool for controllers to establish compliance. It may also serve help controllers to review whether controllers comply with the GDPR, enabling them to hold controllers to account for acts of non-compliance. However, the impact assessment may also add substantive legal norms or, in any case, bring them within the realm of the GDPR. In these scenarios its added value may also lie in the way in which data processing operations are regulated through Article 33. It can be seen as a way of regulating which is "meta" or "risk-based", to name a few. Each of these categorisations cast a certain light on the functions of the impact assessment, allowing it to be investigated from a different angle.

1.3 Research questions and scope and outline of the research

Capturing the aim of analysing the different forms and functions of the data protection impact assessment from a legal perspective and the perspective of regulatory studies so as to explore what the impact assessment may bring to data protection, the research question is as follows:

What can the data protection impact assessment potentially contribute to data protection regulation?

Legal perspective:

1. **What does the data protection impact assessment entail according to the different versions of the GDPR?**
2. **What are the potential functions of the data protection impact assessment in light of the legal analysis?**

Perspective of regulatory studies:

3. **What are relevant types of regulation and what are their characteristics?**
4. **As what kinds of regulation can the data protection impact assessment be characterised?**
5. **What are the strengths and weaknesses of these types of regulation regarding their ability to effectuate a regulatory outcome? What does this entail for the potential functions of the data protection impact assessment?**

The sub-questions form an outline of the topics which will be researched. After the legal analysis, the perspective of regulatory studies is adopted. The theoretical framework within which this analysis takes place is introduced in section 1.3.2.

Twining has distinguished three primary uses of the term "**function**": social consequences or effects, purposes or goals, and purposes plus effects, i.e. those consequences which were

intended.[38] This thesis is concerned with functions in the first sense of the word, whereby the term is used to refer to an effect which the DPIA *can* have, not an effect which it *will* always display. The effect does not need to arise in every situation for it to be a function.[39] In other words, this thesis looks at what the DPIA can do when it is adopted, not with what it is intended to do by the European legislator. A function may thus be intended or accidental.[40] As noted by Twining, it is problematic to attribute purpose or intent to the group of people which together compose this entity called "the legislator".[41] However, the category of social effects is narrowed down; this thesis is only concerned with functions, not with dysfunctions. This means that only *valuable* effects are taken into consideration, which may coincide with the allegedly *intended* effects. The adopted perspective is that of the legislator: it is researched what the DPIA can do for data protection – the aims of which are, according to the legislator, the protection of the rights and freedoms of individuals, particularly the right to the protection of personal data, and of the free movement of information -[42] not what it can do for, e.g., the controller's reputation management. Because the GDPR has not yet been finalised and the form of the DPIA has not yet been decided, these functions are, at this point in time, still potential.

1.3.1 Sub-question 1 and 2

First, a legal analysis of the data protection impact assessment will be conducted. The focus will be on Article 33 as it appears in the different versions of the GDPR. At the moment of writing (Summer 2015), the European Commission, the European Parliament and the Council of the European Union have each released a version and are now to reach agreement on the final document. This thesis will therefore consider all three versions, according weight especially to the similarities, but also noting the differences.

The data protection impact assessment can be seen as part of a larger "compliance program", including the obligation to appoint a data protection officer and to engage in prior consultation.[43] While the focus of this thesis is not on this compliance program as a whole, but rather on the data protection impact assessment alone, these surrounding obligations will be taken into consideration if they have a bearing on the function of the impact assessment; e.g. if the result of the impact assessment determines whether the controller has to do a prior check with the supervisory authority and/or the data protection officer.[44] Neighbouring obligations, such as privacy by design and by default and proportionality, will also be taken into consideration.

For an adequate understanding of Article 33, it is necessary to consider (the right to) the protection of personal data. All three versions of the GDPR consider that the assessment is of the impact on of the envisaged processing operations on the protection of personal data or the right to the protection of personal data, although the Parliament refers also to the impact on the rights and freedoms of the data subjects. This thesis will therefore research what the protection of

---

[38] W Twining, 'A Post-Westphalian Conception of Law' (2003) 37(1) Law & Society Review 199, 213-314.
[39] See also section 2.3.1.3: **the aim of this research is not to conclude on the effectiveness of the DPIA, but rather on the valuable effects which it may have.**
[40] cf R Schwitters, *Recht en samenleving in verandering: een inleiding in de rechtssociologie* (Kluwer 2008) 27.
[41] Twining (2003) 213, footnote 26.
[42] GDPR, art 1. See also DPD, art 1; section 2.4.1.
[43] P Balboni, D Cooper, R Imperiali and M Macenaite, 'Legitimate interest of the data controller. New data protection paradigm: legitimacy grounded on appropriate protection' (2013) 3(4) International Data Privacy Law 244; 258; Weber (2014).
[44] GDPR, art 34(2).

personal data, and especially the accompanying right, entails. It will do so in relation to the right to privacy, as these rights have or had a special link.[45]Because the impact assessment includes a description of the risk assessment and measures for risk mitigation,[46] it is also necessary to have an understanding of the terms "risk" and also "precaution".[47] For this purpose, a conceptual analysis of these terms will be conducted and used for the legal analysis of the impact assessment.

The legal description will show what the data protection impact assessment requires. It tests and answers the hypothesis that the DPIA can help controllers establish compliance and can help supervisory authorities hold them to account, and the question whether it also sets "extra" standards regarding risk mitigation. It also lays the groundwork to test other functions which the various components might fulfil; it is the input for the second sub-question, for which the functions of the data protection impact assessment will be explored in light of the legal analysis.

1.3.2 Sub-question 3, 4 and 5

To analyse what the data protection impact assessment contributes to data protection regulation, it will be explored whether its contribution lies in the possibilities it offers in regulating behaviour. This is reflected in sub-question three, four and five. This part of the thesis overlaps with the conclusions on the functions of the DPIA presented under sub-question 2. It is a continuation of the effort to identify the functions of the data protection impact assessment, now undertaken by employing the perspective of regulatory studies.

1.3.2.1 Theoretical framework

Regulatory scholarship challenges the state-centric and rule-centric notion of regulation which may be familiar to traditional lawyers. It highlights the fact that the authority of the state is limited, that legal rules are never fully effective, and that alternative techniques for policy implementation exist.[48] This is summed up by Black's decentred understanding of regulation. She disputes the presumption that the state commands and controls, is the only entity which does so, and does so effectively.[49] The state's capacity to regulate by itself is limited by many different factors, of which Black enumerates the following. Firstly, the problems in society which the state wants (or should want)[50] to address are caused by many different factors and are therefore not easily tackled.[51] Indeed, since rationality is bounded, decision-making on the best way to regulate is necessarily limited.[52] The state often does not possess the knowledge needed

---

[45] DPD, art 1(1); G González Fuster and S Gutwirth, 'Opening up personal data protection: a conceptual controversy' (2013) 29(5) Computer Law & Security Review 531, 536; G González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) 214. See also R Gellert and S Gutwirth, 'The legal construction of privacy and data protection' (2013) 29(5) Computer Law & Security Review 522.
[46] GDPR, art 33(3).
[47] cf R Gellert, 'Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative' (2015) 5(1) International Data Privacy Law 3.
[48] Morgan and Yeung (2007) 4.
[49]J Black, 'Critical Reflections on Regulation' (2002) 27 Australian Journal of Legal Philosopy, 3; Morgan and Yeung (2007) 4.
[50] **According to interest group theories, state regulation is never only about promoting public interest. Regulatory developments are rather driven by the concerns of politicians, influential interest groups or of economically powerful actors, whom all seek to maximise their self-interest, leading to regulatory capture.** (Morgan and Yeung (2007) 43; Baldwin, Cave and Lodge (2012) 75).
[51] Black (2002) 4-5.
[52] Baldwin, Cave and Lodge (2012) 74.

to regulate effectively because knowledge is fragmented in society. According to some theories, it cannot possibly possess actual knowledge of the regulatee because he is always seen through the cognitive frame of the regulator.[53] Power, too, is fragmented: the state is not the only actor to have power in the Foucauldian sense of the word because the regulatory systems existing in social spheres influence social ordering in society.[54] Actors or systems in society are to some extent autonomous and ungovernable. They already regulate themselves, as a result of which "outside" regulation will never be fully effective. It will produce unintended effects.[55] Furthermore, social actors and the government are interdependent. In the process of regulation, the regulator and the regulatee are both involved. It is a two-way street. They both have needs and solutions to each others needs.[56] Irrespective of whether this is lamented as regulatory capture, public and private entities produce regulation together which then enjoys the state's authority to make and enforce binding rules.[57]

Systems theory plays a dominant role in this theoretical framework. Black refers to this autonomous and self-regulating nature as **autopoiesis**.[58] According to the legal theory of autopoiesis, subsystems are cognitively open but normatively closed: they perceive facts from outside, but they do so through the normative structure of the subsystem.[59] The subsystems are those of the political, the legal, the social and the economic.[60] Moore's term "**semi-autonomous social fields"** may be more fitting to describe regulation in society. The individual is part of many semi-autonomous social fields, each of which produces and enforces its own rules. They are not fully autonomous, however, because rules from surrounding fields – such as the field of the state – to some extent penetrate the social group.[61] In the words of Griffiths: '[i]t can regulate its internal affairs to a certain extent - maintain its own rules and [regulate] the penetration of competing external rules - but its members are also members of many other social fields and as such exposed to many other sources of regulation'.[62] Some fields can make its rules "stick" better than others.[63] As a result, data controllers operate within a "regulatory space" in which the state must compete with other regulatory orderings for social control.[64] Existing norms, as may be present in a corporate culture or in business practices, also regulate how people behave,[65] as do the market and architecture or code. Indeed, according to Lessig not only law, but also these other three modalities (social norms, the market, and code) regulate behaviour.[66] Some of these modalities may regulate through non-normative signals, that is signals which highlight not what

[53] Black (2002) 5.
[54] Black (2002) 5-6.
[55] Black (2002) 6. **This view is widely shared by systems theorists** (Morgan and Yeung (2007) 69).
[56] Black (2002) 7.
[57] Black (2002) 8.
[58] Black (2002) 5 and 7.
[59] C Scott, 'Regulation in the age of governance: The rise of the post-regulatory state' in J Jordana and D Levi-Faur, *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance* (Edward Elgar Publishing 2004) 151
[60] Scott (2004).
[61] J Griffiths, 'De sociale werking van het recht' in J Griffiths (ed), *De sociale werking van het recht. Een kennismaking met de rechtssociologie en rechtsantropologie* (Ars Aequi Libri 1996) 483.
[62] J Griffiths, 'The Social Working of Legal Rules' (2003) 48(1) Journal of Legal Pluralism & Unofficial Law 1, 24.
[63] Griffiths (2003) 27.
[64] C Parker, 'Reinventing regulation within the corporation: Compliance-oriented regulatory innovation' (2000) 32(5) Administration & Society 529, 532; Griffiths (2003) 27. See also L Hancher and M Moran, 'Organizing regulatory space' in R Baldwin, C Scott and C Hood, *A Reader on Regulation* (Oxford University Press 1989) 148-172; Baldwin, Cave and Lodge (2012) 64; Morgan and Yeung (2007) 59-60.
[65] Parker (2000) 532.
[66] L Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harvard Law Review 501, 506-507.

ought to be done but what can be done or is practical to do.[67] This means that a high price tag, a speed bump or a browser setting can regulate behaviour too.

This theoretical framework allows new visions on the role of law to emerge. Morgan and Yeung clarify that, rather than proscribing or prescribing certain conduct and threatening with sanctions if that command is violated ("law as threat"), the law can also create and police 'the boundaries of a space for free and secure interaction between participants' ("law as umpire").[68] A system of tradeable permits, for example, does not prohibit the regulated activity, but makes use of market mechanisms to achieve the desired result – but always within the boundaries dictated by law.[69] For Black, the decentred understanding brings about a normative view on the role of the state: it should decrease the use of law as threat. Truly 'decentred' strategies are hybrid (combining governmental and non-governmental actors), multi-faceted (using a number of different strategies simultaneously or sequentially), and they are indirect. The role of the government can be stronger or less strong; it can participate fully in rule-setting and rule-enforcement or be a guiding hand or a threatening shadow.[70] It is important, though, that the state makes use of the self-regulatory capacity of actors or systems to effectively govern 'at a distance'.[71] This decentred understanding distances itself from a top-down perspective in which regulation is the responsibility of the government, which is placed next to or above society.[72] Indeed, one of the challenges posed by regulatory scholarship to the lawyers' state-centric vision on regulation is that the state does not necessarily need to be considered 'the primary locus for articulating the collective goals of a community'.[73] Self-regulation is apparently accepted as legitimate, whereas traditional command-and-control type regulation is dismissed as ineffective. This thesis will consider command-based regulation as an option, making note of its strengths and weaknesses with regard to its effectiveness according to a wider body of literature, but it will not discuss whether self-regulation is legitimate; the focus is on effectiveness.[74]

The framework is also accompanied by a new definition of regulation. Hood and others present three possible definitions of **regulation**: it is either 'the presentation of rules and their subsequent enforcement usually by the state', or 'any form of state intervention in the economic activity of social actors', or it is 'any form of social control'.[75] Black's decentred understanding of regulation tries to let go of the state-centric nature of the first two definitions while avoiding the over-inclusiveness of the latter. It defines regulation as '*the sustained and focused attempt to alter the behaviour of others according to defined standards or purposes with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-*

---

[67] R Brownsword and M Goodwin, *Law and the Technologies of the Twenty-First Century* (Cambridge University Press 2012) 27-29.
[68] Morgan and Yeung (2007) 6.
[69] cf Morgan and Yeung (2007) 4-7. **The use of non-traditional modes of regulation is not necessarily less interventionist. Techno-regulation is a clear example in which the reach of the state can be both wider - almost everything can be designed - and more compulsive: it affects what behaviour regulatees can actually display by constraining what is possible rather than by inducing certain behaviour through carrots and sticks. See section 3.2.1.**
[70] Black (2002) 8-9.
[71] Black (2002) 7.
[72] M Oude Vrielink, 'Wanneer is zelfregulering een effectieve aanvulling op overheidsregulering?' in M Hertogh and H Weyers (eds), *Recht van onderop: Antwoorden uit de rechtssociologie* (Ars Aequi Libri 2011) 63-64.
[73] Morgan and Yeung (2007) 4.
[74] **The legitimacy of different types of regulation is beyond the scope of this thesis.**
[75] A Murray, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge Cavendish 2007) 22, footnote 2; Baldwin, Scott and Hood (1998) 4. See also Baldwin, Cave and Lodge (2012) 3.

setting, information-gathering and behaviour modification'.[76] However, this understanding of regulation is not widely adopted. Koop and Lodge have researched how the term "regulation" is actually used, and it turns out that many scholars do employ more or less traditional or legal-centric conceptualisations of regulation. They see "prototype regulation" as intentional and direct interventions of public-sector actors on the economic activities of private-sector actors which involve binding norm-setting, monitoring and sanctioning.[77] These definitions are a useful starting point to consider the dimensions along which an understanding of regulation may vary.

Firstly, regulation need not take the form of command-and-control rules which directly steer behaviour. The other modalities – according to Lessig: social norms, the market, and architecture or code – also regulate. Regulation is typically seen as consisting of three dimensions: a goal, standard, norm or rule is set; performance is monitored; and non-compliance or deviation is responded to.[78] However, under Black's definition efforts to steer behaviour indirectly, for example by steering the economy, can also be regulation.[79] Secondly, regulation can take place in various sub-systems or spheres. For many researchers, regulation is apparently limited to the economic activities of private actors. However, Black's definition does not include such a limitation. Many forms of government regulation also regulate other areas of society. Thirdly, under a decentred understanding also non-state actors are seen as regulators.[80] As noted, extra-legal modalities of regulation can be employed by the state to regulate behaviour, just like the state may promulgate and enforce prohibitions. However, these modalities can also regulate the behaviour of people in the absence of state intervention. Moreover, they can be harnessed by non-state actors too.[81] A voluntary company code is an example of a non-state command-and-control technique enforced through social interaction. Society-oriented researches may be interested in regulation taking place outside of the state, for example amongst citizens or between businesses and individuals.[82] Although not undertaken by the state, these forms of regulation do function against the background of the law's order and threat. Self-regulatory agreements may be enforceable as contracts and take place against the (implicit) threat of state intervention.[83]

If regulation is no longer purely a state activity, the question arises what regulation has become. Does regulation now encompass all mechanisms of social control, as under Hood's third definition?[84] This would include non-intentionality: cultural or social norms are also seen as regulation.[85] Black rejects such a wide definition by limiting regulation to the sustained and focused attempt with the intention of producing a broadly identified outcome. As a result, market forces, social forces and "code" an sich are not seen as regulation. They influence how

---

[76] Black (2002) 26; J Black, 'What is Regulatory Innovation' in J Black, M Lodge and M Thatcher (eds), *Regulatory Innovation* (Cheltenham 2005), 11.
[77] C Koop and M Lodge, 'What is regulation? An interdisciplinary concept analysis' (2015) Regulation & Governance 5 and 10-11.
[78] A Murray and C Scott, 'Controlling the New Media: Hybrid Responses to New Forms of Power' (2002)65 Modern Law Review 491; R Brownsword and M Goodwin, *Law and the Technologies of the Twenty-First Century* (Cambridge University Press 2012), 34.
[79] Koop and Lodge (2015) 4.
[80] J Black, 'Decentring regulation: Understanding the role of regulation and self-regulation in a "post-regulatory" world' (2001) 54(1) Current Legal Problems 103, 105.
[81] Black (2002) 3.
[82] Van Aeken (2015) 98.
[83] Morgan and Yeung (2007) 96, 106.
[84] Baldwin, Scott and Hood (1998) 4; Murray (2007) 22, footnote 2. See also R Baldwin, C Hood and H Rothstein, *The Government of Risk* (Oxford University Press 2001) 23; Morgan and Yeung (2007) 3; Van Aeken (2015) 98.
[85] Koop and Lodge (2015) 3-4.

regulation works and can be harnessed in efforts to alter behaviour, but are not defined as such.[86] However, the distinction between norms which are intentionally enforced over a period of time and those which are not, is not always straightforward. Is a company dress code intentionally enforced if colleagues consciously and systematically look askance at your informal attire? Is "code" regulation if the programmer made a conscious choice for a certain default option?

This thesis is about a legal instrument developed by the European legislature[87] to steer the behaviour of other actors, both public and private,[88] in a direct and/or indirect manner. An instrumental and legal perspective on regulation, according to which the law is one of the instruments of the state, and of the EU, to achieve regulatory goals by shaping the behaviour of regulatees, is therefore adopted.[89] Nonetheless, the theoretical framework above is used to acknowledge that the law can steer behaviour in many different ways, both direct and indirect; that it can do so by employing the self-regulatory capacity of actors; and that it does so within a busy regulatory space, as a result of which compliance is never perfect. Irrespective of whether social and cultural norms and technological frames are also "regulation", their regulating effect is taken into consideration.

1.3.2.2 Relevant types of regulation

The thesis will describe the relevant types of regulation which are commonly drawn in the field of regulatory studies. The categorisations employed by Morgan & Yeung and Baldwin, Cave & Lodge in their handbooks are taken as leading. Because the data protection impact assessment is a piece of government legislation, only types of regulation which fall under that umbrella are considered. This excludes regulation by non-state actors and pure self-regulation. It may include instruments which are not command-based and which may employ extra-legal modalities or sources of regulation – for example in the form of economic incentives. Types of regulation which are evidently not relevant will also be excluded. As a result, the following types will be discussed.

This thesis will first discuss regulatory instruments and techniques. This is one dimension according to which regulation can be qualified as being of a certain type. The different instruments which will be considered are **command, competition, consensus and communication.** In relation to command-based regulation, **principles-based regulation** (in which the norms which are commanded are couched in open terms) is discussed. **Enforced self-regulation** (Ayres and Braithwaite) is discussed as a type of self-regulation. The categories employed by Baldwin, Cave and Lodge generally fit within this model.[90] Hybrid forms are **responsive regulation** (Ayres and Braithwaite), **smart regulation** (Gunningham, Grabosky and Sinclair) and **meta-regulation** (Parker).

Then the thesis will discuss types of regulation along the dimension of enforcement and compliance. Enforcement includes both formal sanctioning mechanisms and informal practices aimed at securing compliance with standards or with their underlying spirit or purpose, such as

[86] Black (2002) 26.
[87] GDPR, art 33.
[88] GDPR, art 4(5); section 2.3.
[89] cf Morgan and Yeung (2007) 4.
[90] Section 3.2.1.

regulatory conversations.[91] Hawkins and Reiss employ two types of enforcement, namely those following a **'compliance' approach** or those adopting a 'sanctioning' or **'deterrence' approach**. **Responsive regulation** (Ayres and Braithwaite), and building upon that **'really responsive regulation'**, are hybrid forms. Similarly, regulatory actions can be **risk-based**. Moreover, intervention or enforcement can be **preventative, act-based** or **harm-based**, in relation to which the difference between design, output and outcome standards is discussed. Another dimension with regard to enforcement which will be explored is that regarding the actors which enforce regulation: **private and public enforcement**.

1.3.2.3 Characterising the DPIA and concluding on its functions

After describing these types of regulation, the thesis will consider as which kinds of regulation the data protection impact assessment can be characterised. Article 33 GDPR is a mix of different kinds of regulation. It shares characteristics with a variety of types of regulation. This will be analysed for the fourth sub-question. The fifth sub-question will be answered by describing and considering the strengths and weaknesses of the types of regulation with which the data protection impact assessment shares characteristics. These strengths and weaknesses will have a bearing on the potential functions which the data protection impact assessment can fulfil. Taken together, the use of these types for the analysis will shed light on the different characteristics which the types denote and the function which these characteristics can fulfil. The regulatory analysis will be used to reassess the functions which were found during the legal analysis and to identify possible new functions.

While this thesis will consider the strengths and weaknesses of the types of regulation with regard to their ability to achieve a certain regulatory outcome, the aim is not to assess the effectiveness of the data protection impact assessment. Rather, the strengths and weaknesses are analysed to see what functions the data protection impact assessment could potentially fulfil. In other words, they are used as lenses through which to analyse the impact assessment. This is not a prediction of whether and when the data protection impact assessment will in fact fulfil these functions and whether it will achieve the regulatory outcomes that it was supposed to fulfil (without damaging side-effects). Indeed, it cannot now be ascertained whether, and under what circumstances, the impact assessment will evolve to become – to use the possibilities described above - a compliance tool, an accountability tool, or an independent substantive norm of data protection law, and whether it will function as such in an effective manner. The modalities of regulation which are used and the ways in which they can and will be enforced are but two factors which may determine if a piece of regulation achieves its regulatory outcome. Other factors include the attitude of the norm-addressee and the level of trust between the regulator and the norm-addressee.[92] They are likely to differ per controller and per situation, and can in any case not be predicted on the basis of the GDPR. This thesis will rather focus on the way in which the data protection impact assessment is formulated and, given the incentive structures and institutional arrangements of the GDPR, could (rather than will) be enforced.

1.3.3 The conclusion

The sub-questions will provide an analysis of the functions which the data protection impact

[91] Morgan and Yeung (2007) 151-152.
[92] Black, Hopper and Band (2007), 194.

assessment can fulfil from the legal perspective and the perspective of regulatory studies. The conclusion on the possible contributions of the DPIA to data protection regulation will be drawn on the basis of this analysis of the functions of the DPIA. The functions will be considered in light of a general analysis of the aims of the data protection reform, as already briefly discussed in section 1.1. The functions of the DPIA will also be appreciated in light of the compliance challenges and risks posed by modern-day data processing operations. These challenges and risks are likely to increase as the data processing concerns so-called "**big data**": i.e. controllers collect or have access to large amounts of data, which is varied in nature, and are able to collect more data with great velocity.[93] The data is analysed not to test a specific hypothesis, but to find relevant relationships, correlations or models by running data mining software containing many different machine-learning algorithms, i.e. algorithms which learn to see specific patterns from ("training") data.[94] This process of inference takes the data and finds or extends models which fit. These models can then be used by deductive algorithms to infer new information.[95] Big data may be problematic with regard to compliance and risky for several rights and freedoms.[96] As a result, it poses difficult cases which the data protection impact assessment could serve to address.

1.4 Significance

As noted above, there are high hopes for the data protection impact assessment. It has been described as an important tool or even the essential core of any data protection framework. Considering the limited role of user empowerment, it is particularly interesting to ascertain whether the data protection impact assessment can add to the responsibility of controllers for their processing operations. However, there is a lack of clarity regarding the data protection impact assessment and what it can actually contribute to data protection. There is an overlap with other provisions of data protection law which also require controllers to assess the impact of their processing operations. So what does the impact assessment add? There are numerous forms and function which the impact assessment of Article 33 GDPR may come to take, which have hardly been explored in the existing literature on the data protection impact assessment.

Firstly, much of the literature concerns a preconceived notion of a privacy impact assessment, rather than the data protection assessment of Article 33. Important work on the privacy impact assessment has been done for the PIAF project and the PRESCIENT project, both of which took place around 2012. The PIAF project aims to encourage the EU and the Member States to adopt a privacy impact assessment, which is defined as a 'methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial

---

[93] A McAfee and E Brynjolfsson, 'Big Data: The Management Revolution' (2012) Harvard Business Review <https://hbr.org/2012/10/big-data-the-management-revolution/ar> accessed 15 August 2015.
[94] Information Commissioner's Office, 'Big data and data protection' (2014) <http://ico.org.uk/for_organisations/data_protection/topic_guides/big_data> accessed 26 July 2015, 8; P Cichosz, *Data Mining Algorithms Explained Using R* (Wiley 2015) xxiii.
[95] van Otterlo (2014), 260.
[96] e.g. C Kuner, F Cate, C Millard and D Svantesson, 'The challenge of "big data" for data protection' (2012) 2(2) International Data Privacy Law 47, 48; Le Métayer and Le Clainche (2012) 319-320; E Kerr and J Earle, 'Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy' (2013) 66 Stanford Law Review Online 65, 67-71; P Leonard, 'Costumer data analytics: privacy settings for 'Big Data' business' (2014) 4(1) International Data Privacy Law 53, 57; Moerel (2014) 53-54; van Otterlo (2014) 257 and 269-270; N Richards and J King, 'Three Paradoxes of Big Data' (2013) 66 Stanford Law Review Online 41, 44.

actions as necessary in order to avoid or minimise negative impacts'.[97] It resulted in a review of the Privacy Impact Assessment in the six countries which have adopted it, of which the UK is the only EU Member State, a survey of data protection authorities and EU policy makers, and recommendations for policy-makers and data controllers who respectively developing and carry out a privacy impact assessment.[98] The PRESCIENT project is broader in scope. It aims to identify and assess privacy issues posed by emerging sciences and technologies and to contribute to the development of new instruments for the governance of science and technology. To this end, it created a common framework for a privacy, data protection and ethical impact assessment.[99] The project therefore has a firm tie with the literature on Responsible Research and Innovation. The project reports regard the conceptualisation of privacy and data protection, case studies on privacy issues, the knowledge and attitude of citizens regarding the storage of personal data, the analysis of existing privacy & ethical impact assessment frameworks and the creation of such a framework.[100]

These projects provide valuable contributions to those concerned with the adoption and implementation of impact assessments for privacy and ethics. They may have inspired or influenced Article 33 of the GDPR, the first version of which was put forward by the Commission in 2012. However, they both employ a predefined notion of the impact assessment which does not align with any of the versions of Article 33 of the GDPR. As such, they are not about the data protection impact assessment of Article 33. PRESCIENT only contains an analysis of one-and-a-half page of the Commission version of the DPIA;[101] PIAF does not analyse the DPIA at all; Article 33 is hardly mentioned.[102] Also the book 'Privacy Impact Assessment', edited by PIAF and PRESCIENT contributors De Hert and Wright in 2012, does not focus on the data protection impact assessment which Article 33 will come to mandate.[103] Moreover, none of these sources could have reflected the Parliament and the Council versions of DPIA, as these appeared at a later point in time. This is not to say that the notions of the privacy impact assessment which are employed in these projects and scholarly works do not overlap or coincide with the data protection impact assessment of Article 33. It has been asked, for example, if the DPIA also entails an assessment of the compatibility with the right to privacy and perhaps the whole spectrum of human rights.[104] This body of literature can be helpful in identifying the different potential forms and functions of the data protection impact assessment, but they are not principally about this legal figure. As a result, there is a gap in the literature on the data protection impact assessment of the different versions of Article 33.

Secondly, although authors have been sensitive to the fact that the contributions of the data protection impact assessment may lie in the way in which it regulates, the possible functions of the impact assessment have not been explored through a systematic analysis on the basis of the different types of regulation which it may constitute. By explicitly bringing in the

---

[97] PIAF, 'A Privacy Impact Assessment Framework for data protection and privacy rights: Deliverable D1' (2011), 14.
[98] PIAF, 'Deliverables' <http://www.piafproject.eu> accessed 15 August 2015.
[99] PRESCIENT, 'Deliverable 4: Final Report – A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies' (2013); S Gutwirth and M Friedewald, 'Emergent technologies and the transformations of privacy and data protection' (2013) 29 Computer Law & Security Review 477; PRESCIENT, 'About PRESCIENT' <http://www.prescient-project.eu> accessed 15 August 2015.
[100] PRESCIENT, 'Description of Work' <http://www.prescient-project.eu/prescient/inhalte/documents/deliverables.php> accessed 15 August 2015.
[101] PRESCIENT (2013) 50-51.
[102] PIAF (2012).
[103] D Wright and P De Hert, *Privacy Impact Assessment* (Springer 2012).
[104] Gellert and Gutwirth (2013), 529. cf De Hert (2012).

interdisciplinary perspective of regulatory studies, this thesis aims to complement the legal perspective so as to provide a fuller, but scientifically substantiated, analysis of the functions of the DPIA.

In short, this thesis aims to fill the gaps by analysing the impact assessment of Article 33, as it is contained in the different versions of the GDPR, both from a legal and regulatory perspective. The arrival of the final GDPR will, to some extent, render this research outdated. However, knowledge of the previous versions of the GDPR can still be useful in interpreting the final product.

1.5 Methodology

In order to analyse what the data protection impact assessment may contribute to data protection regulation, this thesis will analyse what the DPIA can entail and what functions it can fulfil. The main methods employed in this thesis are doctrinal legal research and literature reviews.

The analysis of the various forms which the data protection impact assessment may take is primarily based on a legal analysis of the different versions of the GDPR, particularly its Article 33. The requirement that the "risks" for "the (the right to) the protection of personal data" are assessed, also requires an analysis of these terms. Consulted sources include the Charter of Fundamental Rights, the GDPR, case law of the European Court of Justice, guidance of the Article 29 Working Party and of national Data Protection Authorities, and doctrine and other literature. Relevant bodies of literature are those on the privacy impact assessment, on the right to the protection of personal data and the conceptualisation of data protection, and on risk management and precaution. European scholarship on the privacy / data protection impact assessment has been synthesised in a literature review by the author for a previous research project, which will be put to use. The work of Wright and De Hert is leading in the field of the privacy impact assessment. Particularly relevant for the conceptualisation of privacy and data protection is the work of Gutwirth and De Hert, which has also been discussed by González Fuster and Borgesisus. The literature on privacy or data protection impact assessments will also be used to conclude from the legal analysis which possible functions DPIA might fulfil.

This legal analysis of the functions of the data protection impact assessment will be supplemented by an analysis of the ways in which it can regulate behaviour. A literature review of different types of regulation and their strengths and weaknesses will be conducted and used as a lens through which to analyse the DPIA. Through this method, this thesis incorporates another field of research and gains a tinge of multi-disciplinarily. The literature review will employ the categorisations employed in the handbooks of Morgan & Yeung and Baldwin, Cave & Lodge and draw from the references presented in these works. The subsequent assessment of the DPIA will build on the legal analysis of the DPIA and on the institutional arrangements within which enforcement takes place, as described in the GDPR.

To conclude on the possible contributions of the data protection impact assessment, the functions of the DPIA will be presented in light of the aims of the data protection reform, which are researched on the basis of travaux préparatoires, particularly the Commission's communication and impact assessment. The context of big data will also be taken into account.

The compliance issues and risks presented by big data have already been analysed by the author in a literature review.

1.6 Roadmap

The next chapter will lay out the different versions of the data protection impact assessment as contained in the GDPR. The DPIA is analysed in parts: the risk threshold, the norm addressees, the subject-matter, the outcome requirements and the possible consequences of the DPIA. The process through which the impacts are assessed is not prescribed by the GDPR, but several guidance documents exist and will shortly be reported. This chapter will conclude on the potential functions of the DPIA in light of the legal analysis. The following chapter will analyse the different types of regulation which are mixed in the DPIA. It will describe the types of regulation and analyse how the DPIA can be characterised. Then it will describe the strengths and weaknesses of the types of regulation with which the DPIA shares characteristics and conclude on the potential functions of the DPIA. The conclusion will summarize the functions of the DPIA and answer the main question: what can the data protection impact assessment potentially contribute to data protection regulation?

Sources

Van Aeken K, 'Regulation & governance-onderzoek in het rechtenonderwijs in Nederland: Sranger in a strange land?' 2015(2) RegelMaat 95

Van Alsenoy B, Kosta E and Dumortier J, 'Privacy notices versus informational self-determination: Minding the gap' (2014)28 International Review of Law, Computers & Technology 185

Article 29 Working Party, 'Opinion 03/2013 on purpose limitation'

——, 'Opinion 15/2011 on the definition of consent'

——, 'Opinion 26/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC'

Balboni P, Cooper D, Imperiali R and Macenaite M, 'Legitimate interest of the data controller. New data protection paradigm: legitimacy grounded on appropriate protection' (2013) 3(4) International Data Privacy Law 244

Baldwin R, Scott C and Hood C, *A Reader on Regulation* (Oxford University Press 1998)

Baldwin R, Hood C and Rothstein H, *The Government of Risk* (Oxford University Press 2001)

Baldwin R; Cave M and Lodge M, *Understanding Regulation: Theory, Strategy and Practice* (Oxford University Press 2012)

Black J, 'Decentring regulation: Understanding the role of regulation and self-regulation in a "post-regulatory" world' (2001) 54(1) Current Legal Problems 103

——, 'Critical Reflections on Regulation' (2002) 27 Australian Journal of Legal Philosopy

——, 'What is Regulatory Innovation' in Black J, Lodge M and Thatcher M (eds), *Regulatory Innovation* (Cheltenham 2005)

Black J, Hopper M and Band C, 'Making a success of Principles-based regulation' (2007) 1(3) Law and Financial Markets Review 191

Borgesius F, 'Improving privacy protection in the area of behavioural targeting' (PhD thesis, University of Amsterdam 2014)

Brownsword R and Goodwin M, *Law and the Technologies of the Twenty-First Century* (Cambridge University Press 2012)

Cichosz P, *Data Mining Algorithms Explained Using R* (Wiley 2015)

Clarke R, 'Privacy impact assessment: Its origins and development' (2009) 25(2) Computer Law & Security Review 123

Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union' COM(2010) 609 final

——, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final

De Hert P, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments', in Wright D and De Hert P (eds), Privacy Impact Assessment (Springer 2012)

Finn R, Rodrigues R and Wright D, 'A Compararive Analysis of Privacy Impact Assessment in Six Countries', (2013) 9(1) Journal of Contemporary European Research 160

Gellert R and Gutwirth S, 'The legal construction of privacy and data protection' (2013) 29(5) Computer Law & Security Review 522

Gellert R, 'Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative' (2015) 5(1) International Data Privacy Law 3

González Fuster G and Gutwirth S, 'Opening up personal data protection: a conceptual controversy' (2013) 29(5) Computer Law & Security Review 531

González Fuster G, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014)

Griffiths J, 'De sociale werking van het recht' in Griffiths J (ed), *De sociale werking van het recht. Een kennismaking met de rechtssociologie en rechtsantropologie* (Ars Aequi Libri 1996)

——, 'The Social Working of Legal Rules' (2003) 48(1) Journal of Legal Pluralism & Unofficial Law 1

Gutwirth S and Friedewald M, 'Emergent technologies and the transformations of privacy and data protection' (2013) 29 Computer Law & Security Review 477

Hancher L and Moran M, 'Organizing regulatory space' in Baldwin R, Scott C and Hood C, *A Reader on Regulation* (Oxford University Press 1989)

Hildebrandt M, 'Who is Profiling Who? Invisible Visibility' in Gutwirth S, Poullet Y, De Hert P, De Terwangne C and Nouwt S (eds), *Reinventing Data Protection?* (Springer 2009)

Information Commissioner's Office, 'Conducting privacy impact assessments: code of practice' (2014) <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/> accessed 15 August 2015

——, 'The Guide to Data Protection' (version 2.2.4, 31 March 2015) <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/> accessed 25 July 2015, 16.

——, 'Big data and data protection' (2014) <http://ico.org.uk/for_organisations/data_protection/topic_guides/big_data> accessed 26 July 2015

International Working Group on Data Protection in Telecommunications, 'Working Paper on Big Data and Privacy' (55th Meeting, 2014)

Kerr E and Earle J, 'Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy' (2013) 66 Stanford Law Review Online 65

Kightlinger M, 'Twilight of the idols? EU internet privacy and the post enlightenment paradigm' (2007-2008) 14(1) Columbia Journal of European Law 62

Koop C and Lodge M, 'What is regulation? An interdisciplinary concept analysis' (2015) Regulation & Governance

Koops B, 'The trouble with European data protection law' (2014) International Data Privacy Law

Kuner C, F Cate, C Millard and D Svantesson, 'The challenge of "big data" for data protection' (2012) 2(2) International Data Privacy Law 47

Leenes R, 'Reply by Ronald Leenes (TILT): Addressing the obscurity of data clouds' (2009) TILT Law & Technology Working Paper No. 012/2009 17 April 2009, Version: 1.0 & Tilburg University Legal Studies Working Paper No. 008/2009, < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1393193> accessed 30 July 2015

Leonard P, 'Costumer data analytics: privacy settings for 'Big Data' business' (2014) 4(1) International Data Privacy Law 53

Lessig L, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harvard Law Review 501

McAfee A and Brynjolfsson E, 'Big Data: The Management Revolution' (2012) Harvard Business Review <https://hbr.org/2012/10/big-data-the-management-revolution/ar> accessed 15 August 2015

Le Métayer D and Le Clainche J, 'From the Protection of Data to the Protection of Individuals: Extending the Application of Non-discrimination Principles' in Gutwirth S, Leenes R, De Hert P and Poullet S (eds), *European Data Protection: In Good Health?* (Springer 2012)

Moerel L, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof' (inaugural lecture, Tilburg University 2014)

Morgan B and K Yeung, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press 2007)

Murray A, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge Cavendish 2007)

Murray A and Scott C, 'Controlling the New Media: Hybrid Responses to New Forms of Power' (2002)65 Modern Law Review 491

Oetzel M and Spiekermann S, 'A systematic methodology for privacy impact assessments: a design science approach'(2014) 23 European Journal of Information Systems 126

van Otterlo M, 'Automated Experimentation in Walden 3.0.: The Next Step in Profiling, Predicting, Control and Surveillance (2014)12(2) Surveillance and Society 255

Oude Vrielink M, 'Wanneer is zelfregulering een effectieve aanvulling op overheidsregulering?' in Hertogh M and Weyers H (eds), *Recht van onderop: Antwoorden uit de rechtssociologie* (Ars Aequi Libri 2011)

Parker C, 'Reinventing regulation within the corporation: Compliance-oriented regulatory innovation' (2000) 32(5) Administration & Society 529

PIAF, 'A Privacy Impact Assessment Framework for data protection and privacy rights: Deliverable D1' (2011)

——, 'Deliverable D3: Recommendations for a Privacy Impact Assessment Framework for the European Union' (2012)

PRESCIENT, 'Deliverable 4: Final Report – A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies' (2013)

Richards N and King J, 'Three Paradoxes of Big Data' (2013) 66 Stanford Law Review Online 41

Scott C, 'Regulation in the age of governance: The rise of the post-regulatory state' in Jordana J and Levi-Faur D, *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance* (Edward Elgar Publishing 2004)

Solove D, 'Introduction Privacy self-management and the consent dilemma' (2013) 126 Harvard

Law Review 1880

Schwitters R, *Recht en samenleving in verandering: een inleiding in de rechtssociologie* (Kluwer 2008)

Tranberg C, 'Proportionality and data protection in the case law of the European Court of Justice' (2011) 1(4) International Data Privacy Law 239

Twining W, 'A Post-Westphalian Conception of Law' (2003) 37(1) Law & Society Review 199

Wadhwa K and Rodrigues R, 'Evaluating privacy impact assessments' (2013) 26 Innovation: The European Journal of Social Science Research 161

Weber R, 'Symposium on EU Data Protection Reform: Privacy management practices in the proposed EU regulation' (2014) 4(4) International Data Privacy Law 290

Wright D and De Hert P, *Privacy Impact Assessment* (Springer 2012)

Wright D, Friedewald M, Gutwirth S and others, 'Sorting out smart surveillance' (2010) 26(4) Computer Law & Security Review 343

Zarsky T, 'Transparent Predictions' (2013)4 University of Illinois Law Review 1503

2 The legal analysis of the GDPR's data protection impact assessment

2.1 Introduction

This chapter will discuss the different forms of the data protection impact assessment (DPIA) as contained in the different versions of the General Data Protection Regulation (GDPR) and conclude on its functions in light of this legal analysis. The DPIA is analysed through its possible components: 1) when is the obligation triggered, 2) to whom does it apply, 3) what needs to be assessed, 4) what output is required, and 5) what consequences are attached to the results. Lastly, a number of guidance documents regarding the DPIA process will be discussed. The larger sections contain a conclusion which summarizes the findings. They also contain a table which compares the Commission, Parliament and Council versions of the GDPR. The final conclusion will draw from the legal analysis of this chapter to conclude on the possible functions of the data protection impact assessment in light of the hypothesis presented in the introduction: that the DPIA can help controllers establish compliance and supervisory authorities to enforce the GDPR, and that it might even introduce a requirement to mitigate "risky" processing operations.[105] It will also consider whether the DPIA can fulfil a function in light of the second objective of data protection law: to protect the free movement of information. Lastly, the tables presented at the end of each section will be presented together in section 2.9.

2.2 The risk threshold

All three versions of the GDPR only require the data protection impact assessment to be conducted if the intended or envisaged processing operations are likely to[106] present *specific risks*[107] or *high risks*[108] to the *rights and freedoms of data subjects*[109]*/individuals*[110]. The Parliament version even contains a separate provision, Article 32a, to cover this risk analysis, which also serves to signal whether a EU representative or a data protection officer needs to be appointed.[111] This section discusses when a risk analysis needs to be carried out, whether a DPIA must always be carried out if specific/high risks are found, whether the risks must be known, and what counts as "risky", including a discussion of the lists of risky situations included in the GDPR. To analyse what it means for a "risk" to be "known", the concepts of risk and precaution are introduced.

2.2.1 When does a risk analysis need to be carried out?

According to the literature on privacy impact assessments, the impact assessment is an ongoing process which should be held at the start of a project, so that there is still time to adjust the outcome.[112] The DPIA helps controllers get it right from the start.[113] The initial risk analysis would logically need to be conducted for each processing operation or for each type of

---

[105] Section 1.2.
[106] General Data Protection Regulation (GDPR) Parliament version, art 32a(1); GDPR Council version, art 33(1).
[107] GDPR Commission version, art 33(1); GDPR Parliament version, art 32a(1).
[108] GDPR Council version, art 33(1).
[109] GDPR Commission version, art 33(1); GDPR Parliament version, arts 32a(1) and 32(3)(c).
[110] GDPR Council version, art 33(1).
[111] GDPR Parliament version, art 32(a)(3).
[112] D Wright, 'The state of the art in privacy impact assessment' (2012) 28(1) Computer Law & Security Review 54, 55; D Wright and P De Hert, 'Introduction to Privacy Impact Assessment' in D Wright and P De Hert (eds), *Privacy Impact Assessment* (Springer 2012) 5-6.
[113] Article 29 Working Party, 'Opinion 01/2012 on the data protection reform proposals' (WP191, 2012) 4.

processing before the operation is started. This does not seem to be limited in any way. It may even be an ongoing obligation. The Parliament explicitly requires the processing operations to be reviewed on a yearly basis or if the nature, scope or purposes of the data processing operations change significantly.[114] The Council mentions that the lapse of time can necessitate that a DPIA is carried out again,[115] indicating that an eye must be kept on any new risks which may arise throughout the lifecycle of the data processing operation. However, like the Commission, the Council does not specify under what circumstances a new risk analysis must be carried out – e.g. after one year has lapsed or if changes are made to an already assessed processing operation.[116]

2.2.2. Exceptions to the risk threshold

If the risk analysis points to specific/high risks, then a DPIA needs to be carried out. The DPIA might not be required for each processing operation which meets the risk threshold. The Commission emphasised that the DPIA should particularly be required for newly established large scale filing systems, and that multiple projects can sometimes be assessed together, mentioning processing applications or platforms which are shared by multiple controllers.[117] The Parliament instead holds that a single DPIA is enough to address 'a set of similar processing operations that present similar risks'.[118] The Council version also accepts that multiple projects are assessed together,[119] and requires the DPIA only 'where a type of processing, in particular using new technologies, (...) is likely to result in a high risk'.[120] This is further explained in Recital 70: 'such types of processing operations may be those which, in particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing'. Therefore, the DPIA may not be required for processing operations which are not in any way new, unless the lapse of time somehow gives rise to reasons which necessitate an impact analysis. Clearly the focus is on new types of projects. They may present risks which have not been analysed before, and perhaps they are deemed to carry the scariest risks, as old risks become accepted. However, a DPIA for old projects is not excluded; it would logically be required if a threshold analysis points out that new risks arise.

In the Commission and Council version, an exception to the risk threshold is the situation in which the processing has a legal basis in EU law or the law of the Member State to which the controller is subject. If the legal ground is that the processing is necessary to be compliant with a legal obligation or if it is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the controller,[121] and this law regulates the processing in question, then a data protection impact assessment only needs to be carried out if the Member State deems it necessary.[122] The remaining question would be when the law sufficiently regulates the processing. If an unforeseen impact risk arises, should it be analysed? Recital 73

[114] GDPR Parliament version, art 32a(4).
[115] GDPR Council version, rec 70.
[116] cf P De Hert and V Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28(2) Computer Law & Security 130, 141.
[117] GDPR Commission version, recs 71 and 72.
[118] GDPR Parliament version, art 33(1).
[119] GDPR Council version, rec 72.
[120] GDPR Council version, art 33(1).
[121] GDPR, arts 6(1)(c) and (e).
[122] GDPR Commission and Council version, art 33(5).

clarifies that this exception aims to avoid overlap with the regulatory impact assessment: public bodies should (Commission) or may (Council) carry out a data protection impact assessment for their processing of personal data if such an assessment was not yet made in the context of the adoption of the legal basis. Perhaps, if a new risk was not yet considered during the RIA it should be subjected to a DPIA. This exception is not present in the Parliament version.

2.2.3 The "risk" must be "known"

This section discusses what the technical meaning of "risk" is, whether the GDPR adheres to this meaning, and what the implications are of such an interpretation. Under a technical interpretation, the data protection impact assessment is only mandated if the processing operation presents risks or is likely to do so, as a result of which situations in which the risks are not clear are excluded. The Article 29 Working Party objects to this limited application of the DPIA.[123] It thereby appears to advocate a precautionary application of the data protection impact assessment. A traditional, non-precautionary risk assessment can only be performed if the **"risks"** (technically defined as **threat x probability**) are known. In the words of PRESCIENT, '[t]he concept of risk, when considered scientifically, takes the form of the calculation of a probability that something bad happens'.[124] According to a communication of the Commission on the precautionary principle, a risk assessment entails that the potential "**threats" (adverse effects)** of a phenomenon are identified and assessed or evaluated in terms of probability and severity. If the threat is known, but the probability is not, the risks cannot be assessed. In that case, the precautionary principle can apply. This principle would allow or even mandate the norm addressee to act in a certain way in the situation in which there are indications of possible adverse effects, but the probability of these risks cannot be determined with sufficient certainty (i.e. there is "**scientific uncertainty"**). In these cases, a risk assessment cannot be comprehensive because the probability of the potential threats cannot be evaluated. The precautionary principle would then supplement the risk assessment by covering exactly those situations in which 'scientific uncertainty precludes a full assessment of the risk'.[125] In turn, the precautionary principle can only apply if the threat is known. In situations of ignorance, possible threats are not foreseen and therefore cannot be assessed at all.[126]

The risk terminology does not explain when something is considered "known" or "uncertain". This has been called the knowledge condition.[127] It refers to a point on a continuum with certainty on one end, and uncertainty on the other. Risks of which the probability can be statistically calculated are certain, but risks can also be "known" if no statistical calculations are available.[128] According to von Schomberg, scientific uncertainty exists if "complete" scientific evidence is not available, there is ongoing scientific controversy, and/or there are disagreements

---

[123] Article 29 Working Party, 'Opinion 01/2012 on the data protection reform proposals', 16.
[124] PRESCIENT, 'Deliverable 4: Final Report – A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies' (2013) 68.
[125] Commission, Communication from the Commission on the precautionary principle, COM (2000) I, para 5 and 7. cf C Tannert, H Elvers and B Jandrig, 'The ethics of uncertainty. In light of possible dangers, research becomes a moral duty' (2007) 8(10) EMBO reports <ttp://www.ncbi.nlm.nih.gov/pmc/ arts/PMC2002561/> accessed on 15 July 2015.
[126] B Wynne, P Harremoës, D Gee and others, *The Precautionary Principle in the 20th Century: Late Lessons from Early Warnings* (Earthscan 2002) 217. cf P Sandin, 'Better Safe than Sorry: Applying Philosophical Methods to the Debate on Risk and the Precautionary Principle' (2004) Theses in Philosophy from the Royal Institute of Technology 5, 11 and 15.
[127] N Manson, 'Formulating the Precautionary Principle' (2002) 24 Environmental Ethics 263, 265. cf Sandin (2004) 13-14.
[128] P O'Malley, *Risk, Uncertainty and Government* (Glasshouse Press 2004) 19.

about the lack of (scientific) knowledge. The borders between certainty, uncertainty and conjecture are then drawn on the basis of the extent of scientific disagreement.[129] Alternatively, agreement amongst citizens can also be an indicator that a threat is sufficiently "known". Under this rationale, the decision whether a threat is "known" is linked not to scientific rationality but to collective deliberation.[130] This ties in to the fact that experts and laypeople frequently interpret risks differently.[131] The more agreement is required for a risk to be known, the higher the threshold is. Under the above understanding of risk, there has to be a certain level of scientific or civic agreement on the threat which is posed and the probability with which it would occur for a DPIA to be required. As a result, a precautionary approach is excluded: the threat and the probability must be "known" for there to be a risk. The lower the knowledge condition is, the more precautionary the risk assessment becomes.

If the GDPR follows the above terminology, Article 33 does not cover situations in which one can imagine a threat but does not "know" how likely it is to become true. While the Parliament and the Commission version do not contain clear indications on the meaning of "risk" for the purposes of the GDPR,[132] the Council version repeatedly refers to the likelihood and severity of the risk[133] and states that risks should be evaluated 'in terms of their origin, nature, likelihood and severity'.[134] This indicates that, according to the Council version, "risk" indeed means a threat of a certain severity (and origin and nature) and of a certain probability. This terminology is also adopted in the CNIL's PIA Guideline.[135] As a result, a pure precautionary approach is excluded because the threat and its probability must be "known" for there to be a risk. The requirement of the Commission and the Parliament that the risk be specific may have the same bearing, but it may also merely denote that the threat must be known. However, the difference between "threat" and "risk" is only really noticeable if the knowledge condition is strict; i.e. if there must be a high degree of certainty regarding the likelihood of the risk, statistical or otherwise.

2.2.4 What counts as risky?

When assessing risk, it must be decided what counts as a severe and likely enough threat. What types of adverse effects are covered and what characteristics must they have to qualify as severe enough? This has been called the damage condition.[136] For the DPIA, any specific/high risk to a right or freedom appears to be covered. The Council gives examples of risks: 'discrimination, identity theft or fraud, financial loss, damage to the reputation, unauthorized reversal of

---

[129] R von Schomberg, 'The precautionary principle and its normative challenges' in E Fisher, J Jones and R von Schomberg (eds), *Implementing the Precautionary Principle: Perspectives and Prospects* (Edward Elgar 2006) 39-41.
[130] cf D Wright, R Gellert, S Gutwirth and M Friedewald, 'Precaution and privacy impact assessment as modes towards risk governance' in R von Schomberg (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Field* (European Commission 2011), 88.
[131] P Slovic, 'Perception of Risk Posed by Extreme Events' (New York conference, 2002) Risk management strategies in an uncertain world <https://www.ldeo.columbia.edu/chrr/documents/meetings/roundtable/white_papers/slovic_wp.pdf> accessed 11 September 2015.
[132] **Only recital 71a of the Parliament version refers to the likelihood of risks, stating that a thorough impact assessments can limit the likelihood of data breaches or privacy-intrusive operations. However, this does not imply that such an assessment should only occur if the likelihood is known.**
[133] GDPR Council version, recs 60a, 60b and 60 and arts 22(1), 23 (1) and 30(1).
[134] GDPR Council version, rec 60c.
[135] Commission nationale de l'informatique et des libertés (CNIL), 'Privacy Impact Assessment (PIA): Methodology (how to carry out a PIA)' (2015) 6.
[136] Manson (2002) 265. cf Sandin (2004) 13-14.

pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage'.[137] The Article 29 Working Party clarifies in relation to the risk-based approach that 'the scope of "the rights and freedoms" of the data subjects primarily concerns the right to privacy but may also involve 'other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion'.[138] Moreover, according to the Working Party not only risks to individuals are relevant, as adverse effects are to be 'assessed on a very wide scale ranging from an impact on the person concerned by the processing in question to a general societal impact (e.g. loss of social trust)'.[139] It is difficult to imagine a data processing operation which cannot be considered, with some probability, to adversely affect (= threaten) the rights and freedoms of individuals, or even society in general. If the right to the protection of personal data is prohibitive, as argued below, any processing of personal data would constitute an interference, although the interference may be justified. Similarly, the data processing will already interfere with the right to privacy if private data is processed.[140] Technically, there is thus already a risk to the rights and freedoms of individuals if there is a known probability that the data which is processed is of a private nature, because that would adversely affect the right to privacy. To give another example: there is already a risk to the right to non-discrimination if the data might be used to make some kind of decision which affects people and if the data may contain information relating to the protected categories of 'sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation'.[141] The threat is that individuals are treated differently on the basis of one of these protected characteristics.

One may wonder whether the European legislature intends the DPIA to encompass such a broad range of issues. The legislator probably means the DPIA to address both data security and a number of other rights concerns which have received a lot of attention lately, most notably discrimination. However, the examples given by the Council and the Article 29 Working Party exclude a less extensive "security-based" interpretation: data leaks cannot harm freedom of thought or discriminate. Moreover, if the legislator had meant the DPIA to only concern particular rights and freedoms, it should have made a distinction. Instead, it opted for a wide DPIA which can be focussed on particular issues; pressing matters can be included on the list of highly risky processing operations or emphasised in later policy guidance or during regulatory conversations. Another way in which the DPIA could have been (but is not) narrower, is by encompassing only so-called management and control risks. In the literature on risk-based regulation, a distinction is made between 'inherent' risks, which arise from the nature of the processing activity - e.g. privacy is harmed if private information is collected, autonomy is impinged if the data is used for personalisation - and 'management and control risks', which concerns the internal control systems which may mitigate or, conversely, exacerbate the inherent risks – e.g. a lack of adequate data security or no controls against discriminatory data

[137] GDPR Council version, art 33(1).
[138] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' (WP218, 2014) 4.
[139] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', 4.
[140] *Amann v Switzerland* (2000) 30 EHRR 843, para 65; *Rotaru v Romania* (2000) IHRL 2923, para 43; *P.G. and J.H. v the United Kingdom* App no 44787/98 (ECtHR 4 September 2001), para 57; R Gellert and S Gutwirth, 'The legal construction of privacy and data protection' (2013) 29(5) Computer Law & Security Review 522, 526.
[141] Charter of Fundamental Rights of the European Union (Charter), art 21.

analysis.[142] CNIL's impact assessment is limited to management and control risks to data security: it sees only to the risks which result from unlawful access, alteration or removal of personal data.[143] The DPIA, however, is not. The fact that discrimination is given as an example of a risk in the sense of Article 33 GDPR shows that, contrary to CNIL's security-based conception of risk assessment, also the way in which data is used falls within the scope of the DPIA. This is because discrimination concerns typically arise if sensitive categories of information are used in a way which affects people. The same goes for the human rights enumerated by the Article 29 Working Party. As a result, anything related to the processing may cause risks in the sense of the DPIA, including not only the way in which information is collected and stored, but also the way in which information is used.

The threshold can be tightened by requiring a higher level of knowledge with regard to the probability or severity of the threat (knowledge condition) or by requiring the threat to be of greater probability or severity (damage condition). The Council requirement that the risk is "high" appears to indicate that the threat must be of a severe and likely nature for the threshold to be met.[144] However, as the high risk has also been referred to as 'a particular risk of prejudice to the rights and freedoms of individuals',[145] it is unclear what the adjective "high" adds. Perhaps a possible interference with a right or freedom is not enough; perhaps the interference should be serious enough be considered disproportionate, constituting a violation. However, according to Recital 71, a processing operation is already particularly risky if it renders it more difficult for data subjects to exercise their rights. As a result, a processing operation is already highly risky if individuals are limited in the control which they have over the data relating to them, as granted by data subject rights. It would be incongruous to require the threat to be so severe so as to require a violation of a right, rather than an interference. Moreover, Recital 74, which regards consultation of the supervisory authority if the DPIA points to high risks, mentions that high risk processing may result in damage or an *interference* with rights and freedoms of individuals.[146] With regard to the probability, the Parliament and the Council specify that the risks must be 'likely'.[147] A real possibility that the processing may fall within the scope of a right or freedom appears to be eligible to constitute a specific or high risk.

The Commission and the Council version elaborate on how to assess if such risks are present, specifying that processing operations may pose such risks by virtue of their nature, their scope or their purposes or taking into account the nature, scope, purposes and the context of the processing.[148] Similarly, according to the Article 29 Working Party risks 'should be determined taking into consideration specific objective criteria', such as 'the nature of personal data (e.g. sensitive or not), the category of data subject (e.g. minor or not), the number of data subjects affected, and the purpose of the processing'.[149] Recitals 60b and 60c of the Council version imply that these risks should be evaluated through an objective assessment 'in terms of their origin, nature, likelihood and severity'.[150] The likelihood partly depends, as the CNIL points out, on the

[142] J Black and R Baldwin, 'Really Responsive Risk-Based Regulation' (2010) 32(2) Law & Policy 181, 184; R Baldwin; M Cave and M Lodge, *Understanding Regulation: Theory, Strategy and Practice* (Oxford University Press 2012) 282.
[143] See differently CNIL (2015) 14.
[144] GDPR Council version, rec 60c.
[145] GDPR Council version, rec 60b.
[146] GDPR Council version, rec 74.
[147] GDPR Parliament version, art 32a(1); GDPR Council version, art 33(1).
[148] GDPR Commission and Council version, art 33(1).
[149] Article 29 Working Party 'Statement on the role of a risk-based approach in data protection legal frameworks', 4.
[150] GDPR Council version, rec 60c.

level of vulnerabilities of the file management system and the capabilities of risk sources to use them.[151] This may refer, for example, to the capacity of cybercriminals to hack into the system or of a bribed employee to access the data. These criteria indicate that not every possible interference with a right or a freedom is sufficiently severe or likely to count as a threat. They must be of a particular severity or likelihood, or a particular nature or scope, or arise from a purpose which has little benefit to society. However, these criteria do not by themselves indicate when a threat is risky enough; they merely indicate which factors play a role on this assessment.

All three versions contain a list of processing operations which are considered to meet the threshold. The Parliament version contains an extensive list in Article 32a(2), and the DPIA is only required as a follow-up on the risk analysis in the cases described there.[152] However, in the Commission and the Council version the list should not be interpreted as exhaustive. A Note from the Presidency of the Council states otherwise,[153] indicating that cases which are not on the list cannot trigger the obligation to conduct a DPIA, irrespective of the level of risk which they present. The phrasing, employed by both the Commission and the Council, is ambiguous: the list contains cases for which the DPIA shall 'in particular' be required or which 'in particular' present specific risks.[154] However, it seems illogical to first present a general test (if specific/high risks to the rights and freedoms of data subjects are likely/present) and then to present a number of cases, if the cases render the general test superfluous. Moreover, Recital 71 of Council version, mentions both the general category of high risk processing operations and the three situations included in the list. The Council also requires the supervisory authority to draw up 'a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1'.[155] This again indicates that the list in the GDPR is not exhaustive. Furthermore, according to the Article 29 Working Party, the lists relate to cases which are risky 'by essence',[156] indicating that other cases may also be risky, given the circumstances of the case. While the Parliament list should still be regarded as exhaustive, the Commission's and the Council's should not. However, as discussed below, the Parliament version contains such broad cases that the difference is negligible.

The three lists all include, in differing formulations, the large scale monitoring of publicly accessible areas and significant or large scale decisions which are based on profiling or on certain categories of sensitive data.[157] The Commission and the Parliament versions also include large scale decisions on the provision of health care, epidemiological researches, or surveys of mental or infectious diseases and large scale filing systems with data on children, genetic data or biometric data.[158] The Parliament version further contains a number of quite broad cases: if the personal data of more than 5000 data subjects is processed for at least a year, if the core activity of the controller or the processor is one which requires the regular and systematic monitoring of data subjects, and situations 'where a personal data breach would likely adversely affect the

[151] CNIL (2015) 6.
[152] GDPR Parliament version, arts 33(1) and 32a(3)(3).
[153] The Council of the European Union, 'Presidency Note: Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Data Protection Impact and Prior Checks' (5880/14 2012/0011(COD), 2014) 2.
[154] GDPR Commission and Council version, art 33(2).
[155] GDPR Council version, art 33(2a). See also GDPR Council version, rec 60c.
[156] Article 29 Working Party, 'Statement on the role of a risk based approach in data protection legal frameworks', 4.
[157] GDPR Commission and Council version, art 33(2); GDPR Parliament version, arts 32a(b), (c) and (e).
[158] GDPR Commission version, arts 33(b) and (d); GDPR Parliament version, arts 32a(b) and (d).

protection of the personal data, the privacy, the rights or the legitimate interests of the data subject'.[159]

The Commission, Parliament and Council version all delegate to the supervisory authority or the European Data Protection Board the power to make a list of risky cases. In the Commission and the Parliament versions, this power is found in the reference to processing operations for which prior consultation is required by Article 34(2)(b).[160] This provision requires a prior consultation with the supervisory authority (or, alternatively, the data protection officer in the Parliament version) in the case in which the authority deems this necessary for processing operations 'that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes'. These risky processing operations are to be specified in a public list drawn up by the supervisory authority (in the Commission version) or the European Data Protection Board (in the Parliament version).[161] Therefore, these authorities would be free to decide which other cases require a prior consultation and, thereby, also a data protection impact assessment. As stated above, the Council requires the supervisory authority to establish and make public a list on the processing operations for which a data protection impact assessment needs to be carried out. The supervisory authority may also make a list of cases in which no DPIA is required.[162] The Commission version further empowers the Commission to adopt delegated acts to specify the criteria and conditions for processing operations likely to present specific risks – a provision which both the Parliament and the Council have deleted.[163]

2.2.5 Conclusion

In sum, the risk analysis has to be carried out for each processing operation or type of processing before the operation is started. It would logically also be an ongoing obligation to regularly reassess the risks – although the Commission does not expressly point this direction. Only the Parliament clarifies under what conditions a risk analysis has to be carried out: at the start of a project and again after one year or if the nature, scope or purposes of the processing change significantly. The Council merely refers to the lapse of time.

Generally, if the risk analysis points to specific or high risks, a data protection impact needs to be carried out for the processing activity. However, sometimes different projects can be grouped together in one DPIA. New kinds of projects should be more readily subjected to a DPIA, but old projects can still turn out to be risky, which would necessitate a(nother) impact assessment. Moreover, in the Commission and Council versions, a DPIA does not need to be carried out for processing which is based on a legal obligation or necessary to perform a public task, unless the Member State decides otherwise. This avoids collision with the regulatory impact assessment.

A DPIA has to be carried out if the risk analysis points to specific/high risks, whereby the Parliament describes which categories of processing operations do so. However, under the Commission and the Council version, the controller will have to determine whether specific or high risks are present.

---

[159] GDPR Parliament version, arts 32a(2)(a), (g) and (h).
[160] GDPR Commission version, art 33(2)(e); GDPR Parliament version, art 32a(f).
[161] GDPR Commission and Parliament version, arts 34(2)(b) and (4).
[162] GDPR Council version, arts 33(2a) and (2b).
[163] GDPR Commission version, art 33(6).

A DPIA is only required for "known" risks. Under the Commission and Parliament version, it is not clear whether "risk" should be ascribed its technical meaning: it might simply be intended to mean "threat". This would render the DPIA precautionary; action is required even if there is uncertainty on the probability of the threat. The Council does clearly see risk as something which can be assessed in terms of probability and thereby adheres to the technical definition: a risk is a threat of a certain probability. The boundary between risk and precaution depends on *when* the probability of a risk is "known"; this can, for example, depend on the amount of agreement amongst experts or amongst citizens. The more agreement is required, the higher the so-called "knowledge condition" and the less precautionary the rule. The Council version is not technically precautionary, but if the knowledge condition is very lenient, the difference is negligible.

It is argued above that, for the purposes of the DPIA, any interference with a right or a freedom is eligible to constitute a threat. As it is difficult to imagine a processing operation which does not, with some likelihood, interfere with a right or freedom, this is a very wide category. There are a number of criteria to determine whether the threat is probable and severe enough (the so-called "damage condition"). These include the severity and the likelihood of the processing (of course), and also the nature, the scope and the purpose of the processing. However, these criteria do not specify, by themselves, when a threat is risky enough to qualify as a specific/high risk. The GDPR contains a list of processing operations which meet the threshold. Although the Council has stated that the list is exhaustive, this does not appear to hold for the Council, nor for the Commission. The lists only concern operations which are by essence risky, mainly because of the large scale, but other cases can also present high risks. However, the Parliament's list is exhaustive, although it is so broad that the scope of the DPIA will not be smaller in practice. The supervisor authority (Commission, Council) or the European Data Protection Board (Parliament) can make additional lists of these risky cases.

The Parliament version is more detailed and offers more guidance. In contrast to the other two versions, it is clear in which cases a risk analysis needs to be carried out; what to look for during the analysis (the situations described in Article 32a(2)(a)-(h)); and when the processing qualifies as risky (if one of these situations is present). However, by offering an exhaustive list, the danger is that some potentially harmful processing operations slip through the net. The Commission and the Council version avoid this by posing as an overarching test the question whether the processing is risky.

	Commission	**Parliament**	**Council**
Risk threshold			
When is a DPIA required?	If the processing presents *specific risks* to the rights and freedoms of *data subjects*.	If the processing is likely to present *specific risks* to the rights and freedoms of *data subjects* by virtue of falling within the categories described in *Article 32a(2)(a)-(h).*	If the processing is likely to result in *high risks* to the rights and freedoms of *individuals*.
Is the initial risk analysis a continuing obligation?	Not clear.	Yearly review + if nature, scope or purposes change significantly.	Not clear: if necessitated by "the lapse of time".
Can multiple projects be can assessed together?	Yes, e.g. shared applications or platforms.	Yes, if similar processing operations present similar risks.	Yes.
Is there an exception if the processing is legally	Yes.	No.	Yes.

required or necessary to carry out public task?			
Does "risk" mean threat x probability?	Not clear: probability may not need to be known.	Not clear: probability may not need to be known.	Yes, both elements must be known. How precautionary this is depends on the knowledge condition.
What counts as risky?	Any risk to any right or freedom. See also Article 29 Working Party: privacy, freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination (...).	Any risk to any right or freedom. See also Article 29 Working Party: privacy, freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination (...).	Any risk to any right or freedom, e.g. discrimination, identity theft or fraud, financial loss, damage to the reputation (...). See also Article 29 Working Party.
How to assess riskiness?	Processing operations may pose risks by virtue of their nature, their scope or their purposes. See also Article 29 Working Party (→).	Article 29 Working Party: Risks must be assessed taking into account specific objective criteria, such as the nature of personal data, *the category of data subject*, the number of data subjects affected, and the purpose of the processing. The legitimate interests of the controller should not be taken into account.	Risks must be assessed taking into account the nature, scope, purposes and the *context* of the processing and in terms of their origin, nature, likelihood and severity. See also Article 29 Working Party (←).
Which types of processing are risky in essence?	Medium list, see Article 33(2). Supervisory authority must also make a list. The Commission can also specify criteria and conditions.	Long and broad, but exhaustive, list. See Article 32a(2). European Data Protection Board must make an additional list.	Short list, see Article 33(2). Supervisory authority must also make a list.

2.3 The duty bearer

In the Council version of the General Data Protection Regulation, Article 33 only applies to controllers. This implies that the controller cannot delegate this task to the processor – although the processor must assist the controller if this is necessary to carry out a DPIA.[164] As stated in Recital 66a, the controller should be responsible for the carrying out of a data protection impact assessment.[165] Considering that the controller should be the entity to make the decisions regarding the processing, the fact that the controller is the primary duty-bearer of the DPIA is in line with the general division of responsibility between the processing entities. The controller, being the party which bears the primary responsibility for data protection, is the entity which determines the purposes, conditions and means of the processing,[166] and so it is logical if the controller is the entity to assess the impact - or at least to determine which measures are to be taken to mitigate adverse effects.

However, it is imaginable that the processor, i.e. the entity which processes personal data on behalf of the controller,[167] carry out the impact assessment, after which any decisions as to the purposes, conditions and means of the processing are made by the controller. This appears to be envisaged by the Commission and the Parliament. In the Commission and Parliament version of

[164] GDPR Council version, rec 74a.
[165] GDPR Council version, rec 66a.
[166] GDPR, art 4(5).
[167] GDPR, art 4(6).

the General Data Protection Regulation, the controller *or the processor* should carry out the data protection impact assessment.[168] Should the processor thereby overstep the line, then it will also assume the responsibility of a controller. Indeed, if the processor processes personal data 'other than as instructed by the controller' or (in the Parliament version) 'becomes the determining party in relation to the purposes and means of data processing', then he shall be considered a joint controller, assuming the responsibility which is accompanied by that characterisation.[169]

As discussed above, the processing entity may be exempt from the obligation to carry out a data protection impact assessment if the processing is required by law or necessary to perform a public task. This exception , which is absent in the Parliament version, will mostly benefit public bodies and entities which fulfil a public function. Community institutions are also excluded from the GDPR; they will be covered by Regulation (EC) No 45/2001. Subject to the limits of the material and territorial scope of the GDPR,[170] the requirement to carry out a DPIA otherwise extends to all kinds of controllers.

In this thesis, the norm-addressee will generally be called the "controller", even though processors may also have obligations in relation to the DPIA under the Commission and Parliament version.

	Commission	**Parliament**	**Council**
Duty bearer			
	Processor or controller	Processor or controller	Controller

2.4 The subject-matter of the DPIA: what needs to be assessed?

While the Parliament requires that the impact of the processing operation 'on the rights and freedoms of the data subjects, especially their right to protection of personal data' is assessed,[171] the Commission and the Council both specify that the DPIA assesses 'the impact of the envisaged processing operations on the protection of personal data'.[172] However, also according to the Commission and the Council versions the impact assessment includes an assessment or evaluation of the risks to the rights and freedoms of data subjects. This is clarified by Article 33(3), which specifies what the DPIA must contain. Also Recital 70 of the Commission and the Council version presents the DPIA as a procedure or mechanism which focuses on processing operations which present a specific/high risk to the rights and freedoms of data subjects/individuals. The Council adds that such a high risk is present 'in particular where those operations render it more difficult for data subjects to exercise their rights'.[173] Meanwhile, the Parliament is apparently mostly concerned about data breaches and privacy-intrusive operations.[174] Is the DPIA a broad rights impact assessment, or is the focus on data security, (informational) privacy or compliance with data protection law?

Much of this confusion may be due to the conceptual lack of clarity from which data protection and particularly the right to the protection of personal data suffers. The next section will

[168] GDPR, art 33(1); GDPR Parliament version, art 32a(3).
[169] GDPR Commission and Parliament version, arts 26(4) and 24.
[170] GDPR, arts 2-3.
[171] GDPR Parliament version, art 33(1).
[172] GDPR Commission and Council version, art 33(1).
[173] GDPR Council version, rec 71.
[174] GDPR Parliament version, rec 71a.

therefore discuss what the protection of personal data, and especially the corresponding right, entails. It will argue that data protection has emerged as a legally autonomous right which is best understood as prohibitive. Nonetheless, the substance of data protection should be seen as safeguarding some of the dimensions of privacy and as instrumental to a possibly unlimited number of other rights and freedoms. This explains why a data protection impact assessment can focus on the protection of personal data, including data security and data subject rights, on privacy, and also on rights and freedoms. Finally, the DPIA is argued to be both a broad rights impact assessment, which includes an assessment of the right to the protection of personal data, and, to some extent, a data protection compliance check.

2.4.1 What is (the right to) protection of personal data?

2.4.1.1 Data protection and privacy: towards legal autonomy

Data protection law emerged in the 1970s, after digital data processing became possible.[175] While the wording appears to indicate differently, data protection does not exist for the protection of data (i.e. data security). For a long time, data protection was commonly seen as safeguarding the "informational" dimension of privacy concerned with the control individuals have over the information which relates to them.[176] Not all Member States, however, developed data protection under the heading of privacy. The German Federal Constitutional Court famously ruled that data protection is based on the right to informational self-determination. Similar to informational privacy, it concerns the possibility for individuals to determine what data on them is processed, protecting the free development of personality of individuals. However, it emanates not from privacy but from the right to dignity.[177] Nonetheless, data protection was frequently framed as a safeguard of privacy – most notably by the Data Protection Directive. Back in 1995, the Data Protection Directive was given the two-fold objective of protecting both 'the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data' and the free flow of personal data between Member States.[178] While this does not ambiguously exclude a relationship between data protection and other rights, this has strengthened the understanding of data protection as instrumental to privacy: data protection "serves" privacy,[179] or, perhaps more accurately, provides for a balance between privacy and the free flow of information.

In the meantime, the European Court of Human Rights has treated cases on the processing of personal data within the framework of Article 8 ECHR, which protects the right to respect for private and family life, home and correspondence. If the data concerns the private life of individuals or if the data processing is very extensive, then the processing will fall within the scope of the right to privacy. As a result, some cases which are covered by data protection legislation also affect privacy (some personal data is also private data), while it is also imaginable that some data processing which is not covered by data protection is covered by

---

[175] F Borgesius, 'Improving privacy protection in the area of behavioural targeting' (PhD thesis, University of Amsterdam 2014) 133.
[176] G González Fuster and S Gutwirth, 'Opening up personal data protection: a conceptual controversy' (2013) 29(5) Computer Law & Security Review 531, 536; G González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) 214.
[177] González Fuster (2014) 176-177.
[178] Data Protection Directive (DPD), art 1.
[179] González Fuster and Gutwirth (2013) 535. See also PRISMS, 'Deliverable 5.2: Consolidated legal report on the relationship between security, privacy and personal data protection in EU law' (2014) 17.

privacy (some non-personal data is private).[180] It should be noted that the scope of Article 8 ECHR goes far beyond situations of data processing. It also concerns, for example, the right to marry and found a family, the right to protection of one's reputation, the right to develop one's personality, the right to gender identification and sexual orientation, the right to residence and legal identity, and the right to a healthy living environment.[181] A part of data protection is thus also a part of privacy in the case law of the ECtHR.

With the coming into full legal effect of the Charter of Fundamental Rights of the European Union in 2009 – the Charter was drafted already in 2000, but is a binding instrument by virtue of Article 6(1) TEU -[182] the right to the protection of personal data was given its own place in Article 8, existing next to the right to privacy of Article 7 of the Charter and Article 8 ECHR. The idea that data protection is a part of privacy gave place for the conceptualisation of data protection as an autonomous right which may emanate from or partly overlap with privacy.[183] Thus, in the *Deutsche Telekom* case, the European Court of Justice states that the Data Protection Directive is designed to ensure observance of the right to protection of personal data.[184] Anno 2015, the GDPR is drafted by the Commission, the Parliament and the Council to lay down 'rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data' and to protect '~~the~~ fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'.[185] All three versions of the GDPR present this as the objective of the General Data Protection Regulation. As data protection law now 'develops first and foremost the EU right to the protection of personal data', [186] the formal ties between data protection law and privacy have been severed by the birth of the right to the protection of personal data as an autonomous right.

Now that data protection has been presented in EU law as an autonomous right, the question arises what the object of its protection is. The next sections will argue that the common conceptualisation of data protection as a transparency tool is not sufficient, and that it should be regarded instead as a prohibitive right which protects privacy as limited access and privacy as control. It also serves other rights and freedoms, but it does not exhaust them.

2.4.1.2 Data protection is not a transparency tool

The most prominent conceptualisation of data protection is that of a transparency tool. It appears to avoid an analysis of the object of protection of data protection law and the corresponding right**.** According to this widely accepted portrayal, the difference between data protection and privacy can be explained by what has been called their 'rationale':

---

[180] *Amann* 65; *Rotaru v Romania* 43; *P.G. and J.H. v the United Kingdom* 57; Gellert and Gutwirth (2013) 526.
[181] B van der Sloot, 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"' (2015) 31(8) Utrecht Journal of International and European Law 25; Gellert and Gutwirth (2013) 527.
[182] G Di Federico, 'Fundamental Rights in the EU: Legal Pluralism and Multi-Level Protection After the Lisbon Treaty' in G Di Federico (ed), *The EU Charter of Fundamental Rights: From Declaration to Binding Instrument* (Springer 2011) 38.
[183] González Fuster and Gutwirth (2013) 536; González Fuster (2014) 214-215.
[184] Case C-543/09 *Deutsche Telekom AG v Bundesrepublik Deutschland [*2011] ECR I-03441, para 50. **However, in other recent cases the CJEU does not clearly separate data protection from privacy,** see Gellert and Gutwirth (2013) 528-529.
[185] GDPR, arts 1(1) ad 1(2).
[186] PRISMS, 'Deliverable 5.1: Discussion paper on legal approaches to security, privacy and personal data protection' (2013) 21.

'*Privacy is an opacity tool, that is, a prohibitive and normative tool that determines whether an interference with individual autonomy is acceptable or not. If such interference is deemed unlawful then the state must restrain from interfering with the right. (...) Instead, we have coined data protection a transparency tool, that is, a tool that channels the normatively accepted exercise of power through the use of safeguards and guarantees in terms of accountability and transparency. Data protection legislations obey such logic: they generally do not dispute the fact that personal data might be processed, but they submit the processing to rules and conditions, they empower data subjects by giving them subjective rights and they establish supervisory bodies in order to make sure that data processors don't abuse their powers*.'[187]

Thus, according to this conceptualisation, privacy limits the reach of the state, while data protection permits access to data but also subjects this to positive obligations. It is frequently stated that privacy draws 'normative limits', 'protecting individuals by saturating their opacity in front of power', while data protection provides for transparency 'by organising and regulating the ways a processing must be carried out in order to remain lawful'.[188] 'Data protection as such does not aim to prohibit the processing of data, but rather only 'some unlawful data processing practices'.[189] The difference is thus captured by an interpretation of data protection as a permissive rather than a prohibitive system. Data protection says "yes, but", managing rather than prohibiting data flows.[190] One of the ways in which the fairness of data processing is ensured, is through the requirement that data processing is transparent. 'Hence: a transparency tool'.[191] However, this does not say anything about the substance of the rules which regulate data processing and their object of protection. Are they designed to protect privacy, or perhaps also other rights and interests?

This conceptualisation is limited not only by the lack of a theory on what data protection protects. It does not do justice to the right to privacy as protected by the ECtHR, which does include positive obligations. It has grown from a classic negative right to a personality right, requiring Member States to take action to protect the personal development of individuals.[192] Privacy also requires government action in the sphere of data processing. In the *Klass* case, the ECtHR formulated conditions under which wiretapping – an interference with the right to privacy – is justified, which included measures to guarantee the transparency and accountability of the wiretapping process.[193] Privacy is not just opacity, also in the data processing context.[194] Moreover, case law of the CJEU indicates that data protection is prohibitive, while its conceptualisation as a transparency tool characterises it as permissive. This is discussed in the next section.

---

[187] PRESCIENT, 'Deliverable D1: 'Legal, social, economic and ethical conceptualisations of privacy and data protection' (2011) 8. See also P De Hert and S Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E Claes, A Duff and S Gutwirth (eds), *Privacy and the criminal law* (Intersentia 2006) 10-18.
[188] González Fuster and Gutwirth (2013) 536; PRISMS (2013) 15.
[189] PRISMS (2013) 15.
[190] González Fuster and Gutwirth (2013) 536; Borgesius (2014) 150.
[191] Borgesius (2014) 150.
[192] van der Sloot (2015).This is acknowledged: De Hert and Gutwirth (2006) 11-13.
[193] *Klass and others v Federal Republic of Germany* (1978) 2 EHRR 214; PRESCIENT (2013) 48.
[194] A Rouvroy and Y Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in S Gutwirth, Y Poullet, P De Hert, C De Terwangne and S Nouwt (eds), *Reinventing Data Protection?* (Springer 2009) 76.

2.4.1.3 A prohibitive notion

This section will argue that data protection is prohibitive. In European scholarship, some view data protection as permissive (data processing is allowed, but only if...) while others view it as prohibitive (data processing is not allowed, except if...).[195] To investigate the issue, this thesis makes a distinction between data protection *law* and the corresponding *right.*

The characterisation of the *right* to the protection of personal data is important because signifies when the right to the protection of personal data is respected or infringed. In the following, it is argued that Article 8 is prohibitive; this interpretation has more support. First, the permissive interpretation is considered. According to this interpretation, Article 8 is respected if the principles of data protection law in paragraphs 2 and 3 are adhered to. The most persuasive argument is that the other rights of the Charter specify what they protect in the corresponding Article (e.g.: 'Everyone has the right to respect for his or her private and family life, home and communications' in Article 7), whereby limitations are permitted on the basis of Article 52. Similarly, the whole of Article should be seen as the core of the right. Article 8 was even first presented in one paragraph and only divided later to improve the readability.[196]

However, Article 8 contains, in paragraph 2 and 3, a number of conditions under which data may be processed. As such, it does not follow the same structure of the other rights. The question therefore arises whether Article 8 prohibits the processing of personal data except if the conditions of paragraph 2 and 3 and/or of Article 52 apply, or whether it allows the processing of personal data, whereby the conditions of paragraph 2 and 3 and/or of Article 52 must be met. The prohibitive explanation is that Articles 8(2) and 8(3) present specific lawful limitations, as a lex specialis over the lex generalis of Article 52.[197] This would entail that the principles of data protection form lawful limitations to the right to protection of personal data.

Article 8
Protection of personal data
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

The prohibitive interpretation is supported by the Explanations relating to the Charter and by a strand of case law of the CJEU. The Explanations state that the Data Protection Directive and the Regulation for processing by Community Institutions 'contain conditions and limitations for the exercise of the right to the protection of personal data'.[198] This indicates that the principles of data protection law, which are present in paragraph 2 of Article 8 and in the abovementioned Directive and Regulation, form exceptions to a prohibitive right rather than the core of a permissive

[195] PRISMS (2013) 15.
[196] Praesidium of the European Convention, 'Presidency Note: Draft Charter of Fundamental Rights of the European Union - Complete text of the Charter proposed by the Praesidium' (CHARTE 4422/00 CONVENT 45, 2000) 4; González Fuster and Gutwirth (2013) 535.
[197] González Fuster and Gutwirth (2013) 535-536.
[198] Praesidium of the European Convention, 'Explanations relating to the Charter of Fundamental Rights' (2007/C 303/02).

right. Moreover, as aptly phrased by González Fuster and Gutwirth, the CJEU 'habitually equates any processing of personal data with a limitation of the right, implying that the right's core content is substantiated in Article 8(1) of the Charter, to be read, therefore, as proclaiming that personal data shall in principle be left unprocessed'.[199] In *Deutsche Telekom* and *Schecke*, the CJEU considered that Article 8(1) of the Charter states that '[e]veryone has the right to the protection of personal data concerning him or her', but that this is not an absolute right. It then states that 'Article 8(2) of the Charter thus authorises the processing of personal data if certain conditions are satisfied'.[200] Therefore, *Schecke* should be read as finding an interference of Article 8 of the Charter because data was processed, which was not authorised by Article 8(2) because consent was not obtained.[201] Like Article 7(1), Article 8(1) contains the core of the right, which is not absolute. Unlike the other rights of the Charter, the interference of which can be justified on the basis of Article 52 only, Article 8 goes on to provide for the conditions under which the right can be interfered with in paragraphs 2 and 3 (e.g. consent).

In two other cases the mere processing alone is again regarded as an interference. In *Scarlet* and *Netlog*, the Court deals with an injunction which would require the processing of personal data by balancing a number of rights which are at stake, including the right to the protection of personal data. The CJEU finds that the requested injunction might unjustifiably interfere with Article 8 of the Charter, as it would involve the 'systematic analysis' of personal data.[202] It engages in a balancing exercise on the rights level and finds that data protection law and other directives must be interpreted in light of this balance.[203] González Fuster and Gutwirth erroneously conclude therefrom that Article 8 is permissive : they argue that if Article 8 was prohibitive, then its justification should also be investigated on the basis of the fair information principles of Article 8(2).[204] However, the Court had good reason not to go through the fair information principles. The issue was whether EU law precludes the contested injunction. Copyright law requires the injunction, but it processes personal data. It had been decided in *Promusicae* that data protection law allow Member States to provide for exceptions so as to protect copyright.[205] Member States are thus not precluded from providing such measures. But because the copyright directives apply without prejudice to data protection, the CJEU finds that they do not *require* Member States to make use of this possibility to provide for an exception to data protection in order to enable rights holders to enforce their copyright either.[206] The resulting discretion must be used in a manner which strikes a fair balance between the various

---

[199] González Fuster and Gutwirth (2013) 538.
[200] *Deutsche Telekom*, paras 49-51.
[201] *Schecke*, paras 60-64; Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR v Land Hessen* [2010] ECR I-11063, paras 47-49.
[202] Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeur SCRL (SABAM)* [2011] ECR I-11959, para 54; Case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)* v *Netlog* [2012] 2 CMLR 18, para 51.
[203] *Scarlet*, para 54; *Netlog*, para 51. **The CJEU requires Member States to strike a fair balance, which is marginally tested.** See also Case C-101/01, *Bodil Lindqvist* [2003] ECR I-12971, para 87; Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I-00271, para 68; Case C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH* [2009] ECR I-01227, para 28; Case C-461/10 *Bonnier Audio AB and Others v Perfect Communication Sweden AB* (ECJ, 19 April 2012), para 56-58; Case C-314/12 UPC *Telekabel Wien GmbH v Constantin Film Verleih GmbH* (ECJ, 27 March 2014), para 43-62.
[204] González Fuster and Gutwirth (2013) 538-538.
[205] Promusicae, para 53.
[206] Promusicae, para 57. See also Lindqvist, para 97; Joined Cases C-468/10 and C-469/10, *ASNEF* [2011] ECR I-12181, para 34.

rights at stake.[207] Instead of looking whether the interference with each of the rights at stake is justified, the CJEU requires them to be reconciled or balanced in a fair manner. The issue in *Scarlet* and *Netlog* is thus whether a fair balance is struck; not whether the interference with the right to the protection of personal data is illegitimate.

In *Google Spain*, the CJEU also appears to use a prohibitive understanding of the right to data protection. The right to the protection of personal data (and also the right to privacy) is liable to be significantly affected by the processing of personal data which Google performs if an individual's name is googled because this allows a detailed profile about an individual, composed of the information which is available about him or her online, to be obtained.[208] In short, because a detailed profile about an individual can be accessed through a Google search, the right to the protection of personal data is significantly interfered with. Insofar as this right is additionally interfered with by Google, as opposed to the original publishers of the information, Google has to ensure that the requirements of data protection law are met.[209] These requirements must be interpreted in light of fundamental rights,[210] which leads to the construction of the "right to be forgotten" for which the ruling is famous.[211] As a result, in *Schecke*, *Deutsche Telekom*, *Scarlet*, *Netlog* and *Google Spain* the CJEU has treated Article 8 of the Charter as a prohibitive right.

The prohibitive interpretation of the right to the protection of personal data is logically accompanied by a prohibitive understanding of the GDPR. When considered in isolation, the GDPR seems to be permissive. The processing of personal data is allowed if the controller complies with a set of principles and rules. The structure is that of "yes, but".[212] Article 5 GDPR does not state that personal data may not be processed, but rather that personal data must be processed in a manner which complies with the data quality principles.[213] Moreover, the twofold objective of data protection law includes the free flow or movement of information.[214] However, the principles of data protection provide the conditions under which an interference with the right to the protection of personal data is in principle lawful - subject to a constitutional or fundamental rights review by the court. It is inconsistent to characterise them as permissive because they mark the exception to the "no".

2.4.1.4 The substance of the protection of personal data and the corresponding right

What does it mean to protect personal data? It is not enough to say that data protection is about treating data fairly or with due care; this only shifts the problem, because it is not clear what fairness or "due care" requires. It can be tied to privacy, but privacy as a whole is too broad a notion; as argued under section 2.4.1.1, privacy includes many things which data protection law does not cover. At the same time, privacy is too narrow: data protection also protects the right to non-discrimination, for example. This section will conduct a legal analysis into what data protection protects by discussing the three dimensions of privacy identified by Borgesius and

[207] Promusicae, para 67-68.
[208] Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos (AEPD)* (ECJ, 13 May 2014), para 80.
[209] *Google Spain*, para 83.
[210] *Google Spain*, para 68.
[211] *Google Spain*, para 97.
[212] Borgesius (2014) 150;
[213] GDPR, art 5. cf DPD, art 6.
[214] GDPR, arts 1(1) and 1(3); DPD, art 1(2); PRESCIENT (2013) 47.

the notion of data protection as ancillary to other rights and freedoms. It follows from the cases discussed above that the processing of personal data interferes with Article 8(1), but that it can be authorized or justified if a number of conditions are met, including consent. This can be tied to privacy as limited access and on privacy as control. The conditions which can authorize the inference also protect fundamental rights and freedoms. As a result, data protection also serves to protect other rights and freedoms – but, it is argued, without exhausting them.

Privacy

The fact that data protection is now *legally* an autonomous right does not mean that its substance is no longer (partly) about privacy. Privacy is an ill-defined and multifaceted notion. The right to privacy has been conceptualised, amongst others, as containing three overlapping dimensions, which are by themselves incomplete or insufficient: privacy as limited access, privacy as control over personal information, and privacy as freedom from unreasonable constraints on identity construction. This classification is put forward by Borgesius on the basis of work by Gürses.[215] The three conceptualisations succeeded each other in time and now exist next to each other as three different perspectives on privacy.[216] Privacy as limited access protects a personal sphere within which people can remain free from interference by the state or other actors. It regards the extent to which we are accessible by others; the extent to which we are known by them (confidentiality) and to which we are subject to their attentions ("the right to be let alone",[217] "the right not to be annoyed").[218] Privacy as control, as the claim 'to determine when, how and to what extent information about them is communicated to others',[219] became influential as worries grew about the "secret" decisions which would be made about people on the basis of their (possibly incorrect or irrelevant) data.[220] This dimension of privacy has been very influential in European data protection law.[221] A third dimension of privacy protects "the freedom from unreasonable constraints on the construction of one's identity".[222] People should be free to develop their identity and try to influence how they are perceived by others. This may be alone or together with others, and it may include sharing information or keeping it confidential. It includes a protection against 'unreasonable steering or manipulation' by other people or by the digital environment -[223] keeping in mind that code can regulate.[224] Online personalisation can influence people and therefore constrain the construction their identity.[225]

The first two dimensions of privacy are present in the right to the protection of personal data as interpreted by the CJEU and substantiated by the GDPR. This right, as applied by the CJEU,

---

[215] Borgesius (2014) ch 3.1. See also S Gürses, 'Multilateral Privacy Requirements Analysis in Online Social Networks' (PhD thesis University of Leuven, 2010) 24-32.
[216] Borgesius (2014) 83-95.
[217] Commonly attributed to S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193, 195.
[218] H Varian, 'Economic aspects of personal privacy' in W Lehr and L Pupillo (eds), *Internet policy and economics* (Springer 2009) 102. See also R Gavison, 'Privacy and the Limits of Law' (1980) 89 Yale Law Journal 421, 424; Borgesius (2014) 85.
[219] A Westin, *Privacy and Freedom* (The Bodley Head 1970) in Borgesius (2014) 87.
[220] Borgesius (2014) 87-88.
[221] Borgesius (2014) 90.
[222] P Agre, 'Introduction' in P Agre and M Rotenberg (eds), *Technology and Privacy: the New Landscape* (MIT Press 1998) 7; Borgesius (2014) 92.
[223] Borgesius (2014) 93.
[224] L Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harvard Law Review 501.
[225] M Hildebrandt, 'Who needs stories if you can get the data? ISPs in the era of big number crunching' (2011) 24(4) Philosophy & Technology 371, 381; Borgesius (2014) 94.

protects privacy as limited access. As explained above, in *Scarlet* and *Netlog* the CJEU considers that any processing of personal data falls within the scope of this right. Apparently, the collection, storage, use or disclosure of personal data infringes the right to the protection of personal data. These actions all entail that the data is accessed or can be accessed at a later point. In *Google Spain*, the issue was that a detailed profile could be accessed. This makes for a *significant* interference with the right to the protection of personal data. Taken together, these rulings indicate that Article 8(1) of the Charter is interfered with if personal data is made accessible. The GDPR contains requirements which must be met for data to be accessed lawfully. This protects privacy as limited access. The obligation to maintain data security can also be seen in this light: unauthorized disclosures should be prevented.[226]

Privacy as control is protected by data protection law and by Article 8. The Commission stated that, 'in this new digital environment, individuals have the right to enjoy effective control over their personal information. Data protection is a fundamental right in Europe, enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (...)'.[227] This implies that the right to the protection of personal data entails not only a right of limited access to personal data but also a right of control over personal data. If data is processed in a manner which leaves little power to data subjects, it is interfered with more harshly or is less readily justified. The GDPR emphasises data protection as privacy as control, also known as informational privacy or informational self-determination. According to PRESCIENT, privacy impact assessments usually target informational privacy, which they present as the aspect of privacy which coincides with data protection.[228] Recital 6 of the GDPR highlights that the data protection *framework* should give individuals control over their data. Consent and data subject rights accordingly take an important place in data protection law. At the moment, consent is a frequently relied-on ground to legitimize the processing of personal information. In many cases, it is the only available legal ground.[229] Data subject rights include the right to be informed of a number of categories of information,[230] to access, rectify or erase data concerning you,[231] and to object to the processing or the ability to withdraw your consent.[232] The GDPR extends the definition of consent and strengthens the data subject rights.[233]

The third dimension, privacy as freedom from unreasonable constraints on identity construction, is less clearly protected by data protection. Rouvroy and Poullet argue that data protection and privacy both aim to protect 'the autonomic capabilities of the individual legal subject'.[234] They consider data protection and privacy as together advancing 'the capacity of the human subject to keep and develop his personality in a manner that allows him to fully participate in society without however being induced to conform his thoughts, beliefs, behaviours and preferences to those thoughts, beliefs, behaviours and preferences held by the

[226] GDPR, art 30.
[227] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century' COM(2012) 9 final, 2.
[228] PRESCIENT (2013) 73.
[229] DPD, arts 7(a) and 8(2)(a); ePrivacy Directive, arts 6, 9 and 13.
[230] DPD, art 10.
[231] DPD, art 12.
[232] DPD, art 15; Article 29 Working Party, 'Opinion 15/2011 Consent' (WP197, 2011).
[233] GDPR, rec 25 and arts 4(8), 17, 19 and 20(1).
[234] Rouvroy and Poullet (2009) 76.

majority'.[235] This is in line with the right to informational self-determination, which grants individuals control in order to protect the free development of personality of individuals.

However, data protection does not directly express this object. It probably should be the underlying value, as argued by Rouvroy and Poullet, but positive law does not clearly indicate that it is protected; there is no legal reason to assume that an unreasonable constraint constitutes an interference with Article 8. The GDPR restricts profiling: the use of data to evaluate personal aspects of an individual to analyse and predict his or her performance at work, economic situation, health, personal preferences or interests, location or movements, or more generally his or her behaviour. Data subjects can object to profiling if it produces legal effects or significantly affects them.[236] As noted in section 2.2.4, profiling is also considered one of the "risky" types of processing which should be subject to an assessment of the impact on the right to the protection of personal data.[237] This regulation of measures which may significantly affect people implies a concern for individuals which is reminiscent of the protection of their freedom to develop their identities. However, the regulation of profiling may also be intended to protect other values – a concern over discrimination is explicitly mentioned.[238] Moreover, under a regulation of profiling which serves privacy as identity construction, a data subject should arguably not be able to consent away[239] his or her freedom to not be manipulated by a digital environment which is personalised on the basis of his or her profile. It would be farfetched to argue that the right to the protection of personal data serves to protect against unreasonable constraints on identity construction only because the GDPR restricts profiling.

Fundamental rights and freedoms

Data protection does not only concern privacy as limited access and privacy as control. The Data Protection Directive and the GDPR both have as their objective the protection of fundamental rights and freedoms, in particular privacy and data protection respectively.[240] In the *Lindqvist* case, it was clarified that the Data Protection Directive sees to all fundamental rights at stake, not just privacy.[241] The GDPR further contains many references to rights and freedoms, sometimes accompanied by the adjective "fundamental", indicating that data protection law also aims to protect them. For example, Recital 8 of the GDPR stresses that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data should be equivalent in all Member States, highlighting that other rights and freedoms are also relevant to data processing. Moreover, while the Commission found that personal data which are particularly sensitive and vulnerable in relation to fundamental rights *or privacy* deserve specific protection, the Council finds that data protection law should be extra protective of sensitive data because the context of their processing may create important risks *for the fundamental rights*

---

235 Rouvroy and Poullet (2009) 75.
236 GDPR Parliament and Council version, art 4(12)(a); GDPR, art 20.
237 GDPR Commission and Council version, art 33(2)(a); Parliament version, art 32a(2)(c).
238 GDPR Parliament and Council version, rec 58.
239 GDPR, rec 59 **clarifies that profiling is permitted on the basis of the data subject's consent.**
240 DPD, art 1(1); GDPR, art 1(2).
241 *Lindqvist*, para 97; Gellert and Gutwirth (2013) 529. **Note that the TFEU did not contain a legal basis for the protection of fundamental rights. According to Advocate General Tizzano, fundamental rights protection is therefore not an independent objective of the Data Protection Directive** (Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof v Österreichischer Rundfunk* [2003] ECR I-04989, Opinion of AG Tizzano, paras 52-55). **However, the EU is now competent to adopt 'rules relating to the protection of individuals with regard to the processing of personal data'** (Article 16 Treaty on the Functioning of the European Union (TFEU)).

and freedoms.[242] Similarly, the situations which are considered risky and which should therefore be subjected to a data protection impact assessment are also linked to rights other than privacy. Article 33 refers to the risks to the rights and freedoms of individuals – privacy is not even mentioned as such. One of the situations which is explicitly considered risky, profiling, may be especially relevant with regard to right to non-discrimination. Online personalisation or (credit) scoring on the basis of profiles can be discriminatory even if the profile does not contain information relating to the legally protected categories.[243] For example, if the inhabitants in certain area codes are predominantly from a certain ethnic background, this characteristic may creep into the model and indirectly discriminate against minorities.[244] Article 33(3)(c) of the Parliament version even mandates that the risk of such "encoded" discrimination should be addressed. Clearly data protection law is about other rights too – and the special relationship with privacy in particular may even be coming to an end.

Data protection law has accordingly been interpreted as protecting against consequences for privacy *and* other fundamental rights. Indeed, it covers data processing operations which may impact a host of other rights and freedoms. 'For example, data processing can impact upon people's freedom of expression, freedom of religion and conscience, voting rights, etc. Most importantly, the know- ledge of individuals that can be inferred from their personal data may also bear risks of discrimination.'[245] Some scholars even consider data protection a purely procedural body of law which serves other rights and freedoms. Data protection (both the right and the body of law) 'does not directly represent any value or interest *per se*, it prescribes the procedures and methods for pursuing the respect of values embodied in other rights'.[246] In other words, data protection law provides channels for the coordination of different rights, through which controllers 'try to reconcile fundamental but conflicting values such as privacy, free flow of information, the need for government surveillance, applying taxes, etc'.[247] Poullet and Rouvroy take a different stance. As previously noted, they argue that data protection serves individual autonomy, rather than the collection of other rights and freedoms which pop up in the digital context. Autonomy is a precondition 'to any meaningful exercise of all other rights and freedoms acknowledged by the Council of Europe'.[248] However, the prominent place of other rights and freedoms in the GDPR indicates that data protection law is more directly concerned with these rights and freedoms than "only" safeguarding the autonomy which they require.

The rules for fair and legitimate processing laid down in data protection law can authorize or help legitimise an interference with Article 8. Consequently, the right to the protection of personal data indirectly serves to protect a range of rights and freedoms, just as data protection law does. It is debatable whether the procedural or ancillary perspective on the right to the protection of personal data is commensurate with its prohibitive nature. Data protection law

---

[242] GDPR, rec 41.
[243] T Zarsky, 'Understanding Discrimination in the Scored Society' (2014) Washington Law Review 89(4).
[244] L Moerel, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof?' (inaugural lecture 2014) 11.
[245] PRESCIENT (2013) 52.
[246] N de Andrade, 'Oblivion: The Right to Be Different.. from Oneself. Reproposing the Right to Be Forgotten' (2012) 13 Revista de los Estudios de Derecho y Ciencia Política de la UOC 122, 125; Gellert and Gutwirth (2013) 529-530; G Zanfir, 'Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law' in S Gutwirth, R Leenes and P De Hert (eds), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014) 245.
[247] P De Hert and S Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in S Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009) 3.
[248] Rouvroy and Poullet (2009) 75-76.

indeed provides mechanisms and methods to reconcile various rights and interests in the digital context, but this is not its principal object under a prohibitive conceptualisation of the right to the protection of personal data. The mechanisms and methods of data protection law provide for exceptions to this right. However, also under a prohibitive notion, these mechanisms are there for a reason – they just operate under a different "rationale". At the end of the following section, a conceptualisation of a legally autonomous, prohibitive and substantially ancillary right to protection of personal data is provided.

The GDPR ≠ fundamental rights protection

According to the fourth PRESCIENT deliverable, it is possible to regard processing operations which do not violate data protection law as ipso facto commensurate with the right to the protection of personal data and therefore with the fundamental rights and freedoms which the right to the protection of personal data serves.[249] Data protection would be the ultimate rights reconciler in the digital context. This requires two assumptions. Firstly, data protection law is seen as exhaustively providing for protection of the right to the protection of personal data. In other words, the right to the protection of personal data has no say, it has been fully substantiated in data protection law. This view is counter to the function of fundamental rights. As a fundamental right, the right to the protection of personal data must be understood to protect a certain object or value above and beyond the law which substantiates this protection. In other words, data protection law does not exhaust the right to the protection of personal data, just like non-discrimination laws do not exhaust the right to non-discrimination. Fundamental rights rather serve as a check on state power, and increasingly also as a check on the actions of both governmental and non-governmental entities.[250] While the European Union is not a federal state with one constitutional identity, the Charter is a bill of rights which bestows on the CJEU a power of judicial review.[251] As a result, the actions of governmental entities, and perhaps also those of non-governmental entities, are subject to a rights review which exceeds a mere review of the compliance with legislation.

Moreover, the case law of the CJEU indicates that European data protection law does not exhaustively strike the right balance between the various rights and freedoms. The principal case is *Lindqvist*, in which the CJEU reasoned that because the Data Protection Directive contains relatively general provisions with a degree of flexibility, leaving the Member States to decide on the details or choose between various options,[252] the balance between the rights and interests must be found at the stage of the application at national level.[253] '*Consequently, it is for the authorities and courts of the Member States not only to interpret their national law in a manner consistent with Directive 95/46 but also to make sure they do not rely on an interpretation of it which would be in conflict with the fundamental rights protected by the Community legal order or with the other general principles of Community law, such as inter alia the principle of proportionality*.'[254] As a result, the provisions of the Data Protection Directive do not, in

[249] PRESCIENT (2013) para 4.3.
[250] A Reinisch, 'The Changing International Legal Framework for Dealing with Non-State Actors', in P Alston, *Non-State Actors and Human Rights* (Oxford University Press 2005). T**he Charter only addresses Member States and EU bodies and institutions (Article 51(1) of the Charter).**
[251] cf O Zetterquist, 'The Charter of Fundamental Rights and the European Res Publica' in G Di Federico (ed), *The EU Charter of Fundamental Rights: From Declaration to Binding Instrument* (Springer 2011).
[252] *Lindqvist*, para 83.
[253] *Lindqvist*, para 85.
[254] *Lindqvist*, para 87.

themselves, bring about a restriction of freedoms or fundamental rights, but it is for the national authorities and courts to ensure a fair balance between these rights and interests.[255] This ruling is later refined in a number of cases which concern the balance between data protection and effective copyright protection. In *Promusicae*, the CJEU ruled that not only the Data Protection Directive but all the directives relevant to the mater at hand must be interpreted in a manner which strikes a fair balance.[256] The mechanisms for balancing the different rights and interests are contained in these directives and in their national implementations.[257] The AG explains, in line with *Lindqvist*, that the balance between the relevant fundamental rights must be struck first by the Community legislature and the Court, although Member States have to observe it 'when using up any remaining margin for regulation in the implementation of directives'.[258] Note that the balance is struck not only in data protection law, but also in other instruments of EU law. Together, these instruments must be interpreted in a way which reconciles the applicable rights in a proportionate manner. Similarly, in *Scarlet* and *Netlog* the balance was found not through the directives but by weighing up the different rights which are involved. The directives are then interpreted in light of this balancing act on the rights level.[259]

What all these cases have in common, is that the Data Protection Directive does not exhaustively strike the right balance. It rather leaves a room for manoeuvre for Member States, which they must use in a manner which strikes a proportionate balance. As a result, mere adherence to the provisions of data protection law is not necessarily enough to respect the right to the protection of personal data and the other rights and freedoms which may be involved. However, this conclusion is subject to two reservations; of which the last one sticks. Firstly, the GDPR is not a directive but a regulation, and thus it has direct effect. This may entail that the balance provided by the EU legislature in the GDPR is necessarily, exhaustively correct. While this conclusion might have held under *Lindqvist* alone, the fact that the balancing act takes place through other directives also (*Promusicae*) or even solely on the rights level indicates that no instrument of EU law (*Scarlet* and *Netlog*) can have the last word. A balancing act must be undertaken to reconcile different instruments of EU law and may even take place on the rights level. Just as the Data Protection Directive must be interpreted in light of other directives (which are its hierarchical neighbours) or rights (which stand higher in the hierarchy), the General Data Protection Regulation must surely be interpreted in light of its neighbours or its superiors. The second reservation is that the duty to reconcile the various legal instruments is addressed to the courts and authorities of Member States. Just like the legal accountability of non-state actors for human rights abuses is still incomplete, this duty may not fully extend to other entities.

The second assumption which is required to argue that any data protection compliant processing can no longer be held to conflict with fundamental rights and freedoms is that the right to the protection of personal data exhaustively provides for fundamental rights protection in the digital context. It has been argued in the preceding section that the right to the protection of personal data could be a procedural or ancillary right, serving other fundamental rights by providing mechanisms and procedures which pursue to respect the values embodied in these other rights. This does not necessarily mean that the mechanisms and procedures through

[255] *Lindqvist*, para 90.
[256] *Promusicae*, para 68.
[257] *Promusicae*, para 67.
[258] *Promusicae*, Opinion of AG Kokott, para 56.
[259] *Scarlet*, para 54; *Netlog*, para 52; Section 2.4.1.3.

which the various rights and interests are reconciled exhaustively provide the right balance. Fundamental rights and principles should still have a say in the matter. None of the non-absolute fundamental right trumps the others.[260] As indicated in *Scarlet* and *Netlog*, rights need to be reconciled. The right to the protection of personal data can be the place where these rights are reconciled in the digital context, but it should not do so in isolation. Considering that these other rights would continue to exist, at least in the non-digital context, the different vessels should remain in communication. The "non-digital freedom of expression" and the "non-digital right to privacy", for example, will evolve and will be reconciled in different ways, and the right to the protection of personal data should evolve with it and provide for reconciliations that match. As a result, the non-digital counterparts of the rights which data protection protects still have a say.

To conclude, compliance with the GDPR does not equal respect for fundamental rights. The GDPR is ancillary; it protects numerous dimensions of privacy and other rights and freedoms, and somewhere in that mix is the right to the protection of personal data. However, this does not necessarily mean that controllers, by being compliant with data protection law, also respects the right to the protection of personal data. More may be needed to prevent infringements of Article 8 of the Charter. The same applies to other rights. Courts and governmental authorities, and to some extent also non-governmental entities, cannot escape accountability for violations of fundamental rights because they comply with an EU regulation. This is even provided for in a separate provision in the Parliament version: the GDPR 'shall not have the effect of modifying the obligation to respect fundamental rights and fundamental legal principles'.[261]

A conceptualisation of the right to the protection of personal data as a legally autonomous, prohibitive and substantially ancillary right could work out as follows. The protection of personal data is interfered with if personal data is processed, and less justifiably so if it is processed in a manner which leaves little control to data subjects. Exceptions should be assessed during a rights review on a number of different levels. 1. The principles of Article 8(2) and (3) of the Charter must be met. Any interference must meet these requirements, which are ancillary to a number of rights and freedoms. Moreover, data protection law needs to be interpreted in light of a proper rights balance, so the fundamental rights and principles of EU law come in again. Compliance with data protection law is necessary to justify the processing of personal data, but it is not enough: the test of Article 52 should also be met. 2. The assessment of Article 52 includes the legality and proportionality of the interference. The principles of data protection, as contained in Article 8(2) and (3) of the Charter and in the GDPR, may or may not serve as the legal basis. The interference with the right to the protection of personal data which any compliant processing of personal data necessarily constitutes, is only legitimate if it is proportionate. This requires a balancing between the interest behind the processing and the right to the protection of personal data.

[260] **According to Gewirth, there is only one absolute right: to not be made victim of a homicidal project. Other rights should not automatically take priority in case of conflict; there is no fixed hierarchy.** A Gewirth, 'Are there any absolute rights?' in J Waldron, *Theories of Rights* (Oxford University Press 1981), 81-109; L Wenar, 'Rights' (Fall 2011) The Stanford Encyclopedia of Philosophy <http://plato.stanford.edu/archives/fall2011/entries/rights/> accessed 16 August 2015, paras 5.1-5.2.
[261] GDPR Parliament version, art 85a.

2.4.2 Conclusion

To summarize, the right to the protection of personal data became legally autonomous through the adoption of Article 8 of the Charter. The GDPR does not protect privacy in particular, but the right to data protection. Consequently, the formal ties between privacy and data protection are severed. As an autonomous right, the question arises what its object of protection is. Its most prominent conceptualisation hinges on its characterisation as permissive, while the case law of the CJEU indicates that data protection is prohibitive - although it is true that data protection provides for conditions under which an interference could be justified. The core of the right to the protection of personal data is Article 8(1), under which any processing of data constitutes an interference. This protects privacy as limited access, for which data minimization and data security are of special importance. However, the conditions of Article 8(2) and the GDPR specify a number of criteria which must be met for an interference to be justified - and they protect privacy as control and are ancillary to other rights and freedoms, as well as privacy. Data protection as a whole serves to protect a potentially boundless category of rights and freedoms. Nonetheless, it does not exhaust them: it is still possible that conduct which complies with data protection law violates other rights and freedoms. The apparently confused drafting of Article 33 is understandable in light of the overlap between (the right to) the protection of personal data, data security, privacy, and other rights and freedoms.

All three versions of the DPIA see to both the protection of personal data as contained in the GDPR and to the protection of rights and freedoms, including the right to the protection of personal data. At first sight, there are major differences. On the one hand, the Commission and Council versions requires an assessment of 'the impact (...) on the protection of personal data'.[262] They refer to compliance with data protection law. Indeed, the GDPR lays down rules for 'the protection of individuals with regard to the processing of personal data'.[263] As it is hard to imagine a rule being impacted, Article 33 would logically require an assessment of the compliance with these rules. On the other hand, the Parliament version requires an assessment of the impact on the rights and freedoms of data subjects, but especially of the impact on this right.[264] As a fundamental right, the right to the protection of personal data should be taken to require a respect which may exceed the obligations of the GDPR. While this right has not yet crystallized, the case law of the CJEU indicates that it principally protects privacy as limited access: it is violated if data is collected. However, if data is collected, this can be justified on the basis of a number of requirements which protect privacy as control and other rights and freedoms. The GDPR and the accompanying Commission Communication signify that Article 8 indeed entails privacy as control, and the emphasis on the rights and freedoms of individuals in the GDPR indicates that the right to the protection of personal data is also a procedural right intended to safeguard other rights and freedoms.

However, the contradiction between the Commission and the Council versions on the one hand and the Parliament version on the other dissipates. All three versions require the impact on the rights and freedoms of data subjects or individuals to be assessed.[265] 'Rights and freedoms' includes privacy and other rights and freedoms, such as non-discrimination, freedom of speech,

[262] GDPR Commission and Council version, art 33(1).
[263] GDPR, art 1(1).
[264] GDPR Parliament version, art 33(1).
[265] GDPR Parliament version, art 33(1); GDPR Commission and Council version; art 33(3).

and freedom of thought.[266] Discrimination, loss of reputation, financial damage and significant economic or social disadvantage are all considered risks to rights and freedoms.[267] As a result, the DPIA is not only about data subject rights, data breaches or privacy-intrusive operations.[268] This is in line with the objective of data protection law to protect fundamental rights and freedoms.[269] Under an interpretation of data protection as ancillary to other rights and freedoms, it does not surpass the competence of the EU to lay down rules relating to the protection of individuals with regard to the processing of personal data.[270] While Article 1(2) speaks of "fundamental" rights and freedoms, this adjective is not present in Article 33 – the category of rights and freedoms which need to be taken into consideration is therefore, without further clarification, boundless. It includes the right to the protection of personal data and the data subject rights in data protection law.

The requirement to assess the impact on rights and freedoms pushes the DPIA beyond a data protection or even a human rights compliance check. Firstly, as argued above, adherence to data protection law does not exclude that rights and freedoms may be violated. Secondly, both public and private controllers must analyse the impact on the rights and freedoms. Article 33 thus obliges non-governmental entities, who are not bound to respect the Charter, the ECHR, or the national constitution, to assess the harm they cause to human rights and fundamental rights.

While the Commission and the Parliament require an 'assessment of the risks to the rights and freedoms of data subjects',[271] the Council version speaks of an evaluation of 'high risk[s] for the rights and freedoms of individuals'.[272] The reference to individuals rather than data subjects serves as another clarification that "rights and freedoms" does not refer to the data subject rights of the GDPR, e.g. the right to obtain information, the right to erasure, and the right to object. They rather regard all rights and freedoms. It also brings within the ambit of the DPIA a concern for how the processing impacts people who are not represented in the dataset or whose data has been anonymized. However, the impact on people who may be included in the dataset at a later stage or who may become identifiable if further data is collected needs to be considered anyway – so the added value may be negligible. Meanwhile, the reference to the rights and freedoms of 'data subjects' or 'individuals' clearly excludes the interests of the controller from the scope of the evaluation. The Article 29 Working Party has emphasised that the legitimate interests of the controller are not relevant for the DPIA.[273] The DPIA is about how individuals or data subjects are affected, not about how the controller can best serve its own interests.

It follows from the above that the DPIA is a broad rights impact assessment. All three versions of the GDPR require the right to the protection of personal data and other rights and freedoms to be assessed. Are all three also a data protection compliance check? The requirements of data protection law are not the primary substance of the prohibitive Article 8, but if personal data is processed, they are important conditions to legitimise the interference. Moreover, concern for

[266] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', 4.
[267] GDPR Council version, art 33(1).
[268] See also GDPR Parliament version, rec 71a.
[269] GDPR, art 1(2); DPD, art 1(1); *Lindqvist*, para 97; Gellert and Gutwirth (2013) 529.
[270] TFEU, art 16. cf PIAF, 'A Privacy Impact Assessment Framework for data protection and privacy rights: Deliverable D1' (2011) 14.
[271] DGPR Commission version, art 33(3); GDPR Parliament version, art 33(3)(c).
[272] GDPR Council version, arts 33(3) and 33(1).
[273] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', 4.

the data subject rights is brought within the scope of the DPIA through the concern for the rights and freedoms of data subjects or individuals. Further, data security, as required by Article 30 GDPR, is an important aspect of the DPIA in all three versions.[274] The Parliament version also requires descriptions of compliance with a number of specific data protection requirements, which is discussed below.[275] As a result, DPIA is both a broad rights assessment and a compliance check.

	Commission	Parliament	Council
Subject matter			
	Impact on the protection of personal data - but also an assessment of the risks to the rights and freedoms of data subjects.	Impact on the rights and freedoms of the data subjects, especially their *right to* protection of personal data (which should include a compliance review) - but also an assessment of the risks to the rights and freedoms of data subjects.	Impact on the protection of personal data - but also an evaluation of the *high* risks to the rights and freedoms of *individuals.*

2.5 The outcome requirements

The impact assessment is a more elaborate version of the initial risk analysis. The steps which should be taken in the DPIA process are not described in the GDPR, but the ICO, the CNIL and Wright offer guidance. The process is discussed in section 2.7. This section discusses what the DPIA must contain at the end of this process, as the GDPR does prescribe several output requirements in Article 33(3). Next, it discusses whether the DPIA must lead to a certain level of protection. Lastly, the possible avenues for further guidelines are mentioned.

2.5.1 Required output

The DPIA consists of a description of the processing, a risk evaluation, and the identification or description of the of the mitigating measures. A description of the processing is necessary to identify and evaluate the risks, which is necessary to identify mitigating measures. The Commission and Council version reads as follows (formatting added to show changes made by the Council):

The assessment shall contain at least a general description of the envisaged processing operations, an evaluation of the risk referred to in paragraph 1 [a high risk for the rights and freedoms of individuals] ~~assessment of the risks to the rights and freedoms of data subjects~~, the measures envisaged to address the risks~~,~~ including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation~~,~~ taking into account the rights and legitimate interests of data subjects and other persons concerned.

It is not clear if the measures need to be identified, described, or possibly evaluated; the noun is missing. Assumedly, the least the controller has to do is identify the measures which should be taken to address the risks. The same elements are present in the Parliament version, which

[274] GDPR Commission and Council version, art 33(3); GDPR Parliament version, art 33(3)(e).
[275] Section 2.4.1.3.

divides them in subparagraphs and adds a number of other categories.[276] In the Parliament version, it is clear that the envisaged measures need to be described.

2.5.1.1 The risk assessment

The assessment or evaluation of the risks to the rights and freedoms of data subjects/individuals overlaps with the risk analysis which determines whether a DPIA must be carried out. While the initial analysis should determine whether specific or high risks are present, the DPIA entails that they are also assessed or evaluated. However, the distinction is not set in stone. To decide whether something qualifies as a specific or a high risk, which is a potential adverse effect of a certain likelihood and severity (damage condition), already entails an evaluation of the likelihood and the severity of the threat. The criteria for this assessment have been discussed in section 2.2.4. It will be repeated that processing may pose risks by virtue of its nature, scope and purposes.[277] Risks should be determined taking into consideration specific objective criteria, such as 'the nature of personal data (e.g. sensitive or not), the category of data subject (e.g. minor or not), the number of data subjects affected, and the purpose of the processing'.[278] After its identification, the risks must be assessed 'in terms of their origin, nature, likelihood and severity'.[279] They must be 'likely'.[280] These criteria overlap, as a result of which the identification and the assessment overlap. An exception is the Parliament version, under which the controller only needs to check whether the processing falls within the categories specified in Article 32a(2)(a)-(h).

During the assessment some kind of scoring will need to take place. Security-related factors generally lend themselves better to scoring on an ordinal or an interval scale and to a quantitative assessment. Non-security related risks, relating to the impact on fundamental rights of the way in which data is used, are more easily scored on a nominal scale and assessed qualitatively. This is, however, not "objective", as the Council would have it.[281] Qualitative assessments are more dependent on the quality of the subjective judgments made during the assessment.[282]

The assessment does not regard the legitimate interest of the controller. According to the Article 29 Working Party, the balancing act between the rights and interests of the controller and the data subject is to take place under the legitimate interest test, not as part of risk mitigation.[283]

2.5.1.2 The measures envisaged to address the risks

The type of remedy which may or must be taken to address a risk of which it is known (knowledge condition) that it has a certain effect (damage condition) had been called the "remedial condition".[284] For the DPIA, the remedy lies in the mitigating measures which must be identified. They see to address (high) risks to the rights and freedoms of data subjects/individuals. The measures should also ensure the protection of personal data and

[276] GDPR Commission and Council version, art 33(3); Parliament version arts 33(3)(a), (c), (d) and (e).
[277] GDPR Commission and Council version, art 33(1).
[278] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', 4.
[279] GDPR Council version, rec 60c.
[280] GDPR Parliament version, art 32a(1); GDPR Council version, art 33(1).
[281] GDPR Council version, rec 60b.
[282] Black and Baldwin (2010) 185.
[283] Article 29 Working Party 'Statement on the role of a risk-based approach in data protection legal frameworks', 4.
[284] Manson (2002) 265. cf Sandin (2004) 13-14.

demonstrate compliance which the GDPR, which includes the requirement to achieve a certain level of data security.[285] These safeguards and mechanisms must be drawn up 'taking into account the rights and legitimate interests of data subjects *and other persons concerned*'(emphasis added).[286] The DPIA contains the requirement to identify the measures, which makes controllers think about the risks and how to address them. The Parliament makes explicit that the mitigating measures must be described.[287] In sum, the DPIA serves to identify and possibly describe measures which mitigate risks to the rights of individuals and which ensure and demonstrate compliance.

The different versions display differences in formulation. It is difficult to make something of these differences. For the Council, the description of the measures envisaged to address the risks to the rights and freedoms *includes* 'safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation'.[288] The Commission remains ambiguous in this regard.[289] The Parliament version requires the DPIA to contain a separate list of these 'safeguards, security measures and mechanisms'.[290] This implies that risk mitigation and the protection of personal data are seen as different objectives; perhaps risk mitigation should go beyond personal data protection (see also section 2.5.2.2). Similarly, the requirement that the safeguards, security measures and mechanisms must be drawn up taking into account the rights and legitimate interests of data subjects and other persons concerned,[291] is not situated the same in the three versions. In the Commission version it is ambiguous whether this requirement sees to the 'safeguards, security measures and mechanisms' or also to the measures taken to address the risks. The Parliament only links it to the former. Taken literally, this would imply that the interests of individuals which are not data subjects only need to be taken into account in relation to the measures taken 'to ensure the protection of personal data and to demonstrate compliance with this Regulation', and not with regard to the measures which, by addressing the risks to the rights and freedoms, go further than ensuring and demonstrating compliance with the requirements of data protection law. In the Council version the concern for other stakeholders was already mandatory, as it requires an assessment of the impact on "individuals" rather than "data subjects". However, these differences appear to be the result of the Commission's poor drafting and of the Parliament's choice to formulate the required elements in a list, and should, therefore, not be accorded too much weight.

2.5.1.3 Other requirements in the Parliament version

The Parliament version requires a number of elements in addition to the description of the project, the risk evaluation, and the mitigating measures. It also requires a description of the purposes of the processing and, if applicable, the legitimate interest of the controller, a list of the recipients of the data and intended data transfers, and an indication of the time limits for erasure of the different categories of data.[292] In the Commission and the Council version this information should be documented by virtue of Article 28, which contains the obligation to keep

[285] GDPR, art 30.
[286] GDPR Commission and Council version, art 33(3); GDPR Parliament version, 33(3)(e).
[287] GDPR Parliament version, art 33(3)(d).
[288] GDPR Council version, art 33(3).
[289] GDPR Commission version, art 33(3).
[290] GDPR Parliament version, art 33(3)(e).
[291] GDPR Commission and Council version, art 33(3); GDPR Parliament version, art 33(3)(e).
[292] GDPR Parliament version, arts 33(3)(a), (f), (h) and (i).

records. The Parliament further adds the requirement to describe the measures envisaged to minimise the volume of data which is processed and to explain the data protection by design and by default practices which have been implemented.[293] Therefore, the documentation of compliance with the data minimisation principle and with privacy by design and by default has been grouped with the DPIA requirement.

In the Parliament version, the DPIA does not only contain an assessment of the risks for the rights and freedoms, but also of the necessity and proportionality of the processing operations and the context of the processing.[294] These assessments must be documented, subjected to a compliance review, and made available, on request, to the supervisory authority.[295] The obligation to assess the necessity and proportionality is not new. It is already present in the requirements to process only what is 'adequate, relevant and limited to the minimum necessary' in relation to the purpose of the data processing operation and to the lawfulness of the processing (the processing must be necessary for X).[296] Proportionality is also an overarching principle which controllers must comply with.[297] The Dutch *Hoge Raad* goes so far as ruling that a construction of data protection law in line with Article 8 ECHR requires any processing operation to be proportionate to the aim of the processing, requiring a balancing act between the interests of the data subjects and the purpose of the processing.[298] The context may need to be assessed to ascertain if the processing takes place in the employment context,[299] the social security context,[300] or in relation to the accountability principle.[301] The requirement to document the assessment in the DPIA can thus be seen as a requirement to document assessments which need to be performed to achieve compliance.

In conclusion, all these added elements relate to other data protection requirements, indicating that the Parliament's DPIA serves to describe and document compliance. Article 33(3b) explicitly adds that the DPIA must be documented. While this is commonly assumed in the literature on the privacy impact assessment,[302] and is also necessary to communicate the results to the DPIA, as is or may be required,[303] the other versions of the GDPR do not specify it. These additional descriptions may serve to present a more complete picture in one report to the benefit of the controller itself, the data protection officer, and the supervisory authority. The controller is enabled to improve its compliance, and the data protection officer and the supervisory authority are better able to assess it.

---

293 GDPR Parliament version, art 33(3)(b) and (g).
294 GDPR Parliament version, art 33(3)(b) and (j).
295 GDPR Parliament version, art 33(3b).
296 GDPR, arts 5(b) and (c) and art 6(1)(b)-(f) and (2); Article 29 Working Party, 'Opinion 26/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (WP217, 2014), 10 and 41; C Tranberg, 'Proportionality and data protection in the case law of the European Court of Justice' (2011) 1(4) International Data Privacy Law 239, 239; E Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer 2013) 418-426.
297 Article 29 Working Party, 'Opinion 26/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', 10 and 41; Tranberg (2011), 239; Kindt (2013), 418-426.
298 Hoge Raad 9 September 2011 ECLI:NL:HR:2011:BQ8097 para 3.3.
299 GDPR, art 82.
300 GDPR Parliament version, art 82a.
301 GDPR Parliament version, art 22.
302 e.g. D Wright, 'Should privacy impact assessments be mandatory?' (2011) 54(8) Communications of the ACM 121, 123; D Wright and P De Hert, 'Findings and Recommendations' in D Wright and P De Hert (eds), *Privacy Impact Assessment* (Springer 2012) 476.
303 GDPR, art 34(6).

2.5.2 Should the DPIA lead to a certain level of protection?

This section discusses whether controllers need to take measures to achieve a certain level of rights protection. The idea of the risk-based approach is that additional measures need to be taken when specific or high risks are identified. The Article 29 Working Party mentions as examples the DPIA, enhanced security and the data breach notification.[304] However, Article 33 does not contain comprehensive standards on the level of protection which should be reached through the risk evaluation and the identification and adoption of mitigating measures. Under the Commission and the Council version, there is not even a duty to implement the envisaged measures of protection. In the following, the requirements and standards which do exist are discussed. These are data protection requirements which concern the level of riskiness of the processing, requirements concerning the risk assessment of the DPIA, including the stakeholder consultation, and the Parliament's compliance review. Next, the possible construction of a general duty of risk mitigation is considered.

2.5.2.1 Standards which are related to risk mitigation

Data protection requirements

Insofar as the DPIA concerns compliance with other data protection requirements, these external requirements form legal standards for the level of protection which must be achieved. They also pose a legal duty to actually achieve this level of protection. In other words, if the envisaged measures are necessary to achieve compliance, then they must be taken by virtue of the corresponding requirement of data protection. For example, if the controller wishes to rely on its legitimate interest as a legal ground, the processing cannot be so risky as to disrupt the balance between its legitimate interest and the impact on the interests and rights on the data subject.[305] There are guidelines on the balance and the factors which play a role.[306] Furthermore, if the controller intends to process previously collected data for a new purpose, a substantive compatibility assessment needs to be conducted, which includes the impact of the further processing on data subjects and the safeguards adopted by the controller to prevent any undue impact.[307] The principle of purpose limitation thus contains requirements to ensure that further processing is, considering its context, not too risky. Moreover, Article 30 requires the controller and the processor to take appropriate technical and organisational measures to ensure a certain level of security, which is linked to the risks presented by the processing.[308] Pseudonymization is given as an example of such a security measure.[309] The measures should protect against unauthorized disclosure and accidental or unlawful destruction, loss or alteration.[310] In the Commission version, emphasis is on the prevention of unlawful forms of processing.[311] The Parliament rather requires controllers to come up with and implement a 'security policy'.[312]

---

[304] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', 4.
[305] Article 29 Working Party, 'Opinion 06/2014 on the Notion of the legitimate interest of the data controller under art 7 of Directive 95/46/EC', 30-31.
[306] Article 29 Working Party, 'Opinion 06/2014 on the Notion of the legitimate interest of the data controller under art 7 of Directive 95/46/EC', 33-43.
[307] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (WP203, 2013) 25-27.
[308] GDPR, rec 66 and art 30(1).
[309] GDPR Council version, art 30(1).
[310] GDPR, art 30(2).
[311] GDPR Commission version, art 30(2).
[312] GDPR Parliament version, arts 30(1a) and (2).

The fact that controllers have to take appropriate measures to comply with the requirements of the GDPR is reiterated in Article 22, which also requires controllers to be able to *demonstrate* their compliance.[313]

Requirements on the permitted impact or riskiness of the processing can also be found in the nationally developed requirements that the processing is fair,[314] or the requirement that all processing must be proportionate to its purpose by virtue of Article 8 ECHR.[315] Proportionality is further discussed below, as is privacy by design and by default.

Requirements for the risk assessment, including stakeholder consultation

Outside of the principles of data protection – none of which are one and the same as the mitigation of risks to rights and freedoms – there are no legal standards regarding the level of protection which should be reached. To assess the risks properly it needs to be decided 1) when a threat is severe enough and likely enough to constitute a (high) risk; 2) how much knowledge is necessary for the risk to be assigned a certain severity and likelihood; and 3) what remedy is necessary. As stated above, these norms have been called the damage condition, the knowledge condition and the remedial condition.[316] At what point the threat is bad enough and when the remedy is sufficient depends on the level of protection which is strived for.[317] The amount of certainty which is required as to the probability of the threat relates rather to the extent to which precaution is considered suitable.[318] The GDPR indicates what type of threats may qualify: potential adverse effects to the rights and freedoms of data subjects/individuals. This includes the right to the protection of personal data and data subject rights.[319] It was argued under section 2.2.4 that any processing which falls within the scope of the right, thereby interfering with it, is *eligible* to constitute a severe enough threat to the rights and freedoms. As discussed under sections 2.2.4 and 2.5.1.1 concerning the risk threshold and the risk assessment, the GDPR and the Article 29 Working Party provide criteria on the basis of which the risks can be identified and assessed. The criteria indicate that more than a potential interference required, but do not specify when a threat is probable and severe enough. They are methodological requirements: they specify how the risk should be assessed, and not what level of protection should be aimed for. Even less indication is given on the knowledge condition, which remains fully unsubstantiated. Moreover, the remedy is not clarified. Should the measures eliminate the risks, minimise them, or mitigate them? What level of residual riskiness is acceptable? As the GDPR does not provide guidance, the controller is apparently expected to set these norm during the risk assessment.[320]

The stakeholder consultation could help the controller set these norms. In the Commission version and the Council version, the controller must 'seek the views of data subjects or their

---

313 GDPR, art 22(1).
314 Information Commissioner's Office (ICO), 'The Guide to Data Protection' (version 2.2.4, 31 March 2015) <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/> accessed 25 August 2015, 16.
315 Hoge Raad 9 September 2011, ECLI:NL:HR:2011:BQ8097, para 3.3.
316 Manson (2002) 262. cf Sandin (2004) 13-14.
317 cf von Schomberg (2006) 25.
318 See section 2.2.3.
319 See section 2.4.2.
320 **The norms can be evaluated and rephrased by and with the supervisory authority during the prior consultation (but they only get this chance if the norms have been applied in a manner which results in a DPIA that points to high risks, see section 2.6.1.2) or during other regulatory conversations.**

representatives on the intended processing'.[321] Also in the body of literature on privacy impact assessments, some stress that the impacts should be assessed in consultation with stakeholders, or following a public consultation. Wright and others argue that this can aid in understanding the perspectives of the stakeholders and the risks they perceive. The information which stakeholders bring to the table helps to identify and assess risks.[322] They may be able to anticipate emerging rights issues (threats) which the developer did not spot[323] and assess collectively whether the threat should be regarded as severe and probable. [324] Because assessing risks is a somewhat subjective exercise, the views of stakeholders and experts matter.[325] They can also help set the level of protection, which determines what counts as a risk and what the remedies should strive for. In the absence of legal standards, the level of protection which is aimed for is an ethical or political decision.[326] Stakeholders can help decide 'what type of information society is desirable, and what values constitute that society'.[327] This ties in to the uncertainty which shrouds even "known" risks. The legislator cannot foresee and address everything. The DPIA is a solution to this problem which, however, is perceived as suffering from a legitimacy deficit. Stakeholder engagement is seen as responding to this democratic necessity: 'if the consequences of new technological developments – which were not yet visible at the moment of the elections – are uncertain, the taking of action and of risks is a question of collective decision-making, and thus becomes a political issue'.[328] The requirement to consult data subjects in the GDPR is, however, 'without prejudice to the protection of commercial or public interests or the security of the processing operations'.[329] Therefore, the obligation to consult stakeholders is not a hard one. It will probably be cast aside frequently, as stakeholder consultations can be very expensive and may conflict with the desire of product developers to keep their projects secret.[330] Moreover, there is no duty to align to the views of the data subjects. As a result, the stakeholder consultation is purely methodological. It can help in reaching a proper level of risk mitigation, but it does not provide any real safeguards as to the level of protection which should be reached.

The compliance review

The Parliament version contains the compliance review of Article 33a, which requires controllers to review whether they adhere to the promises they make in the DPIA every two years. This is not, however, a duty to actually mitigate risks; it is a duty to *demonstrate* that the measures described in the DPIA are undertaken.[331] 'This compliance review shall demonstrate that the processing of personal data is performed in compliance with the data protection impact

[321] GDPR Commission and Council version, art 33(4).
[322] Wright (2011) 127; Wright, Gellert, Gutwirth and Friedewald (2011) 96; P De Hert, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments', in D Wright and P De Hert (eds), Privacy Impact Assessment (Springer 2012) 75; R Finn, R Rodrigues and D Wright, 'A Comparative Analysis of Privacy Impact Assessment in Six Countries', (2013) 9(1) Journal of Contemporary European Research 161, 162-163; PRESCIENT (2013) 74.
[323] Wright, Gellert, Gutwirth and Friedewald (2011) 95.
[324] cf Wright, Gellert, Gutwirth and Friedewald (2011) 88. See section 2.2.3.
[325] PRESCIENT (2013) 95.
[326] PRESCIENT (2013) 95.
[327] PRESCIENT (2013) 73.
[328] Wright, Gellert, Gutwirth and Friedewald (2011) 96. **However, consensus or compromise is not necessarily the best way to make ethical decisions under a pluralist or relativist view on ethics** (cf PRESCIENT 2013 85).
[329] GDPR Commission and Council version, art 33(4).
[330]Wright, Gellert, Gutwirth and Friedewald (2011) 97.
[331] GDPR Parliament version, rec 74a and art 33a(1).

assessment'.[332] In other words, it does not matter if the measures are ineffective, as long as they are the measures which were envisaged in the DPIA. This is because Article 33 does require the controller to come up with measures to address the risks, but it does not specify a certain level of protection which must be reached. The idea of the construction of Articles 33 and 33a is not to specify such a standard by law but to have the controller determine the level of protection as part of the DPIA and to monitor its own compliance. The data protection officer is relied on to specify a proper level of protection and to keep an eye on its realization.[333] If there is a change in the specific risks presented by the processing operations, then a new compliance review needs to be carried out.[334] This is apparently with the aim to check whether the measures are still sufficient to reach the identified level of protection. If there are 'compliance inconsistencies', then the review shall include recommendations on how to achieve full compliance with the DPIA and the impact assessment shall be updated.[335] The compliance review not only demonstrates compliance with the DPIA, but also with 'the autonomous choices of data subjects'.[336] This presumably regards data subject rights. The compliance review is, of course, documented and available to the supervisory authority upon request.[337]

2.5.2.2 The construction of a duty to address risks

It is up to the controller to determine the level of protection and to decide whether or not to actually take the measures to achieve this level of rights protection. This is because risk mitigation is not an explicit, independent duty under the GDPR. If there is no legal requirement to mitigate risks, then where does a comprehensive set of standards on the level of protection which is required come from? The stakeholder consultation has not been included in the GDPR as an adequate replacement. Perhaps it is a result of compromises during the drafting of the GDPR that there is no explicit duty to address risks to the rights and freedoms of individuals in the field of data protection. This duty is implied, but not carried, by the requirement to assess the risks to the rights and freedoms of individuals of Article 33 and to describe which measures will be taken to address these risks.[338] The fact that these measures must be described would logically be accompanied by a requirement to actually take them, and to do so in conformity with some quality standard. The construction of such a duty would also be line with the objective of data protection law to protect fundamental rights and freedoms (and in particular the right to the protection of personal data, which may, in turn, exist to serve other rights and principles).[339]

Data protection law contains three avenues which logically lend themselves to the construction of a general duty to address risks to the rights and freedoms of individuals: privacy by design and by default, the principle of proportionality, and the principle of fairness. The right to the protection of personal data could be interpreted as ancillary to other rights and freedoms, but it would be farfetched to construe Article 8 of the Charter as a correlating duty of governmental and non-governmental controllers to address risks to these other rights and freedoms. Under the prohibitive conceptualisation, the rights and freedoms are protected only as part of the

[332] GDPR Parliament version, arts 33a(1) and (2).
[333] GDPR Parliament version, arts 33(3a) and art 33a(5).
[334] GDPR Parliament version, arts 33a(2).
[335] GDPR Parliament version, arts 33(3b) and 33a(3).
[336] GDPR Parliament version, rec 74a.
[337] GDPR Parliament version, art 33a(4).
[338] GDPR, art 33(3) GDPR.
[339] GDPR, art 1(2).

conditions which must be met for the interference to be justified. In other words, the primary duty of Article 8 is to not collect data. Moreover, it only applies to Member States.[340]

Privacy by design and by default

A duty to mitigate risks to the rights and freedoms of individuals can be based on privacy by design and by default. This is laid down in Article 23 GDPR and requires controllers to implement technical and organisational measures to ensure compliance with the GDPR and to protect the rights of the data subject.[341] In the body of literature concerning the privacy impact assessment, some authors view the impact assessment as a way of mitigating (organizational and/or technical) risks during the development or procurement phase, as is required by Privacy by Design.[342] Others slightly rephrase it as a method for managing Privacy by Design,[343] or even as providing input for accountability by design.[344] This implies that the actual level of risk mitigation achieved is a matter of privacy by design and by default. The question is whether Article 23(1) GDPR requires the (fundamental) rights and freedoms of data subjects to be protected, or whether it only sees to data subject rights, such as the right to information. It appears to see only to the requirements of data protection. The Parliament specifies that the measures particularly see to the principles laid out in Article 5.[345] The Council states that controllers, taking into account the risks for rights and freedoms of individuals, should implement measures such as data minimisation and pseudonymization so that the processing will be compliant with the GDPR, and protect the rights of data subjects.[346] Their rights can be protected trough measures which implement 'transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features'.[347] This is to make sure that 'controllers and processors are able to fulfil their data protection obligations'.[348] In this reading, Article 23 is not a requirement to protect the rights and freedoms of individuals.

To the contrary, the CNIL appears to see risk mitigation as part of data protection compliance on the basis of Privacy by Design as codified in Article 34 of the French Data Protection Act. The French data protection authority makes a distinction between the fundamental principles and rights of data protection law, which cannot be modulated, and risk management, which serves to determine the adequate technical and organizational controls to protect personal data.[349] Both

---

340 Charter, art 51(1). cf below in this section, under 'The principle of proportionality'.
341 GDPR, art 23(1).
342 M Pocs, 'Will the European Commission be able to standardise legal technology design without a legal method?' (2012) 28(6) Computer Law & Security Review 641, 644-645; S Spiekermann, 'The RFD PIA - Developed by Industry, Agreed by Regulators', in D Wright and P De Hert (eds), *Privacy Impact Assessment* (Springer 2012) 323-324; M C Oetzel and S Spiekermann, 'A systematic methodology for privacy impact assessments: a design science approach'(2014) 23 European Journal of Information Systems 126, 126.
343 S Davies, 'Why Privacy by Design is the next crucial step for privacy protection' (2010) <www.i-comp.org/wp-content/uploads/2013/07/**privacy-by-design**.pdf> accessed 11 September 2015, 2-3.
344 D Butin, M Chicote and D Le Métayer, 'Strong Accountability: Beyond Vague Promises', in S Gutwirth, R Leenes and P De Hert, *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014) 367.
345 GDPR Parliament version, art 23(1). **However, it had earlier advocated that privacy by design and by default should protect 'individual's right to privacy and data protection'.** European Parliament, 'Personal data protection in the European Union: European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union' P7_TA(2011)0323, para 35.
346 GDPR Council version, art 23(1).
347 GDPR Council version, rec 61.
348 GDPR Council version, rec 61.
349 CNIL (2015) 7.

respect for the principles of data protection and risk mitigation are seen as part of compliance. The impact assessment helps controllers to demonstrate their compliance and to show that their products do not breach privacy because they incorporate privacy by design - whereby privacy is interpreted as encompassing all rights and freedoms.[350] However, risk mitigation only relates to illegitimate access, unwanted alteration and disappearance of personal data.[351] Other causes of potential harm, such as how the data is used -for example the impact on privacy and the freedom of thought of personalised advertising - are not taken into consideration. The CNIL thus sees the impact assessment as a way to demonstrate compliance and to demonstrate privacy by design, whereby the former requires respect for fundamental principles of data protection and the latter requires *certain* risks to the rights and freedoms to be managed. This is illustrated by the CNIL's figure below.

Figure 3 – Compliance approach using a PIA

[352]

The ICO sees the impact assessment as a part of privacy by design.[353] However, privacy by design is currently not considered mandatory; it is only one way to establish compliance at an early stage of the project.[354] It is also considered a tool to minimise privacy risks and build trust.[355] It is therefore fitting that the privacy impact assessment is a non-mandatory way to establish and demonstrate compliance, [356] also with the ECHR's right to privacy, if applicable.[357] The purpose of the impact assessment is 'to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible'.[358] The outcome of a privacy impact assessment should be the minimisation of privacy risk.[359] 'A project which has been subject to a PIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way'.[360] Contrary to the CNIL, though, the ICO does not assume a legal duty to mitigate risks.

The principle of proportionality

Another candidate to base a duty of risk mitigation on is proportionality. If all processing operations which interfere with a right or freedom must be proportionate, then any unnecessary interferences must be avoided; in other words, the risks must be mitigated. This would limit the concept of "risk" to interferences with fundamental rights. According to Gutwirth and Gellert, the

[350] CNIL (2015) 3-4.
[351] CNIL (2015) 14.
[352] CNIL (2015) 7.
[353] Information Commissioner's Office (ICO), 'Conducting privacy impact assessments: code of practice' (2014) < https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/> accessed 15 August 2015, 1.
[354] ICO (2015) 128.
[355] ICO (2015) 128.
[356] ICO (2014) 4 and 8.
[357] ICO (2014) 8.
[358] ICO (2014) 5.
[359] ICO (2014) 7.
[360] ICO (2014) 8.

proportionality test could take this extensive form only under an ancillary interpretation of data protection. If data protection is conceptualised as an instrument to protect other human rights, then any interference with these rights must be proportionate.[361] Under an autonomous interpretation, data protection already strikes the right balance, as a result of which the proportionality test is wholly captured in the principles of purpose limitation and data minimization. Gellert and Gutwirth note that the GDPR appears to advance an autonomous interpretation.[362] However, it is not at all decided whether the GDPR – even under an autonomous interpretation - will exhaustively provide the right balance between the various rights involved. As argued at the end of section 2.4.1.4, compliance with the GDPR does not equal respect for fundamental rights. As a result, the principle of proportionality applies in its extensive form and could, thus, function as a principle of risk mitigation. However, the duty to interpret data protection law in a manner which is proportionate to other rights and freedoms may not fully extend to non-governmental entities. They are not the norm addressees of the Charter[363] and are therefore not bound by the extensive form of the principle of proportionality, which emanates from the duty to respect Article 8 and 52 of the Charter. Fundamental rights can have indirect horizontal effect: government agencies, including the court, can be obliged to restrict the actions of one civilian against another in order to protect its fundamental rights. Technically, however, the norm addressee is still the government.[364] National courts can assign direct horizontal effect to rights, but this is not required by international documents such as the Charter.[365] As discussed under section 2.6.1.2, the principled approach argues, in short, that citizens or at least companies which endorsed corporate social responsibility (CSR) should interpret the law in line with its spirit. This might oblige (CSR) non-governmental entities to interpret the GDPR in a manner which reconciles the applicable rights and interests in a proportionate manner. However, this is only a moral duty, and if it were a legal duty its enforceability would be severely limited.

The principle of fairness

Article 5(1)(a) requires that personal data is processed lawfully, fairly, and in a transparent manner. The principle of fair processing could be used to construct a duty to mitigate risks. It is so devoid of meaning at the European level that it could theoretically be developed to encompass almost anything. Under English law, fairness generally requires controllers to be clear to individuals on how their information is used,[366] but according to the ICO it can also require them not to 'use the data in ways that have unjustified adverse effects on the individuals concerned'.[367] Under Dutch law, fairness requires adherence to due care.[368] The term due care ("*zorgvuldigheid"*) was chosen to connect to the due care which tort law requires and the due care which is present as a principle of good administration.[369] The requirements of data protection are, in general, characterised as substantiating what the public sector ought to do in accordance with the principles of good administration ("*algemene beginselen van behoorlijk bestuur*") and what is required of private parties under the due care ("*maatschappelijke*

361 Gellert and Gutwirth (2013) 529.
362 Gellert and Gutwirth (2013) 529.
363 Charter, art 51(1).
364 *X and Y v. The Netherlands*, A. 8978/80, 26 March 1985.
365 A Nollkaemper, *Kern van het internationaal publiekrecht* (Boom 2009) 269-270.
366 Data Protection Act 1998, sch 1(1); *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47.
367 ICO (2015) 16-17.
368 Wet bescherming persoonsgegevens, art 6.
369 *Kamerstukken II* 1997-1998, 25892, nr. 3, 77.

zorgvuldigheid") which they owe each other.[370] Fairness is thus the overarching principle of data protection law. It relates to transparency,[371] but also to, for example, a lack of safeguards on the circulation of sensitive data between government agencies.[372] Member States have developed fairness in a manner which connects to their own legal order. Clearly, fairness has little meaning at the European level. This is also why it is not as suitable as privacy by design, which only needs to be slightly reinterpreted to bring to life a duty to mitigate risks. It would be a much larger leap to use fairness for such a construction, and it would fill in a principle which can otherwise be used as a catch-all safety net.

Differences between the Parliament, the Commission and the Council version

The GDPR thus provides openings for the construction of a duty to mitigate risks which applies to all controllers. Although none of the versions of the GDPR reject such a construction, it would be more in line with the Parliament version than with the Council version. While the Council version mentions compliance and risk mitigation as separate goals of the DPIA, the Parliament version appears to see risk mitigation as part of compliance. The Parliament, and less frequently the Commission, present risk mitigation as part of compliance with the GDPR. Article 34(2) of the Commission and Parliament version refers to risk mitigation as part of compliance: the aim of the prior consultation is to establish compliance, and in particular to mitigate risks for data subjects.[373] Moreover, Recital 71a of the Parliament version does not find it necessary to mention separately the goal of risk mitigation, nor that of demonstrating compliance, which is already required by Article 22 GDPR. It states that the DPIA requires a description of 'the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure compliance with the regulation' – implying that not only the obligation to demonstrate compliance but also mitigation of the risks to the rights and freedoms of data subjects is part of compliance with the requirements of data protection law. In other words, the GDPR is presented by the Parliament as containing a duty to address risks. The Council version, to the contrary, makes explicit that the measures are for ensuring data protection and demonstrating compliance, and also for mitigating the risks to the rights and freedoms of individuals.[374] The lawfulness of the processing and the impact of the processing are mentioned as separate things.[375] The Council thus presents compliance and risk mitigation as separate goals. It may be for this reason that the Council removed the statement that the aim of the prior consultation is compliance, and in particular risk mitigation.[376] This presented risk mitigation as part of compliance, and was therefore not in line with the Council's view. While the construction of a duty to mitigate risks through guidance and case law is not precluded, it would be less in line with the intentions of the legislator.

---

370 *Kamerstukken II* 1997-1998, 25892, nr. 3, 14-15.
371 *Kamerstukken II* 1997-1998, 25892, nr. 3, 149.
372 ABRvS 4 July 2007, ECLI:NL:RVS:2007:BA8742, mt. nt. G Overkleeft-Verburg.
373 GDPR Commission and Parliament version, art 34(2). **The Commission indicates that the measures are to effectuate compliance with the GDPR in a manner which respects the rights and freedoms of individuals, but does not specify the relationship between the GDPR and risk mitigation. According to Article 33(3) the measures are to 'ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned'.**
374 GDPR Council version, rec 70a and arts 33(3) and (3a).
375 GDPR Council version, art 33 (3a).
376 GDPR Council version, art 34(2); GDPR Commission and Parliament version, art 34(2). See also GDPR Commission and Parliament version, art 34(6).

2.5.3 Further guidance

The supervisory authorities are called upon to provide guidance on the DPIA, as the CNIL and the ICO have done.[377] They will have the power to give opinions on any issue related to the protection of personal data.[378] The European Data Protection Board will issue guidelines, recommendations and best practices for the supervisory authorities. This has the aim of encouraging a consistent application of the GDPR.[379] More harmonized guidance is provided for in the Commission version. In the Commission version, the Commission is empowered to adopt both delegated acts and implementing acts to further specify the requirements for the assessment and standards and procedures for carrying out the DPIA.[380] All these entities might make use of their possibility to provide guidance to specify whether is it required to actually implement the measures and to reach a certain level of protection. These decisions have to be made to fill in Article 33 and Article 23, so they would not be ultra vires; to construct a very extensive duty to mitigate risks, on the other hand, would be stretching the mandate.

The Commission is especially asked to consider conditions for scalability in Article 33(6), which also requires the Commission to consider specific measures for micro, small and medium-sized enterprises.[381] It has been critiqued that SME's may lack the financial means to conduct a proper DPIA.[382] In the absence of such delegated acts – which the Parliament and the Council version do not allow - there are no clear-cut derogations from the obligation to conduct a DPIA for SME's. Nonetheless, data protection law is scalable because regard must be had to the nature and scope of the processing.[383] Delegated and implementing acts can also specify the conditions for the verification and auditability of the assessment, and standards and procedures for verifying and auditing the DPIA.[384] In the literature on privacy impact assessments, many authors argue that the PIA should be subject to follow-up, like a third-party review or audit,[385] or oversight, like through a certification system.[386] The Parliament wants the controller's ability to ensure and be able to demonstrate compliance with the GDPR to be verified by independent internal or external auditors.[387] Accountants could fulfill this function. Further, the GDPR requires an audit of sorts through the prior consultation requirement, which will be discussed in the next section. It also contains the possibility of certification in Article 39.

2.5.4 Conclusion

The GDPR specifies in Article 33(3) what the DPIA must contain. All three versions require it to describe the envisaged processing operation, conduct a risk assessment/evaluation, and identify or describe mitigating measures. The risk assessment overlaps with the initial risk analysis,

---

377 Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' 4.
378 GDPR Commission and Parliament version, art 53(1)(i); GDPR Council version, art 53(1c)(aa).
379 GDPR, art 66(1)(b).
380 GDPR Commission version, art 33(6) and (7).
381 GDPR Commission version, art 33(6).
382 De Hert and Papakonstantinou (2012) 41; PIAF, 'Deliverable D3: Recommendations for a Privacy Impact Assessment Framework for the European Union' (2012) 13.
383 Article 29 Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks' 3.
384 GDPR Commission version, arts 33(6) and (7).
385 Wright (2011) 129; Finn, Rodrigues and Wright (2013) 164; K Wadhwa and R Rodrigues, 'Evaluating privacy impact assessments' (2013) 26 Innovation: The European Journal of Social Science Research 161, 163.
386 R Weber, 'Symposium on EU Data Protection Reform: Privacy management practices in the proposed EU regulation' (2014) 4(4) International Data Privacy Law 290, 296.
387 GDPR Parliament version, rec 60.

discussed in section 2.2, which serves to determine whether specific or high risks are present. An exception is the Parliament version, because the threshold analysis only requires the controller to assess whether the processing falls within the described categories. The criteria which are discussed there, also apply here; one addition is that the legitimate interests of the controller do not play a role in the risk evaluation. The measures specify the remedial condition: the type of remedy which may or must be taken to address a risk of which it is known (knowledge condition) that it has a certain effect (damage condition). The measures are to address risks to the rights and freedoms of individuals and (Council: 'including') 'to ensure the protection of personal data and to demonstrate compliance with this Regulation'.[388] The safeguards and mechanisms must be drawn up 'taking into account the rights and legitimate interests of data subjects and other persons concerned'.[389] As a result, the DPIA helps controllers identify measures to mitigate risks to the rights of individuals and to ensure and demonstrate compliance. The Parliament emphases that these measures must be described and that the DPIA must be documented and made available to the supervisory authority, on request.[390]

The Parliament version requires the DPIA to describe a number of additional elements, which all see to other data protection requirements. For example, the purpose of the processing and the measures envisaged to implement data protection by design and by default need to be described. Not only the risks for the rights and freedoms need to be assessed, but also the necessity and proportionality of the processing operations and the context of the processing. This is also necessary for other principles of data protection law. Therefore, these additions serve to describe and document compliance. This may assist the controller, the data protection officer and the supervisory authority in determining whether the processing will be compliant with the GDPR.

Although the DPIA requires controllers to assess the risks and identify mitigating measures, the GDPR does not set comprehensive standards regarding the level of protection and precaution which must be reached through the risk evaluation and the adoption of mitigating measures. Insofar as the risk mitigation is necessary for one of the data protection requirements, this requirement provides the level of protection which should be reached and the obligation to actually implement measures to achieve this level of protection. However, insofar as the risk evaluation and mitigation surpass the rest of the GDPR there are no standards as to the level of protection and precaution which should be achieved through the implementation of mitigating measures. There are criteria on the basis of which the risks can be identified of assessed, but they do not specify when a threat counts as a risk and whether the remedies should eliminate the risk, minimise it, or mitigate it. A stakeholder assessment can help controllers identify and assess risks and set the level of protection. However, the obligation to consult data subjects and to take into account their views is not hard and it is even absent in the Parliament version. As a result, the controller is left to set the norms itself; to identify itself what type of information society is desirable and to perform the DPIA on the basis of this image. Moreover, in the Commission and the Council version there is no obligation to take the measures which are identified in the DPIA, as in the Parliament's compliance review. Even in the Parliament version, the lack of standards on the level of protection means that there is no clear duty to implement adequate risk mitigation measures.

[388] GDPR Commission and Council version, art 33(3); GDPR Parliament version, art 33(3(e).
[389] GDPR Commission and Council version, GDPR Parliament version, art 33(3); 33(3)(e).
[390] GDPR Parliament version, art 33(3b).

If the GDPR would contain a duty to mitigate risks, this would be the source of the level of protection which is strived for and the obligation to take measures to reach this level of protection. As it currently stands, the GDPR does *not* contain the duty to address risks to the rights and freedoms of individuals in actuality - it is only present in potential. Although the different versions of the GDPR do not contain an explicit duty to address such risks, this duty is implied by Article 33 and 34 and can be based on privacy by design and by default, the principle of fair processing or, particularly with regard to non-governmental entities, on the principle of proportionality. Such a duty would be commensurate with all three versions and is even implied by the Parliament. Data protection law may thus be interpreted and developed by national legislatures and courts as containing a duty to address the risks to the rights and freedoms of individuals.

Meanwhile, guidance can be provided by supervisory authorities, the European Data Protection Board and, if it is empowered to adopt delegated and implementing acts, the Commission. They may be able to clarify whether controllers are required to aim for or achieve a certain level of protection and what this level may be. Other topics which could be addressed are scalability and the verification and auditing of the DPIA. The Commission is especially asked to provide guidance relating to these topics.

	Commission	**Parliament**	**Council**
Required output			
	A description of the processing, an assessment of the risks, and the *identification/description(?)* of measures envisaged to address the risks, *and/including(?)* safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.	A description of the processing, an assessment of the risks, a *description* of measures envisaged to address the risks, *and* a list of safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR + a large number of other descriptions and assessments which relate to other data protection requirements (see Article 33(3).	A description of the processing, an assessment of the risks, and the *identification/description(?)* of measures envisaged to address the risks, *including* safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.
Are there legal standards on the level of protection and precaution which must be aimed for (e.g. when does something count as risky, when is a risk known, when are remedies sufficient)?	No. There are only methodological requirements on how to assess riskiness and a soft duty to seek the views of data subjects or their representatives.	No. There are only methodological requirements on how to assess riskiness.	No. There are only methodological requirements on how to assess riskiness and a soft duty to seek the views of data subjects or their representatives.
Is there a duty to take the envisaged mitigating measures?	No.	Yes. The controller has to carry out a compliance review and demonstrate that the measures described in the DPIA are taken.	No.
Can privacy by design and by default form a duty to mitigate risks to the rights and freedoms of data subjects/individuals and	Maybe, it also sees to protection of the rights of the data subject.	Maybe, it also sees to protection of the rights of the data subject. However, this is principally in relation to the principles	Maybe, it also sees to protection of the rights of the data subject. However, this sees to transparency and user control and is to

reach a certain level of protection?		of Article 5.	meet the 'data protection obligations'.
Who can provide further guidance on the DPIA?	Supervisory authorities, the European Data Protection Board, and the Commission.	Supervisory authorities and the European Data Protection Board.	Supervisory authorities and the European Data Protection Board

2.6 The consequences

This section discusses the consequences which can be attached to the DPIA. Can a controller be sanctioned for not carrying out a DPIA or for not implementing the identified measures? The focus is on the instances in which the GDPR would technically be complied with, except that the risks are not sufficiently mitigated. If the DPIA points to high risks, then a prior consultation needs to take place. The prior consultation can lead to a prohibition of the processing operation if the risks are not sufficiently identified or mitigated. This is discussed in section 2.6.1. Moreover, a failure to carry out a DPIA or to implement mitigating measures may be subject to sanctions or liability. This is discussed in section 2.6.2. The self-assessment system in the Parliament version, i.e. the compliance review of Article 33a, has already been discussed at the end of section 2.5.2.1.

2.6.1 The prior consultation

2.6.1.1 When is a prior consultation required?

The results of the DPIA determine whether the supervisory authority – or in the Parliament version: the data protection officer - needs to be consulted. More specifically, if the DPIA indicates that the processing operations are likely to present a high degree of specific risks (Commission and Parliament) or a high risk (Council), then a prior consultation will need to take place.[391] In the Council version, a prior consultation only needs to take place if 'the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation', so that despite the measures which are possible, a high risk remains.[392] In the Commission and Parliament versions, the competent authority or the DPO can also choose to carry out a prior consultation if the processing presents any of the risks which are on a list to be produced by the supervisory authority or the European Data Protection Board.[393] These risks also qualify as risks which need to be subjected to a DPIA.[394] As a result, if these risks are present, then controllers must carry out a DPIA and may be faced with a prior consultation.

Under the Parliament version, a prior consultation with the supervisory authority is only required if there is no data protection officer.[395] The supervisory authority can still prohibit processing operations, even though it has not been consulted,[396] but it must now look for intended risky processing operations on its own accord. It can request the documentation on the

[391] GDPR Commission and Parliament version, art 34(2)(a); GDPR Council version, art 34(2).
[392] GDPR Council version, recs 66a and 74 and art 34(2).
[393] GDPR Commission and Parliament version, art 34(2)(b).
[394] GDPR Commission version, art 33(2)(e); Parliament version, art 32a(2)(f).
[395] GDPR, art 34(2). **Strangely, one of the tasks of the DPO is nonetheless to monitor the (...) application for prior consultation, if required pursuant to arts (...) 34'** (GDPR Parliament version, art 37(f)).
[396] GDPR, art 34(3).

DPIA and the compliance review, obtain other relevant information and access premises.[397] Nonetheless, it must somehow gain the knowledge that a controller is looking to start a potentially risky processing operation. The Parliament version emphasises that the insufficiency of the processing can only be determined in accordance with the powers of the supervisory authority, thereby reminding it to stay within its investigatory powers.[398] Under the Commission version, the DPIA must be provided to the supervisory authority – it does not need to request the report, as in the Parliament version.[399] The Council requires the controller to hand over the DPIA report only if a prior consultation takes place.[400] Whether it is wise to trust the DPO's or to involve the supervisory authorities depends on whether they can fulfil their assigned roles properly. Would the supervisory authorities be able to deal with the workload that would come their way in the Commission and Council version?

While public bodies are sometimes exempt from the initial risk analysis, and thus also the subsequent DPIA, if the processing takes place on the basis of the law, the prior consultation is required when new laws are made, i.e.. 'in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards'.[401]

2.6.1.2 What are the possible consequences of the prior consultation?

An agreement on risk mitigation

The prior consultation enables the supervisory authority to make proposals or give advice on risk mitigation. It is not obliged to do so, but can make use of this possibility if it estimates that it would be effective to help the controller. According to the Commission and the Parliament, 'the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation'.[402] The Council first gives controllers a chance to identify mitigating measures outside of the purview of the supervisory authority. If it fails to identify measures to lessen the high risk to an acceptable level, the supervisory authority will give advice to the controller.[403] While this advice is not binding, it occurs in the shadow of the threat of a prohibition. The Council empowers supervisory authorities to issue official warnings,[404] while the Commission and the Parliament allow the controller to be warned or admonished.[405] The advice should see to compliance with the GDPR, but may in practice cross into the area of pure risk mitigation.

A prohibition or limitation of the processing

If the prior consultation does not lead to an agreement on ways to sufficiently mitigate the risk, the processing can be prohibited. The Commission's version of the prior consultation has the most teeth. If the supervisory authority 'is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated'

397 GDPR Parliament version, arts 33(3b), 33a(4), 34(6) and 53(2).
398 GDPR Parliament version, art 34(3).
399 GDPR Commission version, art 34(6).
400 GDPR Council version, art 34(6)(e).
401 GDPR Commission and Parliament version, rec 74.
402 GDPR Commission and Parliament version, rec 74.
403 GDPR Council version, recs 74 and art 34(2) and (3).
404 GDPR Council version, arts 34(3) and 53(1b)(a).
405 GDPR Commission and Parliament versions, art 53(1)(e).

then it 'shall prohibit the intended processing and make appropriate proposals to remedy such incompliance'.[406] The supervisory authority is thus required to make use of one of its strictest powers, namely to prohibit the future processing. This is a preventive measure: it targets problematic projects which have not yet been started. The Parliament version also requires the 'competent supervisory authority' to prohibit the processing.[407] However, because the authority is not notified whether controllers are looking to start a risky project if they have a data protection officer, the Parliament's prior consultation is less powerful.

The Council version does not empower the supervisory authority to prohibit the processing, but rather refers to its powers in Article 53, which it may use with discretion.[408] These powers include a 'temporary or definitive limitation on processing';[409] a full prohibition is not possible. The other powers referred to are discussed in section 2.6.2.1 Many of the corrective powers see to existing breaches, but other preventive measures are the power to issue warnings[410] and the power to suspend data flows to third countries.[411] In the Council version the supervisory authority is bound to make use of its powers within a maximum period of 6 weeks, which can be extended with another 6 weeks, following the request for consultation.[412] However, according to Recital 74 the supervisory authority can still use its powers even if it has not reacted within these time limits.

All three versions are ambiguous as to whether supervisory authorities can prohibit/limit processing operations which would technically comply with the requirements of data protection law, e.g. are necessary for a specified purpose, have a legal ground and allow data subjects to exercise their rights, but which would present unaddressed risks. Because risk mitigation is not an independent obligation under the GDPR, there is a risk of creative compliance. Can supervisory authorities tackle situations of creative compliance? One possible solution is the "principled approach", another is to stretch the supervisory authority's power to prohibit the processing.

Creative compliance

Creative compliance arises when the law is technically complied with, but any meaningful achievement of its objectives is avoided. Detailed rules and technical requirements risk being reduced to a box-ticking exercise: organizations comply with the rules without considering whether this achieves the underlying objective. The norm addressee does not help achieve the desired outcome beyond what is required by the rules.[413] In other words, substantive compliance is avoided. Creative compliance is possible because '[r]ules are imperfect. It is just not possible perfectly to 'translate' the goal sought to be served into a rule (justification)'.[414] Less detailed norms, also called principles, minimise the scope for avoidance or manipulation of the

[406] GDPR Commission version, art 34(3).
[407] GDPR Parliament version, art 34(3).
[408] GDPR Council version, art 34(3).
[409] GDPR Council version, arts 34(3) and art 53(1b)(e).
[410] GDPR Council version, art 53(1b)(a).
[411] GDPR Council version, art 53(1b)(f).
[412] GDPR Council version, art 34(3).
[413] J Black, M Hopper and C Band, 'Making a success of Principles-based regulation' (2007) 1(3) Law and Financial Markets Review 191, 194-195.
[414] H Gribnau, 'Corporate Social Responsibility and Tax Planning: Not by Rules Alone' (2015) 24(2) Social & Legal Studies 225, 227.

norm because they cover more situations.[415] Note, though, that even if there would be an explicit duty to address risks to the rights and freedoms of individuals, creative compliance is hard to avoid. Even if a principle specifies an outcome (e.g. address risks to fundamental rights and freedoms) rather than a means to the outcome (e.g. limit personal data processing to what is necessary for the specified purpose), it still requires a fair and objective measure as to when that outcome has been reached (under what conditions are risks to fundamental rights and freedoms addressed?).[416] These measures can, in turn, be bent and avoided. As soon as the rules which explain principles can be relied on to exhaustively specify these principles, they raise the problem of creative compliance.

In the absence of a duty to address risks to the rights and freedoms of individuals,[417] there is ample space for creative compliance. This is because compliant processing may still be risky to (fundamental) rights and freedoms. Although data protection is ancillary to other rights and freedoms, it was argued at the end of section 2.4.1.4 that data protection does not exhaust the protection of other rights and freedoms. As a result, these rights and freedoms can be considered harmed or even violated by GDPR-compliant processing operations. While non-governmental entities are not under a full duty to respect fundamental rights, governmental entities may be subject to a rights review on top of a data protection compliance review. A supervisory authority may thus be faced with an envisaged project which would be compliant, but which would not address potential harm to or even violation of the rights and freedoms of individuals. In principle, human rights violations are addressed by National Human Rights Institutions, but since they may also fall within the scope of data protection, supervisory authorities may also have the mandate to address them. The question is whether they can do so if there is technically no violation of data protection law.

The principled approach

The problem of creative compliance is tackled if rules must be interpreted in light of underlying (legal-)ethical principles. This solution is advocated by Gribnau and Happé, who address the problem of creative compliance in tax law. In this area of law, the problem has its own name: tax avoidance. Tax avoidance may be legal because it follows the rules, but it does conflict with the fair share principle if organizations avoid paying a fair share of tax.[418] Happé argues that citizens are under a moral duty to avoid interpretations of the law of which they should know that they would have caused the legislator, if it had had the foresight, to adapt the law.[419] Assuming that the legislator wants a fair distribution of the tax burden, this would place a moral duty on citizens to pay a fair share of tax. Taking a slightly different road, Gribnau argues that organizations which endorse corporate social responsibility should acknowledge the duty to pay a fair share of tax as a *legal* responsibility. They should interpret rules in accordance with the underlying principles (in the Dworkinian sense of the word) and acknowledge these principles as legally binding, even though they are not binding from a formalistic perspective. 'CSR companies see legal responsibilities in conformity with the internal morality of tax law.'[420]

---

[415] Black, Hopper and Band (2007) 194-195.
[416] Black, Hopper and Band (2007) 199.
[417] Section 2.5.2.2.
[418] Gribnau (2015) 244.
[419] R Happé, 'Belastingrecht en de geest van de wet: Een peidooi voor een beginsel-benadering in de wetgeving' (inaugural lecture, Tilburg University 2011) 38.
[420] Gribnau (2015) 245.

Similarly, it can be argued that controllers should interpret data protection law in accordance with an underlying principle of mitigation of risks to rights and freedoms. As opposed to tax law, there already is a duty to respect this underlying principle: governments, and to some extent non-governmental entities, need to respect fundamental rights and freedoms. Governments bear the moral and legal duty to respect fundamental rights on the basis of national constitutions and, if they are Member to the Council of Europe and/or the European Union, the ECHR and/or the Charter.[421] According to the *Promusicae* case law discussed above,[422] the courts and authorities of Member States must interpret European legislation in light of these fundamental rights. However, non-governmental entities are not the norm-addressees of these legal instruments, nor of the *Promusicae* duty of rights-conform interpretation. Their legal accountability for fundamental rights violations is tricky. The principle of accountability in data protection law might have a role to play here in the future; but as drafted in the GDPR, it only requires controllers to be compliant and be able to demonstrate their compliance.[423] The problem is that the word "compliant" can be interpreted as meaning "technically compliant" or "minimally compliant". It is not possible to draft a duty to achieve substantive compliance in terms of compliance: words can always be ascribed a minimalist meaning which does not accord with the meaning intended by the legislator. It is up to supervisory authorities and courts to give further substance to the words in a way which limits the space for creative compliance.

Following Happé, organizations should make sure to interpret Article 33 as a duty to address risks to rights and freedoms, as this is probably what the legislator envisaged with the risk-based approach. Following Gribnau, the duty can also be seen as part of the "internal legal morality" of data protection law, as a result of which CSR companies would be under a moral responsibility to construe it as part of data protection law. Both roads lead to the same outcome: controllers should not apply the law in a manner which conflicts with the duty to address risks to the rights and freedoms of individuals. As a result, the law should be interpreted in line with its spirit and creative compliance is avoided. However, in both the account of Happé and Gribnau, the duty to interpret the law in line with its spirit is solely a moral one. Even if it is a legal duty in the case of mitigation of risks to fundamental rights, controllers surely cannot be punished for their no-longer-creative compliance without qualification. They might rely on good faith interpretations as to what this responsibility entails, possibly on the basis of legitimate expectations which have arisen due to guidance given by the supervisory authority. Enforcement of the duty to interpret the law in line with its spirit would be limited by, at the very least, the principle of legality[424] and, depending on the circumstances, the protection of legitimate expectations.

In sum, while there is an opening for the argument that governmental entities are under a duty to construe data protection law in line with a responsibility to address risks to fundamental rights and freedoms, there is no legal duty for non-governmental entities to construe the law in line with fundamental rights. Moreover, the construct would be limited by its lack of clarity and the accompanying limits to enforcement. Vague norms cannot be enforced to mean whatever the government wants them to mean, especially not if assurances have been made on their content and how they will be enforced.

---

[421] European Convention on Human Rights (ECHR), art 1; Charter, art 51(1); Treaty on the European Union (TEU), art 6(1).
[422] Section 2.5.2.2.
[423] GDPR, art 22.
[424] cf text at footnote 438 and footnote 438.

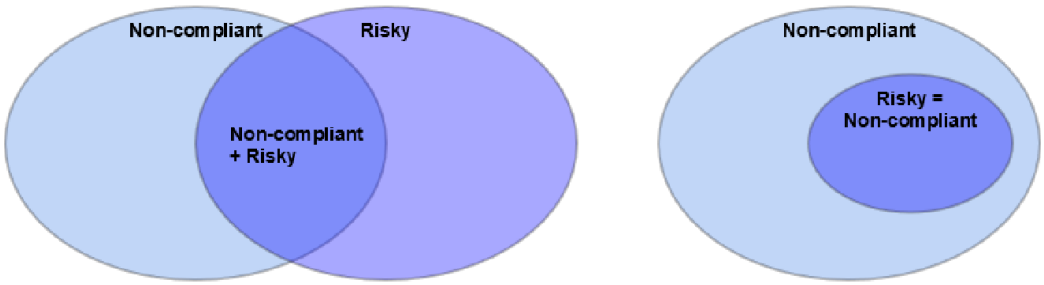
A prohibition or limitation of processing which is risky, but compliant?

The GDPR does not clarify whether the supervisory authority can prohibit future risky processing operations on account of their riskiness. Normally, the starting point would be that only real acts of non-compliance can be prohibited, leaving creative compliance without sanction. However, the broad meaning attached to the term 'risk' makes things blurry. Article 34(3) allows the supervisory authority to prohibit the intended processing operation[425] or to use its powers[426] if it 'is of the opinion'[427] or if it 'determines in accordance with its power'[428] that *the processing would not comply with the GDPR, in particular where the risks are insufficiently identified or mitigated*.[429] The provision apparently assumes that if risks would not be sufficiently mitigated, this would be an instance of non-compliance with the GDPR. Given that the DPIA concerns risks to rights and freedoms above and beyond those protected by the requirements of the GDPR,[430] the term 'risks' in Article 34(3) should again refer also to the broad notion of risks to rights and freedoms which is employed in relation to the DPIA. It would be inconsistent to interpret Article 34(3) as seeing only to the situation in which risk mitigation would be required by the GDPR, e.g., to rely on legitimate interest as a legal ground for the processing. But, if the term 'risks' is so broad, then not all risky situations are non-compliant. The GDPR ignores this difficulty, pretending instead that risky processing operations are also non-compliant (see figure below).

Two other subparagraphs of Article 34 point in different directions. On the one hand, Article 34(6) indicates that the supervisory authority should be interested only in assessing the risks for the protection of personal data of the data subject, and not those to other rights and freedoms which fall outside the scope of the data protection principles. It specifies that the supervisory authority can request information to allow it 'to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards'.[431] On the other hand, Article 34(2) also presents the prior consultation as a compliance check which entails the mitigation of a broader array of risks. The supervisory authority should be consulted 'in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects'.[432] Article 53, which specifies the powers the supervisory authority can make use of, does not provide the needed clarity. The supervisory authority can impose a temporary or definitive ban[433] or limitation on processing.[434] While other powers relate to breaches or acts of non-compliance,[435] this power is not explicitly restricted to (anticipated) violations of data protection law. It is not formulated in relation to breaches or acts of non-compliance.

---

425 GDPR Commission and Parliament version, art 34(3).
426 GDPR Council version, art 34(3).
427 GDPR Commission and Council version, art 34(3).
428 GDPR Parliament version, art 34(3).
429 GDPR, art 34(3) GDPR.
430 Section 2.4.2.
431 GDPR Commission and Parliament version, art 34(6).
432 GDPR Commission and Parliament version, art 34(3). See also GDPR Commission and Parliament version, rec 74: **the supervisory authority should be consulted 'on a risky processing which might not be in compliance with this Regulation'.**
433 GDPR Commission and Parliament version, art 53(1)(g).
434 GDPR Council version, art 53(1b)(e).
435 GDPR Commission and Parliament version, arts 53(1)(a) and (d); GDPR Council version, art 53(1b)(d).



Actual situation under GDPR

Assumption of the GDPR

It remains ambiguous whether the prior consultation aims to prevent situations which would be both non-compliant and risky, or whether it also targets risky situations which are technically compliant. As stated, the GDPR pretends that risky processing operations are also non-compliant (see figure above).[436] It apparently assumes either that there *is* a duty to mitigate risks, or that GDPR-compliant processing *cannot* be considered an interference with rights and freedoms. While the constitutional courts probably would not accept the latter, at least not with regard to governmental entities, the former might become a reality. The ambiguity allows such a duty to be developed in a piecemeal fashion, outside of the lobby-rich legislative process through which the GDPR is negotiated.

Whether or not the power to prohibit the processing should be limited to risks which are relevant for a requirement of data protection law depends on a balancing act which Member States need to make. A broad interpretation of Article 34(3), allowing supervisory authorities to prohibit risky processing in the absence of a corresponding explicit duty of controllers, could greatly benefit the rights and freedoms that are potentially adversely affected by the processing operation. However, it would be at odds with the principle of legality and the freedom to conduct a business. The freedom to conduct a business is safeguarded by Article 16 of the Charter. It entails the freedom to exercise an economic or commercial activity, protecting 'economic activity and the ability to participate in the market' and serving as a limit on the legislative and executive actions of the EU and the Member States.[437] Data processing operations for economic or commercial purposes can therefore only be restricted if this is proportionate. It is not necessarily disproportionate to prohibit data processing operations because of their risks to (fundamental) rights and freedoms. To do so in a manner which leaves controllers to the whims of supervisory authorities might not, however, be the best way to achieve rights protection. Allowing supervisory authorities to prohibit actions which are risky but not non-compliant would leave the supervisory authorities virtually unbounded. Such a large discretion is at odds with the principle that any government action must be authorized by a clear legal basis (the principle of legality).[438] The various rights and principles need to be balanced by the Member

[436] **It does not do so consistently. According to Recital 74 of the Commission and Parliament version, processing which presents a high degree of specific risks '(...) might not be in compliance with this Regulation'.**

[437] e.g. Case C-4/73 *J Nold, Kohlen- und Baustoffgroßhandlung v Ruhrkohle Aktiengesellschaft* [1977] ECR 00491; Case C-426/11 *Alemo-Herron v Parkwood* [2014] 1 CMLR 21, Opinion of AG Cruz Villalón, paras 50-51; European Union Agency for Fundamental Rights, Freedom to conduct a business: exploring the dimensions of a fundamental right (Publications Office of the European Union 2015) 21.

[438] **There may also be tension with the narrower principle of legality as protected by Article 49 of the Charter and Aticle 7 ECHR. It protects citizens against sanctions which are not prescribed by law or which are prescribed on the basis of an extensive interpretation of the law. Non-criminal sanctions are included within its scope if they are generally applicable and of a deterrent and punitive, rather than a compensatory, nature.**

States in their interpretation and application of the GDPR.[439] Through its ambiguity, the GDPR leaves it up to the Member States to determine the balance between the protection of rights and freedoms of individuals in the digital context on the one hand, and the principle of legality and the freedom to conduct a business on the other.[440] From the perspective of constitutional pluralism,[441] this sensitive topic may indeed best be regulated at the national level. It may therefore be for the best that the poor drafting of the GDPR leaves it for Member States to determine to what extent preventive risk mitigation is enforceable under the risk-based approach.

2.6.2 Sanctions and liability

2.6.2.1.Powers of the supervisory authority

The GDPR grants the supervisory authority a number of powers in Article 53. Under the Commission and Parliament versions, the choice to prohibit the intended processing operation can be enforced by the supervisory authority. The authority is empowered to ensure compliance with prior consultations.[442] This power may also extend to any agreement reached on the measures which are to be taken to address the risks. While there is no obligation to follow the advice given by the supervisory authority, the controller probably made promises with regard to risk mitigation to prevent the supervisory authority from prohibiting its risky processing operation. If these promises can be enforced, then risk mitigation can be enforced!

The power to impose a ban[443] or a limitation[444] on the processing is also mentioned in Article 53, separate from the prior consultation. As a result, the power exists even if no prior consultation took place. By itself this power is not preventive; there is no reference to "envisaged" processing. Although the GDPR does not add that it can only be used in relation to non-compliant processing operations, there is no indication that the provision should be interpreted to cover processing which is risky, but compliant. Again, a wide interpretation would conflict with the principle of legality. Many of the other powers only see to specific breaches or data subject rights. They see to rectification of the deficit, not to a prohibition or a prevention thereof.[445] An exception is the

---

This can include administrative sanctions. A prohibition of processing operations by an administrative authority may qualify as a criminal sanction because of its deterrent and punitive effect. However, considering its risk-based rationale, it could also be seen as wholly of a preventive nature. In the latter case, there would be no interference with the principle of legality as laid down in the Charter and the ECHR. See Charter, art 52(3); *Engel and Others v the Netherlands* (2008) Series A no 22, paras 82-83; *Öztürk v Germany* (1984) Series A no 73, paras 48-50; *Menarini Diagnostics s.r.l. v. Italy* App no 43509/08 (ECtHR 27 September 2011); *Tadeusz Matyjek v Poland* App no 38184/03 (ECtHR 30 May 2006), paras 43-47; Case C-45/08 *Spektor Photo Group NV v Commissie voor het Bank, Financie- en Assurantiewezen* [2009] I-12073, para 42; S Peers, T Hervey, J Kenner and A Ward (eds), *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2014) 49.20.

[439] *Lindqvist*, para 87; *Promusicae*, para 68; Section 2.4.1.4.

[440] **The Council expressly acknowledges that Member States can provide for penalties which are applicable to violations, in particular where the GDPR does not specify an administrative fine.** GDPR Council version, art 79b(1). cf GDPR Commission version, art 78.

[441] **Constitutional pluralism includes the normative claim that the EU should be pluralist, i.e. 'premised upon mutual recognition and respect between national and supranational authorities'.[441] The different legal orders and their constitutional discourses should co-exist in a heterarchical rather than hierarchical relationship because there is no way of assessing their relative strength or validity**. N Walker, 'The Idea of Constitutional Pluralism' (2002) 65 Modern Law Review 317, 337.

[442] GDPR Commission and Parliament version, art 53(1)(d).

[443] GDPR Commission and Parliament version, art 53(1)(g).

[444] GDPR Council version, art 53(1b)(e).

[445] GDPR Commission and Parliament version, arts 53(1)(a), (b) and (f); GDPR Council version, arts 53(1b)(ca) and (d).

power to suspend data flows to third countries.[446] In the Council version, this powers can be used by the supervisory authority in the context of the prior consultation, and thus as a preventive measure.

In addition to these powers, a sanction can be issued in accordance with Articles 79 and 79a.[447] Fines must be effective, proportionate and dissuasive.[448] The Parliament follows a different system than the Commission and the Council. In the Commission and Council version, the GDPR meticulously specifies what fine can be attached to which violations. Other cases may still be penalised on the basis of national law if this is necessary, 'for example in cases of serious infringements of the Regulation'.[449] The GDPR specifies that the controller (or processor) can be sanctioned for intentionally or negligently not carrying out a DPIA or for skipping the prior consultation, if it was required.[450] Apparently the controller cannot be fined for carrying out a DPIA poorly –only for not doing so at all.[451] The same with the prior consultation: the fine can only be issued if the controller processes data without a prior consultation, even though the consultation is required by Article 34. The GDPR does not provide for the penalisation of a failure to carry out the advice of the supervisory authority or to abide by its prohibition. The fine has a maximum of 1 million Euros or, if the controller or processor is an undertaking, 2 % of the total worldwide annual turnover of the preceding financial year.[452] In the Commission version, the supervisory authority must impose the fine, with an exception for small and unknowing first-time offenders.[453] In the Council version, the supervisory authority may choose whether it issues a fine.[454]

In the Parliament version, the offences are not described. The supervisory authority shall impose a sanction 'to anyone who does not comply with the obligations laid down in this regulation'.[455] Thus, controllers can be sanctioned for not carrying out a DPIA in the manner required by Article 33 – and perhaps even for not aiming for a proper level of protection with the envisaged mitigating measures, if this is read into the requirement to describe measures to mitigate the risk.[456] There is currently no hard duty to effectuate the mitigating measures, although the Parliament does require controllers to review whether they comply with the DPIA.[457] If a duty to carry out risk mitigating measures of a certain level would come into existence as a hard norm, the Parliament version entails that controllers should also be fined for not mitigating risks properly. This possibility is not provided for by the Commission and Council versions, so that national law would need to be implemented. The supervisory authority must sanction non-compliance, but it can choose between 1) a warning in cases of first and non-intentional non-compliance, 2) regular periodic data protection audits, and 3) a fine up to 1

446 GDPR Commission and Parliament version, art 53(1)(h); GDPR Council version, art 53(1b)(f).
447 GDPR Commission and Parliament version, art 53(4); GDPR Council version, rec 118b and art 53(1b)(g).
448 GDPR Commission and Parliament version, art 79(2); GDPR Council version, art 79(1).
449 GDPR Council version, rec 120a.
450 GDPR Commission version, art 79(6)(i); GDPR Council version, art 79a(3)(de).
451 **However, the Commission also specifies that 'penalties should be imposed to any person, whether governed by private or public law, who fails to comply with this Regulation'.** GDPR Commission and Parliament version, rec 119.
452 GDPR Commission version, art 79(6)(i); GDPR Council version, art 79a(3)(de).
453 GDPR Commission version, arts 79(3) and 79(6).
454 GDPR Council version, art 79a(3),
455 GDPR Parliament version, art 79(2a). See also GDPR Parliament version, rec 119.
456 GDPR Parliament version, art 33(3)(d).
457 GDPR Parliament version, art 33a.

million Euros or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is higher.[458]

2.6.2.2 Liability

The GDPR also regulates the liability of the controller for damage. In the Commission and Parliament version, the controller may be liable for the damage resulting from 'an unlawful processing operation or of an action incompatible with this Regulation'.[459] This leaves open the option that the controller is liable not only for not carrying out a DPIA or for not including the required elements, but also for not identifying sufficient mitigating measures and for not actually achieving a certain level of protection through the implementation of mitigating measures. While there is no explicit duty to mitigate risks, it is incompatible with the DPIA system not to mitigate risks at all. In the context of civil liability, a broad interpretation is not frustrated by the legality principle. Risk mitigation through DPIA's can become a parameter of a duty of care.[460]

In the Council's version, controllers and processors are only liable for damage resulting from 'a processing which is not in compliance with this Regulation'.[461] As a result, the Council's GDPR would only provide for compensation for damage arising from insufficient risk mitigation if data protection law required the risk to be mitigated or if the courts are willing to construct a general duty to address risks. However, Article 77 does not exclude a stricter national liability regime, for example on the basis of national tort law.

Like the Council version, the Parliament version makes explicit that the controller can also be liable for non-pecuniary damage.[462] This opens up the possibility for claims regarding, for example, a social disadvantage or a loss of the freedom of thought.[463] It may also be of help if evidence is hard to come by. In case of identity theft following a data breach, for example, it may be difficult to establish a causal relation. The plaintiff may choose to also base the claim on the non-pecuniary damage caused by the privacy invasion.

According to Article 77(3), the system of liability is culpability-based. Strangely, this paragraph is not included in the online consolidated version of the Parliament version on the website of the European Parliament,[464] but there is no amendment to remove it in the Report of the LIBE Committee either.[465] The provision states that the controller may be exempted from liability if it proves that it is not responsible for the event giving rise to the damage,[466] 'in particular where he established fault on the part of the data subject or in case of force majeure'.[467] Culpability is thus

458 GDPR Parliament version, art 79(2a).
459 GDPR Commission and Parliament version, art 77(1).
460 L Costa, 'Privacy and the precautionary principle' (2012) 28(1) Computer Law & Security Review 14, 20.
461 GDPR Council version, art 77(1) and (2).
462 GDPR Parliament version, art 77(1); GDPR Council version, art 77(1).
463 cf GDPR Council version, art 33(1).
464 European Parliament, 'Text adopted Wednesday, 12 March 2014 – Strasbourg. Protection of individuals with regard to the processing of personal data' <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN> accessed 16 August 2015.
465 European Parliament, 'Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – LIBE Committee' (A7-0402/2013).
466 GDPR Commission and Council version, art 77(3).
467 GDPR, rec 118.

assumed; it is for the controller to prove that it is not culpable. If the controller can show that it was not aware of the risk, it has a chance of escaping liability; according to Costa, 'no liability will exist if threats are not anticipated by the PIA that took place, except if there is fault'.[468] The DPIA report can help counter such efforts because it is evidence of the risks of which the controller was aware. The stakeholder consultation can also help establish or – as pointed out by Wright and others - avoid liability.[469] If the data subjects point to a certain risk, then the controller was aware of it – but this also gives it the opportunity to take action. Under a strict culpability regime, the controller may even be considered at fault if it did not conduct a stakeholder consultation, because then it still "could have known" about the risk.[470] A practical difficulty is that the DPIA report and the stakeholder consultation do not need to be made available to the public, although such transparency has been advocated in the body of literature on privacy impact assessments.[471] However, under the Dutch law on civil procedure, the judge can request documents so as to ascertain what actually happened.[472] The plaintiff will probably also be able to gain access to the report during discovery. The ability of plaintiffs to demand insight into documents is limited so as to prevent fishing expeditions; the report can only be obtained in court if the plaintiff can show a legitimate interest to obtain this specific document.[473] But the plaintiff who needs access to a specified document so as to counter efforts to disprove a plausible tort claim in principle has a legitimate interest to obtain it.[474] Lastly, fault would also be almost non-disputable if the supervisory authority has prohibited the processing, but the controller proceeds anyway. Indeed, the controller would be considered at fault if it was in breach of the GDPR.[475] In these cases, the controller will have a difficult time contesting its responsibility.

However, should the damage arise from an operation which has been authorized during the prior consultation, culpability would be quite easily contested if the consultation had regard to the risk which caused the damage. Supervisory authorities cannot prohibit risky processing in the absence of an explicit duty to mitigate risks, with two exceptions: 1) the processing is contrary to a requirement of the GDPR, for example the duty to implement security measures, and 2) the principle of legality is stretched in favour of fundamental rights protection. With respect to the many risks which the GDPR does not protect against, the supervisory authority will probably need to allow the processing. As a result, the culpability in relation to damage arising from the realization of these risks will be difficult to maintain. It is likely, though, that this caveat is of minor importance only. These risks will probably not be identified in the DPIA, nor discussed during the prior consultation.

---

468 L Costa (2012), 21.
469 Wright, Gellert, Gutwirth and Friedewald (2013) 97.
470 D Wright, 'Making Privacy Impact Assessments More Effective' (2013) 29(5) The Information Society: An International Journal 307, 312.
471 Wright (2011) 130; De Hert (2012) 75; Finn, Rodrigues and Wright (2013) 163-164.
472 Wetboek van Burgerlijke Rechtsvordering, art 22,
473 Wetboek van Burgerlijke Rechtsvordering, art 843a.
474 This follows from *Kamerstukken II* 2011/12, 33 079, nr. 3, p. 7. A Rueb, *Compendium Burgerlijk procesrecht* (Kluwer 2011) 156-157. **Another requirement is that the plaintiff and its counterparty have a concrete legal relationship, but this is fulfilled if the subject of the dispute is the obligation to compensate the plaintiff on the basis of tort. However, the report does not need to be handed over if it is covered by a duty of secrecy or if there are serious reasons outweighing the legitimate interest of the plaintiff.**
475 cf L Costa (2012) 21.

2.6.3 Conclusion

By way of conclusion the consequences which may surround the DPIA are summarized in chronological order. First, the controller can be fined for failing to carry out a DPIA and, under the Parliament version, for not carrying out a DPIA in line with the requirements; e.g. for not carrying out a risk evaluation or failing to identify mitigating measures. The DPIA must always be provided to the supervisory authority (Commission), or only if a prior consultation is taking place (Council), or it must be requested by the supervisory authority (Parliament). If the DPIA points to a high degree of specific risks (Commission and Parliament) or a high risks in the absence of the mitigating measures (Council), then the supervisory authority needs to be consulted before the processing starts. An exception is provided in the Parliament version, which requires the data protection authority to be consulted instead. The controller can be fined for failing to consult the supervisory authority, if this is required. During the prior consultation, the controller may decide to follow the advice of the supervisory authority and agree to implement certain mitigating measures. These negotiations take place in the shadow of the threat of a prohibition of the processing.

In accordance with Article 34 GDPR, the supervisory authority must prohibit the envisaged processing (Commission and Parliament) or may make use of its powers (Council) if it finds that *the processing would not comply with the GDPR, in particular where the risks are insufficiently identified or mitigated*.[476] This is a preventive measure. It is unclear whether the supervisory authority can prohibit processing operations which would comply with the GDPR but would still be risky. There is a lot of space for creative compliance because there is currently no duty to address risks to the rights and freedoms of individuals. Data protection does not exhaust the protection of other rights and freedoms, so these rights and freedoms may still be violated (particularly in the case of government entities, who are subject to a rights review) or harmed, even if the GDPR is complied with. A possible solution to creative compliance is the principled approach, which obliges controllers morally to interpret the law in line with its spirit. However, there is no legal duty for non-governmental entities to construe the law in line with fundamental rights – and even if there was, enforcement would be limited by principles such as the principle of legality. Nonetheless, the GDPR appears to allow Member States to interpret Article 34 in a way which allows supervisory authorities to prohibit processing operations which are risky but compliant. The provision is ambiguous because it appears to assume, wrongly, that if risks would not be sufficiently mitigated, this would be an instance of non-compliance with the GDPR. As a result, Member States should construe it in line with a balancing of the fundamental rights and principles involved. If great weight is accorded to the principle of legality, then processing which is compliant but still risky to rights and freedoms cannot be prohibited. Indeed, to accord such a wide power to an administrative authority in the absence of a clear legal basis conflicts with the principle of legality.

If the processing is prohibited during the prior consultation, this ban can be enforced by the supervisory authority. If not, the controller may start its project. However, the supervisory authorities can still make use of the powers accorded to them by Article 53. They can ensure compliance with the prior consultation, which might mean that any agreement reached on risk mitigation can be enforced. They can also prohibit or limit processing outside of the context of a prior consultation, but it would be at odds with the principle of legality to prohibit operations

[476] GDPR, art 34(3).

which are risky, but compliant. Further, the supervisory authorities can order the controller to remedy breaches of the GDPR and issue fines for non-compliance. The Commission and the Council version prescribe by way of minimum harmonisation which instances of non-compliance can be fined. The Parliament version contains a more general provision, allowing all instances of non-compliance to be fined. Accordingly, should a duty to address risks to the rights and freedoms of individuals/data subjects come into existence on the basis of the GDPR, controllers could be fined for not actually mitigating risks.

Meanwhile, according to the Commission and Parliament versions controllers may still be faced with liability for actions which are incompatible with the GDPR. It is incompatible with the GDPR not to mitigate risks. Because the legality principle does not stand in the way of a broad interpretation, it is much less problematic to "sanction" controllers for not mitigating risks properly through civil liability than through administrative fines. The Council limits liability to processing which is not compliant with the GDPR, but Member States can adopt more strict liability regimes. The Council and Parliament make explicit that the controller can be liable for non-pecuniary damage. However, the liability regime is not one of strict liability; culpability is required. The burden of proof is on the controller. The DPIA report and the stakeholder consultation can strongly indicate that the controller had knowledge of a risk. Non-compliance with a prior consultation would be particularly culpable. In these cases, the controller will have a very hard time disputing its responsibility. The controller may have more success if the supervisory authority permitted the processing, even after having considered the risk which ended up causing the damage to which the claim relates.

	Commission	**Parliament**	**Council**
The prior consultation			
When is a prior consultation required?	If the DPIA indicates that the processing is likely to present a high degree of specific risk.	If the DPIA indicates that the processing is likely to present a high degree of specific risk. The supervisory authority only needs to be consulted if there is no data protection officer.	If the DPIA indicates that the processing *would result* in a *high* risk *in the absence of measures to be taken by the controller to mitigate the risk.*
Can the supervisory authority start a prior consultation in other cases?	Yes, if it deems it necessary with regard to the risks specified on the list of the supervisory authority.	Yes, if it deems it necessary with regard to the risks specified on the list of the European Data Protection Board.	No.
Does the supervisory authority have access to the DPIA report?	Yes, it must always be provided.	Yes, the supervisory authority can request it.	Yes, it must be provided if a prior consultation takes place.
Can the supervisory authority give advice?	Yes, it can make proposals to remedy non-compliance and warn or admonish the controller.	Yes, it can make proposals to remedy non-compliance and warn or admonish the controller.	Yes, it can give advice and issue official warnings.
Can the supervisory authority prohibit the intended processing?	Yes, it shall do so if it *is of the opinion* that the intended processing does not comply with the GDPR, in particular where risks are insufficiently identified or mitigated.	Yes, it shall do so if it *determines in accordance with its power* that the intended processing does not comply with the GDPR, in particular where risks are insufficiently identified or mitigated.	It can make use of its powers, including a temporary or definitive limitation on the processing, if it is *of the opinion* that the intended processing *would* not comply with the GDPR, in particular where *the controller has* insufficiently identified or mitigated the

			risk.
Is there a time limit?	No.	No.	Yes, the supervisory authority should use its powers within a period of 6 weeks, to be extended by another 6 weeks.
Can compliance with the prior consultation be enforced?	Yes.	Yes.	No.
Sanctions			
Can processing still be stopped after it has commenced?	Yes, it can be prohibited.	Yes, it can be prohibited.	Yes, it can be limited.
Can or must the controller be fined?	Yes. The GDPR specifies which acts of non-compliance are subject to what fines. Failing to carry out a DPIA or skipping the prior consultation *must* be fined, although a warning may be given instead in case of a first and non-intentional non-compliance if the processing is carried out by a natural person without a commercial interest or by a SME which processes personal data as an ancillary activity.	Yes. Any act of non-compliance *must* be sanctioned, but the supervisory authority can choose between 1) a warning in cases of first and non-intentional non-compliance, 2) regular periodic data protection audits, and 3) a fine.	Yes. The GDPR specifies which acts of non-compliance are subject to what fines. Failing to carry out a DPIA or skipping the prior consultation *can* be fined.
What is the height of the fine?	A maximum of 1 million Euros or, if the controller or processor is an undertaking, *2 %* of the total worldwide annual turnover of the preceding financial year.	A maximum of 1 million Euros or up to *5%* of the annual worldwide turnover in case of an enterprise, whichever is higher.	A maximum of 1 million Euros or, if the controller or processor is an undertaking, *2 %* of the total worldwide annual turnover of the preceding financial year.
Liability			
	Any person who suffered damage as a result of an unlawful processing operation or *an action incompatible with the GPDR* has the right to *receive* compensation for the damage.	Any person who suffered damage, *including non-pecuniary damage*, as a result of an unlawful processing operation or *an action incompatible with the GPDR* has the right to *claim* compensation for the damage.	Any person who suffered *material or immaterial* damage as a result of a processing which is *not in compliance with the GDPR* has the right to *receive* compensation for the damage.
	The controller or processor is liable unless it proves that it is not responsible for the event which gave rise to the damage.	The controller or processor is liable unless it proves that it is not responsible for the event which gave rise to the damage. (? – The Parliament did not clearly include nor reject this provision)	The controller or processor is liable unless it proves that it is not responsible for the event which gave rise to the damage.

2.7 The process

There are many ways to comply with the requirement to conduct a data protection impact assessment of Article 33 GDPR. Two European Data Protection Authorities have issued guidance on the privacy impact assessment (PIA).[477] While these documents do not concern the future data protection impact assessment of Article 33 GDPR, and differ in substance in some areas, they can give a good understanding of the steps which a controller could follow. The CNIL's PIA Manuel of June 2015 is most recent. The ICO's code of practice dates from February 2014. Further, Wright has published a step plan which builds on the PIAF project and which is also included in PRESCIENT.

The CNIL identifies the following steps, which need to be taken to comply with the French Data Protection Act:

- Define and describe the context of the processing of personal data under consideration and its stakes. What are the purposes and the stakes for the processing; is the data personal data; who receives personal data and how long is it stored; who is the controller and who are the processors; what is the personal data life cycle?
- Identify existing or planned controls to comply with legal requirements (legal controls) and to treat privacy risks in a proportionate manner (risk-treatment controls; i.e. organizational and security measures). It is recommended to first look for cross-organisational controls to manage and control the protection of privacy; to then look for controls to prevent security breaches; then, if the risks are not sufficiently addressed, to prevent the potential impacts; to control risk sources; or to control the vulnerabilities of the file management system.
- Assess privacy risks to ensure they are properly treated. The risk level is determined in layers. First, the risk source is identified. Then the feared events (the events which would cause the threat, such as unlawful access to data) are identified and their impact and severity is analysed. Next, the causes of these feared events are identified, and it is assessed how they would be caused and how likely they are. Lastly, the risk is evaluated in terms of likelihood and severity. The CNIL sees illegitimate access, unwanted alteration and disappearance of personal data as the feared events, which greatly limits the scope of the impact assessment.
- Make the decision to validate the manner in which it is planned to comply with privacy principles and treat the risks, or review the preceding steps. This requires the controller to review whether the controls can be improved and whether the way in which the risks are treated, can be improved. Then it should check whether the risks are acceptable in relation to the stakes. If the PIA is not acceptable, then the controller should identify objectives which should be reached for it to become acceptable. If it is acceptable, then it may be necessary to create an action plan for the controls.[478]

Interestingly, the CNIL first requires the measures or controls to be determined, and then the residual risks to be assessed. To the contrary, the GDPR first requires a preliminary risk analysis.

[477] See also the Guidance on Privacy Impact Assessment in Health and Social Care of the Health Information and Quality Authority of Ireland.
[478] CNIL (2015) 7-16.

ICO's PIA code of practice sees privacy impact assessments as non-mandatory.[479] It contains the CNIL's elements, in a slightly different order, and adds extra steps.

- Identify the need for a PIA.
- Describe the information flows: what information will be obtained, used and retained, and by whom and for what purpose.
- Identify the privacy risks to individuals, compliance risks and any related risks for the organisation (such as regulatory action or fines or reputational damage). This includes a compliance check with data protection law and other relevant legislation. Privacy risks include damage caused by a data breach, or upset caused by an intrusion on privacy.
- Identify and evaluate the privacy solutions. This requires the controller to devise ways to reduce or, if possible, eliminate privacy risks, assess the costs and benefits of each option, and choose an approach which is satisfactory in light of the aims of the project and the impact on privacy. Possible measures are to not collect or store certain types of data, to implement technological security measures, to make staff aware of privacy risks, or to increase the awareness of individuals about how their data is used. If there are unacceptable privacy risks which cannot be eliminated or reduced then the organisation will need to reassess the viability of its project.
- Sign off and record the PIA outcomes. The report should summarise the process and the steps taken to reduce the risks, and record the decisions to eliminate, mitigate or accept the identified risks. It is good practice to record who has signed off what and why, and to publish the PIA report.
- Integrate the outcomes into the project plan, so as to ensure that the recommended steps are implemented.
- Consult with internal and external stakeholders as needed throughout the process.[480]

Building on the PIAF project, Wright presents a process which contains the same elements, but includes more steps to embed them in the organizational processes. The impact assessment for privacy and ethics of PRESCIENT contains the same steps, adapted to also take ethical risks into account.[481]

1. Determine whether a PIA is necessary; i.e. whether the processing potentially impacts upon privacy.
2. Identify the PIA team and set the team's terms of reference, resources, and time frame. The project manager might need additional expertise. The terms of reference include whether public consultations will take place, to whom the report will be submitted, and what the nominal budget and time frame for the PIA is.
3. Prepare a PIA plan: what is to be done by whom and when.
4. Agree on the budget for the PIA. The nominal budget may need to be amended.
5. Describe the proposed project to be assessed. This includes contextual information.
6. Identify stakeholders, i.e. those who are interested in or affected by the project. These may be internal or external to the organization and could include regulatory authorities. A representative should be chosen for groups.

[479] ICO (2014) 4.
[480] ICO (2014).
[481] PRESCIENT (2013) 91-96.

7. Analyze the information flows and other privacy impacts: who will collect what information from whom and for what purpose; how will the information be used and how will it be stored, secured, processed and distributed and for what purpose; how well will controllers protect the information and whether they will pass it on to third recipients. The impact on all types of privacy – not only informational privacy – should be considered.
8. Consult with stakeholders. Stakeholders can help identify and assess privacy risks and the consultation may help avoid later criticism or liability.
9. Check that the project complies with legislation.
10. Identify risks and possible solutions. The risk identification entails the identification of all the possible risks and of who will be impacted by the risks, and an assessment in terms of likelihood and consequence (magnitude of the impact) and the number of people who could be affected.
11. Formulate recommendations. It should be clear to whom the recommendations are directed.
12. Prepare and publish the report, for example on the organization's website. The sensitive bits can be redacted or put into a confidential annex.
13. Implement the recommendations. The organization should make public which recommendations are accepted.
14. Third-party review and/or audit of the PIA by supervisory authorities, data protection officers or independent auditors. This is the only way to ensure that PIAs are carried out properly and that their recommendations are implemented.
15. Update the PIA if there are changes in the project. If the changes are large, a new PIA should be carried out – as if it were a new project.
16. Embed privacy awareness throughout the organization and ensure accountability. The CEO should make sure that all employees are sensitive to the possible impacts on privacy of their work.[482]

Outside of the organizational steps and the substantiation of what needs to be assessed (which risks, posed by which processing operations), these guides are quite similar to each other and to the DPIA. The DPIA also includes a threshold analysis,[483] a description of the project,[484] the identification and assessment of risks,[485] the identification of measures (or so-called controls, privacy solutions, or recommendations),[486] and, in the Commission and Council version, the stakeholder consultation.[487] The need to record the DPIA is either explicit[488] or implied by the fact that the supervisory authority can receive it.[489] The prior consultation[490] and the compliance review[491] provide for a review or an audit. What is lacking is the action plan for implementation and – compared to Wright's PIA - the actual implementation and the publication of the report, and a clear obligation to update the DPIA if changes are made.

[482] Wright (2013), 310-313; PIAF (2012) 24.
[483] GDPR Commission and Council version, art 33(1); GDPR Parliament version, art 32a.
[484] GDPR Commission and Council version, art 33(3); GDPR Parliament version, arts 33(a), (f), (h), (i), and (j).
[485] GDPR Commission and Council version, art 33(3); GDPR Parliament version, arts 33(b) and (c).
[486] GDPR Commission and Council version, art 33(3); GDPR Parliament version, arts 33(d), (e) and (g).
[487] GDPR Commission and Council version, art 33(4).
[488] GDPR Parliament version, art 33(3b).
[489] GDPR Commission and Council version, art 34(6).
[490] GDPR, art 34.
[491] GDPR Parliament version, art 33a.

2.8 Conclusion: functions of the DPIA in light of the legal analysis

In the introduction, it was hypothesised that the DPIA's functions are to help controllers establish compliance and to help supervisory authorities to hold them to account, i.e. to enforce compliance, and perhaps also to oblige controllers to mitigate risks beyond what is required by the requirements of data protection.[492] However, the possible functions of the DPIA are researched in light of both rights protection and the free flow of information. Below, the functions of the DPIA are therefore discussed around the following four categories: achieving compliance and thus preventing non-compliance, accountability, mitigation of risks to rights and freedoms, and the free movement of information. The focus is on what is legally possible. Section 3.5 of next chapter will discuss what this entails from a regulatory perspective, e.g. whether controllers are likely to use the DPIA in the manner envisaged below. In the absence of enforceable requirements on the evaluation and mitigation of risks, legal scholars might consider the function of the DPIA to be limited to a compliance review. However, with regard to additional risk mitigation, DPIA can still fulfil a function – but it is not captured in the paradigm of command-style regulation.

2.8.1 Achieving compliance, preventing non-compliance

The DPIA's function can be to help controllers achieve compliance with regard to a future project - or, in other words, to prevent non-compliance. Firstly, the DPIA provides a mechanism through which they can establish whether the envisaged processing operation would be in line with the GDPR. This may lead to the decision to change or abandon the project. The DPIA requires controllers to give a description of the envisaged processing operations,[493] which helps them get an overview of what they are doing. This is especially so in the Parliament version, which also requires a description of the purposes of the processing, the legitimate interests of the controller, the time limits for erasure of the data, a list of recipients of the data, and a list of intended third country transfers.[494] In the other versions, these descriptions must be given as part of the duty to keep records –[495] but as part of the DPIA, one report provides a complete overview before the processing is started. These elements all relate to a requirement of data protection law, so their description can help controllers establish whether they will be compliant. More generally, the DPIA also is an assessment of the compliance with the GDPR. In the Commission and Council versions, Article 33(1) requires an assessment of 'the impact of the envisaged processing operations on the protection of personal data', which appears to refer to the protection of personal data as laid down in GDPR.[496] The Parliament refers instead to the right to the protection of personal data,[497] but this also requires an assessment of the data protection principles included Article 8(2) of the Charter under a permissive conceptualisation.[498] In all three versions, the risks to the rights and freedoms – which include the data subject rights of the GDPR – must be analysed.[499] These assessments therefore are or contain compliance checks.

---

[492] Section 1.2.
[493] GDPR, art 33(3).
[494] GDPR Parliament version, arts 33(3)(a), (f), (h), and (i).
[495] GDPR Commission and Council version, art 28.
[496] Section 2.4.2.
[497] GDPR Parliament version, art 33(1).
[498] Sections 2.4.2 and 2.4.1.3.
[499] GDPR Commission and Council version, art 33(3); GDPR Parliament version, art 33(3)(c).

Secondly, by requiring these assessments, the DPIA brings controllers one step closer to actually achieving compliance. The risk analysis and the risk assessment, which entail that the risks are identified and evaluated,[500] will give them a much needed understanding of the likely impact of the processing. As described at the start of section 2.5.2.1., many data protection requirements need the controller to understand and weigh the possible impact of the processing: e.g. the ground of legitimate interest, the compatibility test, and the need to address risks to data security. The Parliament version also includes an assessment of the necessity and proportionality, and of the context.[501] These assessments need to be conducted anyway to adhere to a number of requirements, including to process only what is 'adequate, relevant and limited to the minimum necessary'.[502] By obliging controllers to make them, they are one step closer to achieving compliance; to ensure that the processing is lawful, proportionate, and in line with the principle of purpose limitation.

Next to the required assessments of the impact on the (right to) the protection of personal data, Article 33 requires controllers to identify measures to ensure the protection of personal data.[503] The requirements of data protection law thus need to be translated to the context at hand. Most notably, the DPIA provides a mechanism for controllers to establish what measures need to be taken for data security, how to achieve privacy by design and by default, and how to mitigate risks enough to be able to rely on their legitimate interest as a ground for the processing. The measures envisaged to achieve data minimisation and the measures taken to implement privacy by design and by default explicitly need to be described in the Parliament version.[504] This enables controllers to evaluate whether these measures are sufficient and to assess the remaining level of risk. If taken seriously, the DPIA can help controllers establish what they should do to become compliant.

Moreover, the process of the DPIA and the resulting information may give the data protection officer more of a foothold and enable him to assess and improve the controller's compliance. His involvement may be valuable in helping the controller check whether it conforms to the GDPR and in making the final steps to reach full compliance.

Although it is not a function of the DPIA as such, also less cooperative controllers could be incentivized to prevent non-compliance or to maximise their adherence to the GDPR. If the DPIA points to a high degree of specific risks,[505] or a high risk in the absence of the mitigating measures,[506] then the supervisory authority needs to be consulted. This could be avoided by carrying out a lenient DPIA or by identifying high-reaching solutions if it were not for the fact that, under the Commission and Parliament versions, the supervisory authority can also choose to start a prior consultation if the processing presents any of the risks which are on the list of the supervisory authority or the European Data Protection Board.[507] During the prior consultation,

[500] GDPR Commission and Council version, arts 33(1) and 33(3); GDPR Parliament version, arts 32a and 33(3)(c).
[501] GDPR Parliament version, art 33(b) and (j).
[502] GDPR, art 5(c). See also GDPR, arts 6(1)(b)-(f) and 6(2).
[503] GDPR Commission and Council version, art 33(3); GDPR Parliament version, art 33(3)(e).
[504] GDPR Parliament version, art 33(3)(b) and (g).
[505] GDPR Commission and Parliament version, art 34(2)(a).
[506] GDPR Council version, art 34(2).
[507] GDPR Commission and Parliament version, art 34(2)(b).

the supervisory authority can give advice[508] or make proposals,[509] and issue warnings.[510] This advice is not binding, but the controller might be inclined to accept it: if the supervisory authority finds that the risks are not sufficiently addressed, it can prohibit the non-compliant processing.[511] Under the Parliament version, a prior consultation is only required if there is no data protection officer.[512] This weakens the control of the supervisory authority. But it can still negotiate with the controller on intended processing operations under the treat of a prohibition,[513] even if it is not called a prior consultation. All these situations are subject to the caveat that, unless the controller or its data protection officer comes forward, the supervisory authority may find it difficult to gain the knowledge that a controller is planning to start a risky processing operation. It has investigatory powers, but it cannot keep an eye on everyone all the time. However, the preventive measures are supplemented by the power to prohibit and fine violations of the GDPR,[514] which may inspire controllers to keep their data processing in check just in case they will be detected.

Non-compliance is also prevented if the supervisory authority comes to prohibit or limit the processing before it is started. It has this power on the basis of Article 34(3) and can exercise it when the processing would not comply with the GDPR –[515] as may have been established during the prior consultation. The DPIA's function in this regard is to signal when a prior consultation is required[516] and to provide information on the risks which are posed by the processing operation.

2.8.2 Enforcement and accountability

Accountability and enforcement can be enhanced by the DPIA in multiple ways. Accountability is about adopting and implementing the appropriate measures to achieve effective data protection (the requirement of efficiency, which is discussed above under the heading of compliance), and being able to demonstrate that such measures have been taken (the requirement of transparency).[517] The Article 29 Working Party considers it essential that certain organisational measures are taken, including the establishment of internal procedures prior to the creation of new personal data processing operations, and, in specific circumstances, the performance of impact assessments.[518] The impact assessment is therefore a constitutive element of accountability.[519]

Firstly, the DPIA can help controllers to be accountable. It asks controllers to identify measures to demonstrate their compliance.[520] Article 22 requires controllers to be able to demonstrate that their processing operations are compliant with the GDPR, so technically this helps controllers be compliant. More importantly, though, it helps them to ascertain how they can reach the required transparency.

---

[508] GDPR Council version, rec 74 and arts 34(2) and (3).
[509] GDPR Commission and Parliament version, rec 74.
[510] GDPR Commission and Parliament version, art 53(1)(e); GDPR Council version, arts 34(3) and 53(1b)(a).
[511] GDPR, art 34(3).
[512] GDPR, art 34(2).
[513] GDPR, art 34(3).
[514] GDPR Commission and Parliament version, arts 53(1)(g) and 79; GDPR Council version, arts 53(1b)(e) and 79a.
[515] GDPR, art 34(3); GDPR Council version, art 53(1b)(e).
[516] GDPR Commission and Parliament version, art 34(2)(a); GDPR Council version, art 34(2).
[517] GDPR, art 22; GDPR Parliament version, rec 60; PIAF (2012), 16.
[518] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP173, 2010) 13 and 41.
[519] PIAF (2012) 16.
[520] GDPR Commission and Council version, art 33(3); GDPR Parliament version, art 33(3)(e).

The DPIA can also help supervisory authorities hold controllers to account before and after the processing has started. Documentation of the DPIA is one of the ways in which the controller is required to be transparent. The DPIA report can help supervisory authorities to find instances of non-compliance. In the Commission version, the DPIA always has to be given to the supervisory authority.[521] This enables the supervisory authority to keep an eye on the processing which is planned or occurring within its jurisdiction. But even if it is only provided on request[522] it is still a document which provides information on the processing operation and its risks. The supervisory authority can look into the report if it gets suspicious. If the report is more or less reliable, it will provide the supervisory authority with knowledge of the processing operation, thereby enabling him to determine whether or not to use his investigative powers to look further into a certain project. The report might even contain enough information to establish that the processing is or would be very risky or in violation of the GDPR. The Council version does not provide this function, though. The DPIA is only provided when a prior consultation takes place.[523] The supervisory authority would thus need to start a prior consultation to look into the DPIA, but it can only do so if it knows that the DPIA points to high risks.[524] The data protection officer, who needs to be involved with the DPIA,[525] could inform the supervisory authority whether this is the case, but might not always be relied on to do so. This is a loophole which the final GDPR should avoid.

Moreover, victims can use the DPIA report to hold controllers to account ex post. It is evidence of the scope of the processing operation and of the knowledge of the controller. Controllers may be liable for (non-pecuniary)[526] damage resulting from unlawful processing[527] or from 'an action incompatible with this Regulation'.[528] The GDPR's system of liability is culpability-based and the burden of proof lies with the controller.[529] The controller may be able to escape liability if it can show that it was not aware of the risk. The DPIA report may be used to counter such claims if the court grants the plaintiff access to the report. If a publication requirement had been included in the GDPR, the DPIA report could also provide a form of transparency and accountability towards the public regarding the trade-offs which were made and the level of protection which was aimed for.[530] Unfortunately, the EU legislators have not grasped this opportunity. It is therefore limited to fulfil an evidentiary function in light of claims which came to light through other channels.

2.8.3 Additional risk mitigation

The DPIA can result in the mitigation of risks beyond what is required to be technically compliant with the requirements of the GDPR. Many of the principles of data protection include a concern for the risks to the rights and freedoms of individuals, so compliance and risk mitigation overlap. However, compliance with data protection law does not mean that the

521 GDPR Commission version, art 34(6).
522 GDPR Parliament version, art 34(6).
523 GDPR Council version, art 34(6)(e).
524 GDPR Council version, art 34(2).
525 GDPR Council version, art 33(1b).
526 GDPR Parliament version, art 77(1); GDPR Council version, art 77(1).
527 GDPR Council version, arts 77(1) and (2).
528 GDPR Commission and Parliament version, art 77(1).
529 GDPR Commission and Council version, art 77(3); L Costa (2012).
530 cf Weber (2014) 296.

processing cannot harm or (if the controller is bound to respect them) violate rights and freedoms, despite the ancillary nature of data protection and the accompanying right.[531] The GDPR does not contain a general, explicit duty to address these risks.[532] It is therefore possible that compliant processing poses risks to the rights and freedoms. The impact assessment serves not only to prevent compliance issues, but also to make companies aware of the consequences of their projects from the outset so that 'the likelihood of any data breach or privacy-intrusive operation can be fundamentally limited'[533] and other risks to rights and freedoms can be mitigated.

Controllers must engage in a risk analysis[534] and, if this points to specific or high risks to the rights and freedoms of data subjects[535] or individuals,[536] - in the Parliament version: by virtue of belonging to one of the specified categories of processing -¯ they must also conduct an assessment of these risks.[537] This should raise awareness of the possible negative effects of their processing. As argued in section 2.4.2, the DPIA sees to the potentially boundless category of rights and freedoms. It should lead controllers to assess not only the likelihood of data breaches and the control of data subjects over their data,[538] but also the impact of the way in which they use personal data on the equality, freedom of expression and freedom of thought of individuals.[539] The reference to "individuals" in the Council version means that the controller should also look at how the processing impacts people who are not included in the dataset or who are not identifiable. But the difference may be negligible, because it should also look at how the processing affects individuals who may become identifiable or whose information may be collected in the future under the Commission and the Parliament version. It needs to establish what may cause data subjects to be adversely affected (origin), whether the personal data is sensitive (nature), how many data subjects could be affected (scope), and how severe and likely these adverse affects are.[540] Moreover, because it must identify measures to address the risks,[541] it also need to look for ways to avoid, minimise or mitigate these risks. This awareness alone might incentivise them to address these risks above and beyond what compliance with the GDPR requires.

This requires quite a lot of faith in controllers. They need to not only identify and analyse high risks properly, but also take responsibility for these possible consequences of their actions. As noted by De Hert and Papakonstantinou, 'one could not avoid thinking that great expectations for data controllers' responsible behaviour are made'.[542] There is little to guide controllers. It was shown in section 2.5.2.1 that there is not a set level of protection and precaution of the rights and freedoms of individuals which must be reached. The controller must decide when a threat is so severe and likely that it needs to be addressed; what level of knowledge or

[531] Section 2.4.1.4.
[532] Section 2.5.2.
[533] GDPR Parliament version, rec 71a.
[534] GDPR Commission and Council version, art 33(1); GDPR Parliament version, art 32a.
[535] GDPR Commission and Parliament version, art 33(1).
[536] GDPR Council version, art 33(1).
[537] GDPR Commission and Council version, art 33(3); GDPR Parliament version, art 33(3)(c).
[538] cf GDPR Parliament version, rec 71a.
[539] cf Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' 4.
[540] GDPR Commission and Council version, art 33(1); GDPR Council version, rec 60c; Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' 4.
[541] GDPR Commission and Council version, art 33(3); GDPR Parliament version, art 33(3)(d).
[542] De Hert and Papakonstantinou (2012) 141.

agreement is necessary for the risk to be assigned a certain severity and likelihood; and what level of protection the measures should achieve. The GDPR and the Article 29 Working Party specify how the risk should be assessed – taking into account the nature, context, scope and origin of the processing[543] and by conducting a stakeholder consultation -[544] but not what level of protection and precaution should be aimed for. In other words, Article 33 does not require the controllers to reach high; it only provides for methodological requirements. The GDPR lacks a general duty to address risks which could set the level of protection, although it could be constructed on the basis of privacy by design and by default or the principle of fair processing and, particularly with regard to governmental entities, on the basis of the principle of proportionality. Governmental entities are under a duty to prevent risks to fundamental rights and freedoms insofar as this would constitute a violation; they need to prevent disproportionate interferences. However, this duty does not fully extend to non-governmental entities, which are, at most, under a moral duty to interpret the DPIA system in line with its spirit of risk mitigation.[545] The controller must thus set the norms regarding the level of protection and precaution during the risk assessment by itself or with the data protection officer, if there is one –[546] and may be inclined to set them low. Moreover, the Commission and the Council do not require controllers to actually implement the measures which were identified. The Parliament does require the measures to be undertaken, and requires that this is demonstrated in a compliance review.[547] However, because there is no set level of protection, these measures do not actually need to mitigate risks to the rights and freedoms of individuals.

There is little to guide controllers, but there is some push. As discussed above, the DPIA report has to be sent to the supervisory authority always (Commission) on request (Parliament) or as part of a prior consultation (Council). The compliance review is also documented and is accessible to the supervisory authority on request.[548] This may lead to a prior consultation, during which the controller may be persuaded to adopt certain measures under the shadow of a possible prohibition. Such agreements might be enforceable under the Commission and Parliament versions.[549] Moreover, the processing might be put to and end. The GDPR does not clarify whether processing operations which are risky, but compliant, can be prohibited or limited. [550] As a result, it is up to Member States to decide whether such a broad discretion is compatible with the principle of legality and the freedom to conduct a business of controllers for the sake of the rights protection which it could bring.[551] A similar balancing act should be conducted for the non-preventive power to prohibit[552] or limit[553] processing operations. Furthermore, should a general duty to mitigate risks be constructed, possibly on the basis of privacy by design and by default, supervisory authorities would be able to issue sanctions for insufficient risk mitigation under the Parliament version. The power to sanction risky processing

[543] GDPR Commission and Council version, art 33(1); GDPR Council version, rec 60c; Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' 4.
[544] GDPR Commission and Council version, art 33(4).
[545] Sections 2.5.2.1, 2.5.2.2 and 2.6.1.2.
[546] GDPR Commission version, art 37(1)(f); GDPR Parliament version, arts 33(3a) and art 33a(5); GDPR Council version, art 33(1a).
[547] GDPR Parliament version, rec 74a and art 33a(1).
[548] GDPR Parliament version, art 33a(4).
[549] GDPR Commission and Parliament version, art 53(1)(d).
[550] GDPR, art 34(3); GDPR Council version, art 53(1b)(e).
[551] Section 1.6.1.2.
[552] GDPR Commission and Parliament version, art 53(1)(g).
[553]GDPR Council version, art 53(1b)(e).

operations is clearly not provided for in the Commission and Council version, which prescribe the violations which can be sanctioned,[554] but the Parliament version empowers supervisory authorities to sanction all sorts of non-compliance.[555] Lastly, the controller might face liability for (non-pecuniary)[556] damages arising from its conduct.[557] While the Council version only provides for liability for damages resulting from acts of non-compliance, the Commission and the Parliament version include the broader category of 'an action incompatible with this Regulation'.[558] Although there is no explicit duty to mitigate risks, it is incompatible with the DPIA system not to mitigate risks at all – opening up the possibility of a liability claim if risks are not sufficiently addressed. National tort law can be more expansive.

Risk mitigation has another function from the perspective of the legislator: to cope with technological turbulence. The legislator cannot foresee and address everything. The law can become outdated and leave the harm posed by technological developments unregulated. As identified by Clarke, Gutwirth and others, the interest in privacy impact assessments is part of the trend to attempt to manage possible, yet unpredictable future threats of new technologies before actual harm occurs.[559] Stewart sees the impact assessment 'as one of the most flexible and promising techniques for grappling with ever variable privacy challenges of our complex times'.[560] Through its function of risk mitigation, the DPIA provides a solution to the fact that existing laws may not adequately cover changed circumstances and new technologies. It does so by stimulating controllers to mitigate risks even if the legislator did not clearly prescribe this. Guidance documents are more easily adapted than legislation; they can be used to guide controllers in their choices throughout technological turbulent times. While there is no way to ensure that the controller mitigates risks in the manner which the legislator would have prescribed, if it had had the foresight, stakeholders can help guide the political choices.[561] By seeking the views of data subjects or their representatives, as required by the Commission and the Council,[562] 'community values and expectations about privacy' can be taken into account. The stakeholder consultation could therefore add political legitimacy to decisions which are otherwise unregulated, if carried out properly.[563]

2.8.4 The free movement of information

Next to the protection of the rights and freedoms of individuals, the General Data Protection Regulation also aims to protect the free movement of information.[564] Can the DPIA also fulfil a function in this regard? The Article 29 Working Party has clarified that the risk-based approach is not 'an alternative to well-established data protection rights and principles', but instead 'a

---

554 GDPR Commission version, art 79; GDPR Council version, art 79a.
555 GDPR Parliament version, art 79(2a).
556 GDPR Parliament version, art 77(1); GDPR Council version, art 77(1).
557 GDPR Council version, arts 77(1) and (2).
558 GDPR Commission and Parliament version, art 77(1).
559 R Clarke, 'Privacy impact assessment: Its origins and development' (2009) 25(2) Computer Law & Security Review 123, 129; Wright, Gellert, Gutwirth and Friedewald (2011) 97.
560 B Stewart, 'Privacy Impact Assessment: Optimising the Regulator's Role' in D Wright and P De Hert (eds), *Privacy Impact Assessment* (Springer 2012) 444.
561 Wright, Gellert, Gutwirth and Friedewald (2011) 96.
562 GDPR Commission and Council version, art 33(4). **This is, however, not a hard obligation.** See section 2.5.2.1.
563 L Costa and Y Poullet, 'Privacy and the regulation of 2012' (2012) 28(3) Computer Law & Security Review 254, 260. See also A Warren and others, 'Privacy Impact Assessments: international experience as a basis for UK Guidance' (2008) 24(3) Computer Law & Security Report 233, 235.
564 GDPR, art 1.

scalable and proportionate approach to compliance'.[565] It does not allow low-risk data processing operations to be conducted free from the constraints of data protection law. However, fundamental principles of data protection law have regard to the nature and scope of processing, which makes them inherently scalable. The accountability obligations are scalable, too: they do not need to be implemented as fully if the processing is small-scale, simple and low-risk,[566] while processing which presents specific risks must be subject to additional measures.[567] The DPIA permits controllers to assess how extensive their accountability and compliance mechanisms should be.[568] As a result, the DPIA cannot increase the free flow of information by weakening the GDPR's requirements, but it can help controllers assess the extent of those constraints.

At the same time, the continuance of the free flow of information is safeguarded by helping controllers achieve a right level of protection from the start. The DPIA may prevent violations of data protection law, liability for damages arising from the processing, or violations of fundamental rights and freedoms, all of which could lead to a stop on the processing. According to the ICO, the purpose of the impact assessment is 'to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible'.[569] Processing operations do not need to be abandoned if the level of risk is acceptable or if the risks can be avoided or mitigated. How constraining of data processing this is, depends on the level of protection which is strived for. Similarly, under a more precautionary approach to the knowledge condition (when is a risk known), the free flow of information is more limited, but under a less precautionary approach, potential threats are less quickly reason to abandon or adapt the processing operation. Moreover, if controllers make sure that data processing does not present too much harm to individuals and to society as a whole, the EU does not need to intervene with more strict regulation.[570]

[565] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', 2.
[566] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', 3.
[567] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', 4.
[568] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', 2-3.
[569] ICO (2014) 5.
[570] **Although the threat of state intervention may not actually be present, see sections 3.3.3, 3.4.2.2 and 3.5.3.**

2.9 Full table comparing the different versions

	Commission	Parliament	Council
Risk threshold			
When is a DPIA required?	If the processing presents *specific risks* to the rights and freedoms of *data subjects*.	If the processing is likely to present *specific risks* to the rights and freedoms of *data subjects* by virtue of falling within the categories described in *Article 32a(2)(a)-(h).*	If the processing is likely to result in *high risks* to the rights and freedoms of *individuals*.
Is the initial risk analysis a continuing obligation?	Not clear.	Yearly review + if nature, scope or purposes change significantly.	Not clear: if necessitated by "the lapse of time".
Can multiple projects be can assessed together?	Yes, e.g. shared applications or platforms.	Yes, if similar processing operations present similar risks.	Yes.
Is there an exception if the processing is legally required or necessary to carry out public task?	Yes.	No.	Yes.
Does "risk" mean threat x probability?	Not clear: probability may not need to be known.	Not clear: probability may not need to be known.	Yes, both elements must be known. How precautionary this is depends on the knowledge condition.
What counts as risky?	Any risk to any right or freedom. See also Article 29 Working Party: privacy, freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination (...).	Any risk to any right or freedom. See also Article 29 Working Party: privacy, freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination (...).	Any risk to any right or freedom, e.g. discrimination, identity theft or fraud, financial loss, damage to the reputation (...). See also Article 29 Working Party.
How to assess riskiness?	Processing operations may pose risks by virtue of their nature, their scope or their purposes. See also Article 29 Working Party (→).	Article 29 Working Party: Risks must be assessed taking into account specific objective criteria, such as the nature of personal data, *the category of data subject*, the number of data subjects affected, and the purpose of the processing. The legitimate interests of the controller should not be taken into account.	Risks must be assessed taking into account the nature, scope, purposes and the *context* of the processing and in terms of their origin, nature, likelihood and severity. See also Article 29 Working Party (←).
Which types of processing are risky in essence?	Medium list, see Article 33(2). Supervisory authority must also make a list. The Commission can also specify criteria and conditions.	Long and broad, but exhaustive, list. See Article 32a(2). European Data Protection Board must make an additional list.	Short list, see Article 33(2). Supervisory authority must also make a list.
Duty bearer			
	Processor or controller	Processor or controller	Controller
Subject matter			
	Impact on the protection of personal data - but also an assessment of the risks to the rights and freedoms of data subjects.	Impact on the rights and freedoms of the data subjects, especially their *right to* protection of personal data (which should include a compliance review) - but also an assessment of the risks to the rights and	Impact on the protection of personal data - but also an evaluation of the *high* risks to the rights and freedoms of *individuals.*

		freedoms of data subjects.	
Required output			
	A description of the processing, an assessment of the risks, and the *identification/description(?)* of measures envisaged to address the risks, *and/including(?)* safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.	A description of the processing, an assessment of the risks, a *description* of measures envisaged to address the risks, *and* a list of safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR + a large number of other descriptions and assessments which relate to other data protection requirements (see Article 33(3).	A description of the processing, an assessment of the risks, and the *identification/description(?)* of measures envisaged to address the risks, *including* safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.
Are there legal standards on the level of protection and precaution which must be aimed for (e.g. when does something count as risky, when is a risk known, when are remedies sufficient)?	No. There are only methodological requirements on how to assess riskiness and a soft duty to seek the views of data subjects or their representatives.	No. There are only methodological requirements on how to assess riskiness.	No. There are only methodological requirements on how to assess riskiness and a soft duty to seek the views of data subjects or their representatives.
Is there a duty to take the envisaged mitigating measures?	No.	Yes. The controller has to carry out a compliance review and demonstrate that the measures described in the DPIA are taken.	No.
Can privacy by design and by default form a duty to mitigate risks to the rights and freedoms of data subjects/individuals and reach a certain level of protection?	Maybe, it also sees to protection of the rights of the data subject.	Maybe, it also sees to protection of the rights of the data subject. However, this is principally in relation to the principles of Article 5.	Maybe, it also sees to protection of the rights of the data subject. However, this sees to transparency and user control and is to meet the 'data protection obligations'.
Who can provide further guidance on the DPIA?	Supervisory authorities, the European Data Protection Board, and the Commission.	Supervisory authorities and the European Data Protection Board.	Supervisory authorities and the European Data Protection Board
The prior consultation			
When is a prior consultation required?	If the DPIA indicates that the processing is likely to present a high degree of specific risk.	If the DPIA indicates that the processing is likely to present a high degree of specific risk. The supervisory authority only needs to be consulted if there is no data protection officer.	If the DPIA indicates that the processing *would result* in a *high* risk *in the absence of measures to be taken by the controller to mitigate the risk.*
Can the supervisory authority start a prior consultation in other cases?	Yes, if it deems it necessary with regard to the risks specified on the list of the supervisory authority.	Yes, if it deems it necessary with regard to the risks specified on the list of the European Data Protection Board.	No.
Does the supervisory authority have access to the DPIA report?	Yes, it must always be provided.	Yes, the supervisory authority can request it.	Yes, it must be provided if a prior consultation takes place.
Can the supervisory authority give advice?	Yes, it can make proposals to remedy non-compliance and warn or admonish the controller.	Yes, it can make proposals to remedy non-compliance and warn or admonish the controller.	Yes, it can give advice and issue official warnings.

Can the supervisory authority prohibit the intended processing?	Yes, it shall do so if it *is of the opinion* that the intended processing does not comply with the GDPR, in particular where risks are insufficiently identified or mitigated.	Yes, it shall do so if it *determines in accordance with its power* that the intended processing does not comply with the GDPR, in particular where risks are insufficiently identified or mitigated.	It can make use of its powers, including a temporary or definitive limitation on the processing, if it is *of the opinion* that the intended processing *would* not comply with the GDPR, in particular where *the controller has* insufficiently identified or mitigated the risk.
Is there a time limit?	No.	No.	Yes, the supervisory authority should use its powers within a period of 6 weeks, to be extended by another 6 weeks.
Can compliance with the prior consultation be enforced?	Yes.	Yes.	No.
Sanctions			
Can processing still be stopped after it has commenced?	Yes, it can be prohibited.	Yes, it can be prohibited.	Yes, it can be limited.
Can or must the controller be fined?	Yes. The GDPR specifies which acts of non-compliance are subject to what fines. Failing to carry out a DPIA or skipping the prior consultation *must* be fined, although a warning may be given instead in case of a first and non-intentional non-compliance if the processing is carried out by a natural person without a commercial interest or by a SME which processes personal data as an ancillary activity.	Yes. Any act of non-compliance *must* be sanctioned, but the supervisory authority can choose between 1) a warning in cases of first and non-intentional non-compliance, 2) regular periodic data protection audits, and 3) a fine.	Yes. The GDPR specifies which acts of non-compliance are subject to what fines. Failing to carry out a DPIA or skipping the prior consultation *can* be fined.
What is the height of the fine?	A maximum of 1 million Euros or, if the controller or processor is an undertaking, *2 %* of the total worldwide annual turnover of the preceding financial year.	A maximum of 1 million Euros or up to *5%* of the annual worldwide turnover in case of an enterprise, whichever is higher.	A maximum of 1 million Euros or, if the controller or processor is an undertaking, *2 %* of the total worldwide annual turnover of the preceding financial year.
Liability			
	Any person who suffered damage as a result of an unlawful processing operation or *an action incompatible with the GPDR* has the right to *receive* compensation for the damage.	Any person who suffered damage, *including non-pecuniary damage*, as a result of an unlawful processing operation or *an action incompatible with the GPDR* has the right to *claim* compensation for the damage.	Any person who suffered *material or immaterial* damage as a result of a processing which is *not in compliance with the GDPR* has the right to *receive* compensation for the damage.
	The controller or processor is liable unless it proves that it is not responsible for the event which gave rise to the damage.	The controller or processor is liable unless it proves that it is not responsible for the event which gave rise to the damage. (The Parliament did not clearly include nor reject this provision)	The controller or processor is liable unless it proves that it is not responsible for the event which gave rise to the damage.

Sources

Cases

ABRvS 4 July 2007, ECLI:NL:RVS:2007:BA8742

Amann v Switzerland (2000) 30 EHRR 843

Case C-4/73 *J Nold, Kohlen- und Baustoffgroßhandlung v Ruhrkohle Aktiengesellschaft* [1977] ECR 00491

Case C-101/01, *Bodil Lindqvist* [2003] ECR I-12971

Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I-00271

Case C-45/08 *Spektor Photo Group NV v Commissie voor het Bank, Financie- en Assurantiewezen* [2009] I-12073

Case C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH* [2009] ECR I-01227

Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeur SCRL (SABAM)* [2011] ECR I-11959

Case C-543/09 *Deutsche Telekom AG v Bundesrepublik Deutschland [*2011] ECR I-03441

Case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)* v *Netlog* [2012] 2 CMLR 18

Case C-461/10 *Bonnier Audio AB and Others v Perfect Communication Sweden AB* (ECJ, 19 April 2012)

Case C-426/11 *Alemo-Herron v Parkwood* [2014] 1 CMLR 21

Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos (AEPD)* (ECJ, 13 May 2014)

Case C-314/12 UPC *Telekabel Wien GmbH v Constantin Film Verleih GmbH* (ECJ, 27 March 2014)

Common Services Agency v Scottish Information Commissioner [2008] UKHL 47

Engel and Others v the Netherlands (2008) Series A no 22

Hoge Raad 9 September 2011 ECLI:NL:HR:2011:BQ8097

Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof v Österreichischer Rundfunk* [2003] ECR I-04989

Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR v Land Hessen* [2010] ECR I-11063

Joined Cases C-468/10 and C-469/10, *ASNEF* [2011] ECR I-12181

Klass and others v Federal Republic of Germany (1978) 2 EHRR 214

Menarini Diagnostics s.r.l. v. Italy App no 43509/08 (ECtHR 27 September 2011)

Öztürk v Germany (1984) Series A no 73

P.G. and J.H. v the United Kingdom App no 44787/98 (ECtHR 4 September 2001)

Rotaru v Romania (2000) IHRL 2923

Tadeusz Matyjek v Poland App no 38184/03 (ECtHR 30 May 2006)

X and Y v. The Netherlands, A. 8978/80, 26 March 1985

Soft law and literature

Agre P, 'Introduction' in Agre P and Rotenberg M (eds), *Technology and Privacy: the New Landscape* (MIT Press 1998)

de Andrade N, 'Oblivion: The Right to Be Different.. from Oneself. Reproposing the Right to Be Forgotten' (2012) 13 Revista de los Estudios de Derecho y Ciencia Política de la UOC 122

Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP173, 2010)

——, 'Opinion 15/2011 Consent' (WP197, 2011)

——, 'Opinion 01/2012 on the data protection reform proposals' (WP191, 2012)

——, 'Opinion 03/2013 on purpose limitation' (WP203, 2013)

——, 'Opinion 26/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (WP217, 2014)

——, 'Statement on the role of a risk-based approach in data protection legal frameworks' (WP218, 2014)

Baldwin R; Cave M and Lodge M, *Understanding Regulation: Theory, Strategy and Practice* (Oxford University Press 2012)

Black J, Hopper M and Band C, 'Making a success of Principles-based regulation' (2007) 1(3) Law and Financial Markets Review 191

Black J and Baldwin R, 'Really Responsive Risk-Based Regulation' (2010) 32(2) Law & Policy 181

Borgesius F, 'Improving privacy protection in the area of behavioural targeting' (PhD thesis, University of Amsterdam 2014)

Butin D, Chicote M and Le Métayer D, 'Strong Accountability: Beyond Vague Promises', in Gutwirth S, Leenes R and De Hert P, *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014)

Clarke R, 'Privacy impact assessment: Its origins and development' (2009) 25(2) Computer Law & Security Review 123

Commission nationale de l'informatique et des libertés (CNIL), 'Privacy Impact Assessment (PIA): Methodology (how to carry out a PIA)' (2015)

Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century' COM(2012) 9 final

——, Communication from the Commission on the precautionary principle, COM (2000) I

Costa L, 'Privacy and the precautionary principle' (2012) 28(1) Computer Law & Security Review 14

Costa L and Poullet Y, 'Privacy and the regulation of 2012' (2012) 28(3) Computer Law & Security Review 254

Davies S, 'Why Privacy by Design is the next crucial step for privacy protection' (2010) <www.i-comp.org/wp-content/uploads/2013/07/privacy-by-design.pdf> accessed 11 September 2015.

European Union Agency for Fundamental Rights, Freedom to conduct a business: exploring the dimensions of a fundamental right (Publications Office of the European Union 2015)

Di Federico G, 'Fundamental Rights in the EU: Legal Pluralism and Multi-Level Protection After the Lisbon Treaty' in Di Federico G (ed), *The EU Charter of Fundamental Rights: From Declaration to Binding Instrument* (Springer 2011)

European Parliament, 'Personal data protection in the European Union: European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union' P7_TA(2011)0323

Finn R, Rodrigues R and Wright D, 'A Comparative Analysis of Privacy Impact Assessment in Six Countries', (2013) 9(1) Journal of Contemporary European Research 161

Gavison R, 'Privacy and the Limits of Law' (1980) 89 Yale Law Journal 421

Gellert R and Gutwirth S, 'The legal construction of privacy and data protection' (2013) 29(5) Computer Law & Security Review 522

Gewirth A, 'Are there any absolute rights?' in Waldron J, *Theories of Rights* (Oxford University Press 1981)

González Fuster G and Gutwirth S, 'Opening up personal data protection: a conceptual controversy' (2013) 29(5) Computer Law & Security Review 531

González Fuster G, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014)

Gribnau H, 'Corporate Social Responsibility and Tax Planning: Not by Rules Alone' (2015) 24(2) Social & Legal Studies 225

Gürses S, 'Multilateral Privacy Requirements Analysis in Online Social Networks' (PhD thesis University of Leuven, 2010)

Happé R, 'Belastingrecht en de geest van de wet: Een peidooi voor een beginsel-benadering in de wetgeving' (inaugural lecture, Tilburg University 2011)

De Hert P and Gutwirth S, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in Claes E, Duff A and Gutwirth S (eds), *Privacy and the criminal law* (Intersentia 2006)

De Hert P and Gutwirth S, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Gutwirth S and others (eds), *Reinventing Data Protection?* (Springer 2009)

De Hert P, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments', in Wright D and De Hert P (eds), Privacy Impact Assessment (Springer 2012)

De Hert P and Papakonstantinou V, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28(2) Computer Law & Security 130

Hildebrandt M, 'Who needs stories if you can get the data? ISPs in the era of big number crunching' (2011) 24(4) Philosophy & Technology 371

Information Commissioner's Office (ICO), 'Conducting privacy impact assessments: code of practice' (2014) < https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/> accessed 15 August 2015

——, 'The Guide to Data Protection' (version 2.2.4, 31 March 2015) <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/> accessed 25 August 2015

Kamerstukken II 1997-1998, 25892, nr. 3

Kamerstukken II 2011/12, 33 079, nr. 3

Kindt E, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer 2013)

Lessig L, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harvard Law Review 501

Manson N, 'Formulating the Precautionary Principle' (2002) 24 Environmental Ethics 263

Moerel L, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof?' (inaugural lecture 2014)

Moerel L and Prins C, 'Further processing of data based on the legitimate interest ground: the end of purpose limitation' TILT website (2015)

Nollkaemper A, *Kern van het internationaal publiekrecht* (Boom 2009)

Oetzel M and Spiekermann S, 'A systematic methodology for privacy impact assessments: a design science approach'(2014) 23 European Journal of Information Systems 126

O'Malley P, *Risk, Uncertainty and Government* (Glasshouse Press 2004)

Peers S, Hervey T, Kenner J and Ward A (eds), *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2014)

PIAF, 'A Privacy Impact Assessment Framework for data protection and privacy rights: Deliverable D1' (2011)

——, 'Deliverable D3: Recommendations for a Privacy Impact Assessment Framework for the European Union' (2012)

Pocs M, 'Will the European Commission be able to standardise legal technology design without a legal method?' (2012) 28(6) Computer Law & Security Review 641

Praesidium of the European Convention, 'Presidency Note: Draft Charter of Fundamental Rights of the European Union - Complete text of the Charter proposed by the Praesidium' (CHARTE 4422/00 CONVENT 45, 2000)

——, 'Explanations relating to the Charter of Fundamental Rights' (2007/C 303/02)

PRESCIENT, 'Deliverable D1: 'Legal, social, economic and ethical conceptualisations of privacy and data protection' (2011)

——, 'Deliverable 4: Final Report – A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies' (2013)

PRISMS, 'Deliverable 5.1: Discussion paper on legal approaches to security, privacy and personal data protection' (2013)

PRISMS, 'Deliverable 5.2: Consolidated legal report on the relationship between security, privacy and personal data protection in EU law' (2014)

Reinisch A, 'The Changing International Legal Framework for Dealing with Non-State Actors', in Alston P, *Non-State Actors and Human Rights* (Oxford University Press 2005)

Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Gutwirth S, Poullet Y, De Hert P, De Terwangne C and Nouwt S (eds), *Reinventing Data Protection?* (Springer 2009)

Rueb A, *Compendium Burgerlijk procesrecht* (Kluwer 2011)

Sandin P, 'Better Safe than Sorry: Applying Philosophical Methods to the Debate on Risk and the Precautionary Principle' (2004) Theses in Philosophy from the Royal Institute of Technology 5

von Schomberg R, 'The precautionary principle and its normative challenges' in Fisher E, Jones J and von Schomberg R (eds), *Implementing the Precautionary Principle: Perspectives and Prospects* (Edward Elgar 2006)

van der Sloot B, 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"' (2015) 31(8) Utrecht Journal of International and European Law 25

Slovic P, 'Perception of Risk Posed by Extreme Events' (New York conference, 2002) Risk management strategies in an uncertain world <https://www.ldeo.columbia.edu/chrr/documents/meetings/roundtable/white_papers/slovic_wp.pdf> accessed 11 September 2015.

Spiekermann S, 'The RFD PIA - Developed by Industry, Agreed by Regulators', in Wright D and De Hert P (eds), *Privacy Impact Assessment* (Springer 2012)

Stewart B, 'Privacy Impact Assessment: Optimising the Regulator's Role' in Wright D and De Hert P (eds), *Privacy Impact Assessment* (Springer 2012)

Tannert C, Elvers H and Jandrig B, 'The ethics of uncertainty. In light of possible dangers, research becomes a moral duty' (2007) 8(10) EMBO reports <ttp://www.ncbi.nlm.nih.gov/pmc/ arts/PMC2002561/> accessed on 15 July 2015

The Council of the European Union, 'Presidency Note: Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Data Protection Impact and Prior Checks' (5880/14 2012/0011(COD), 2014)

Tranberg C, 'Proportionality and data protection in the case law of the European Court of Justice' (2011) 1(4) International Data Privacy Law 239

Varian H, 'Economic aspects of personal privacy' in Lehr W and Pupillo L (eds), *Internet policy and economics* (Springer 2009)

Wadhwa K and Rodrigues R, 'Evaluating privacy impact assessments' (2013) 26 Innovation: The European Journal of Social Science Research 161

Walker N, 'The Idea of Constitutional Pluralism' (2002) 65 Modern Law Review 317

Warren A and others, 'Privacy Impact Assessments: international experience as a basis for UK Guidance' (2008) 24(3) Computer Law & Security Report 233

Warren S and Brandeis L, 'The Right to Privacy' (1890) 4 Harvard Law Review 193

Weber R, 'Symposium on EU Data Protection Reform: Privacy management practices in the proposed EU regulation' (2014) 4(4) International Data Privacy Law 290

Wenar L, 'Rights' (Fall 2011) The Stanford Encyclopedia of Philosophy <http://plato.stanford.edu/archives/fall2011/entries/rights/> accessed 16 August 2015

Westin A, *Privacy and Freedom* (The Bodley Head 1970)

Wright D, 'Should privacy impact assessments be mandatory?' (2011) 54(8) Communications of the ACM 121

Wright D, 'Making Privacy Impact Assessments More Effective' (2013) 29(5) The Information Society: An International Journal 307

Wright D, 'The state of the art in privacy impact assessment' (2012) 28(1) Computer Law & Security Review 54

Wright D, Gellert R, Gutwirth S and Friedewald M, 'Precaution and privacy impact assessment as modes towards risk governance' in von Schomberg R (ed), *Towards Responsible Research and*

Innovation in the Information and Communication Technologies and Security Technologies Field (European Commission 2011)

Wright D and De Hert P, 'Introduction to Privacy Impact Assessment' in Wright D and De Hert P (eds), *Privacy Impact Assessment* (Springer 2012

——, 'Findings and Recommendations' in Wright D and De Hert P (eds), *Privacy Impact Assessment* (Springer 2012

Wynne B, Harremoës P, Gee D and others, *The Precautionary Principle in the 20th Century: Late Lessons from Early Warnings* (Earthscan 2002)

Zanfir G, 'Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law' in Gutwirth S, Leenes R and De Hert P (eds), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2014)

Zarsky T, 'Understanding Discrimination in the Scored Society' (2014) Washington Law Review 89(4)

Zetterquist O, 'The Charter of Fundamental Rights and the European Res Publica' in Di Federico G (ed), *The EU Charter of Fundamental Rights: From Declaration to Binding Instrument* (Springer 2011)

3 The data protection impact assessment from the perspective of regulatory studies

3.1 Introduction

This chapter will analyse the functions of the data protection impact assessment from the perspective of regulatory studies. Section 1.3.2.1 of the Introduction introduced the theoretical framework, under which regulators can steer behaviour not only through command-and-control type rules. Instead, they can make use of the self-regulatory capacity of actors – but are also limited by the (semi-)autonomous nature of systems in society. This framework is expanded in this chapter, as it describes different types of regulation and the strengths and weaknesses they have in respect of their capacity to steer behaviour. Section 3.2 will describe the types of regulation to which the data protection impact assessment could bear resemblance. Next, section 3.3 will analyse which characteristics the DPIA shares with these types of regulation. Then section 3.4 will describe the strengths and weaknesses of the types of regulation with which the DPIA shares characteristics and apply them to the DPIA, to conclude on what functions the DPIA could fulfil in section 3.5.

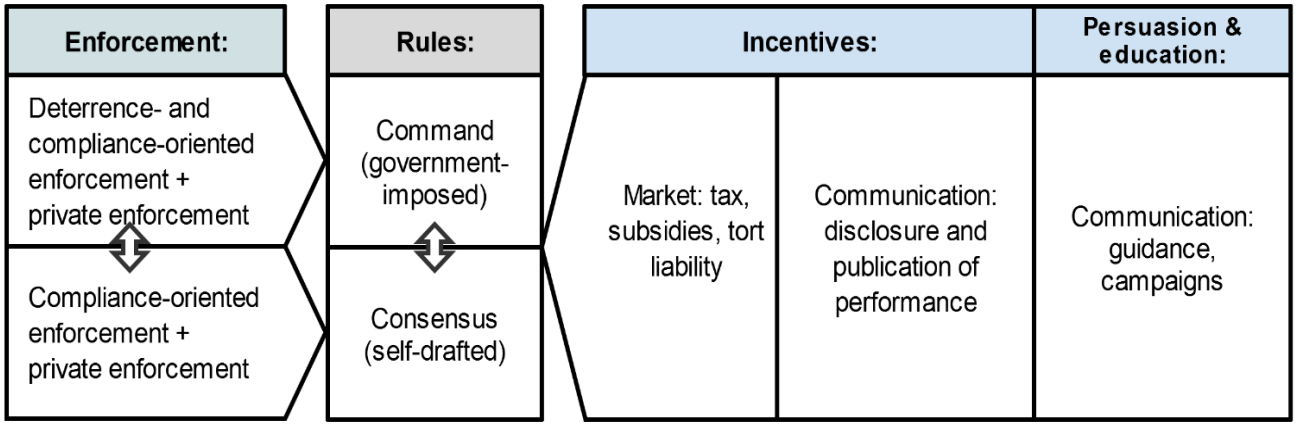
3.2 Types of regulation

Government regulation involves the adoption of policies, rules, tools or other steering mechanisms, which is typically accompanied by enforcement activity.[571] The policies, rules, tools or other steering mechanisms can be characterised on the basis of the modality which is used to steer behaviour, and their enforcement can be captured in a number of types. Regulation can thus be captured on the basis of the modality and the types of enforcement which are used. The different modalities will be discussed in section 3.2.1, after which section 3.2.2 will discuss different types of enforcement. The categories may overlap. For example, a policy can regulate through communication, but regulatory conversations are also a method of enforcement. Tort liability can function as a deterrent through the modality of the market, but is also an enforcement strategy. Nonetheless, the differentiation is a useful heuristic to analyse the data protection impact assessment. Smart regulation and meta-regulation see to both the modalities which are employed and how they are enforced: the first part will be discussed under section 3.2.1, while the accompanying enforcement strategies will be discussed in section 3.2.2.

By way of introduction, the figure below presents the different modalities and their enforcement. Rules can be more or less imposed by the government (the modality of law or command) or self-drafted (the modality of consensus). Other modalities of regulation are the market and communication, which can also incentivize or persuade regulatees to adhere to certain rules. For example, if the required conduct can offer a tax break or if compliance records are made public, the regulatee is incentivized to adhere to the rule. The diagram does not show that regulation which uses the market or communication may harness these modalities through rules; disclosure, for example, can be mandatory. Rules can be enforced by public authorities through deterrence- and compliance-oriented approaches and through public enforcement. However, deterrent approaches are only available if violation of the rule can be sanctioned by

[571] cf the DREAM framework in R Baldwin; M Cave and M Lodge, *Understanding Regulation: Theory, Strategy and Practice* (Oxford University Press 2012) 227; R Baldwin and J Black, 'Really Responsive Regulation' (2007) LSE Legal Studies Working Paper No. 15/2007. **Other steps in the regulatory process are the assessment of the success of these rules and enforcement activities and their modification, but these fall outside the scope of this thesis.**

the enforcement agency, which, due to the principle of legality, is typically only the case if the rule is imposed by the state. The modality and the type of enforcement are connected.



3.2.1 Modalities of regulation

3.2.1.1 Categorisations

As discussed under section 1.3.2.1, government regulation can steer people directly or indirectly. Regulation can take place through different modalities, of which regulation through prescriptive rules is probably most familiar to the lawyer. Lessig identified the modalities of law, social norms and social institutions, the market, and architecture or code; each of these regulate the behaviour of individuals.[572] Taking the example of teenage smoking, these modalities may work as follows. The law, or more precisely the command, orders people to behave in certain ways and threatens with punishment if they don't obey: if a shop sells cigarettes to minors it will be issued a fine. Social norms also regulate and may be enforced by the community, e.g. passers-by may tell teenagers that it is stupid to smoke and smokers may be excluded from certain social groups. The market operates within the boundaries of the law and social norms and regulates through price. The more expensive cigarettes are, the more teenagers may not be able to smoke because of the cost. Architecture and code can also constrain people or create new possibilities; a hidden corner on the school ground could enable pupils to take a cigarette break, while cigarette dispensers which require proof of age constrain underage smoking.[573] These last three modalities can be harnessed through legal or non-legal government interventions in order to regulate behaviour.

Morgan and Yeung employ a more detailed categorisation which focuses on the ways in which the state can harness these modalities. They distinguish command, competition, consensus, communication and architecture or code.[574] Both consensus and communication work through social norms. Baldwin, Cave and Lodge identify a number of government actions, most of which fit nicely within the categorisations of Morgan and Yeung: to command (command), to deploy wealth or confer protected rights (competition), and to inform through disclosure requirements (a subset of communication). Their action 'to harness markets' is difficult to categorize. It

[572] L Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harvard Law Review 501, 506-507.
[573] Lessig (1999) 506-507.
[574] B Morgan and K Yeung, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press 2007) 80.

includes competition law, franchising, regulating by stipulating terms in government contracts, and tradable permits.[575] They add that the state can also act directly, i.e. take physical action, for example to contain a hazard.[576] Subsidized actions,[577] which Morgan and Yeung consider a competition-based strategy, are part of this category.[578] According to Baldwin, Cave and Lodge, state action also includes 'design solutions',[579] which could be considered regulation through architecture or code. Consensus-based regulation is not seen as government action, so it is discussed under the heading of self-regulation.[580]

In the following, the categorisation of Morgan and Yeung is followed because of its cohesiveness and extensiveness. Techno-regulation or code is not discussed because it is not applicable. Enforced self-regulation and responsive regulation are hybrid forms of consensus and command; they are discussed in section 3.2.1.4. Smart regulation and meta-regulation are discussed as hybrid forms which employ a wider array of modalities in section 3.2.1.6.

3.2.1.2 Command-based regulation

Command-based regulation or command-and-control regulation is characterised by the state promulgation of legal standards or rules which prescribe or prohibit a specified conduct and by the threat of sanctions, civil or criminal, for non-compliance.[581] The rules employed in command-based regulation can be defined on the basis of the timing or stage of intervention and on the basis of their specificity. Firstly, rules might seek to prevent harm by controlling the processes that may lead to dangerous situations, for example by requiring safety policies; they can prohibit acts which create harmful situations; or sanction the presence of harmful results.[582] The first category, so-called design standards, prescribe how dangerous situations which may lead to harm must be avoided, while the second category of performance or output standards leaves the regulatee to determine the means.[583] The third category of target or outcome standards regard the avoidance of the harmful consequences by setting targets.[584]

Secondly, and similarly, these rules can be formulated in a manner which is more or less "principles-based". The difference between standards and principles can be captured by the standard to drive a maximum of 120 km/h or the principle to avoid accidents. The difference lies in the 'relative vagueness' of the rule, relating to how general, abstract and universal it is versus how specific, concrete and particular, as indicated by the level of detail and clarification and by the use of (im)precise terms.[585] Standards specify when they apply and what is required. Moreover, standards often prescribe how a result is to be achieved, while principles generally

---

[575] Baldwin, Cave and Lodge (2012) 114-119.
[576] Baldwin, Cave and Lodge (2012) 106.
[577] Baldwin, Cave and Lodge (2012) 121.
[578] Morgan and Yeung (2007) 85.
[579] Baldwin, Cave and Lodge (2012) 122.
[580] Baldwin, Cave and Lodge (2012) ch 8.
[581] Morgan and Yeung (2007) 80; Baldwin, Cave and Lodge (2012) 106. **This has also been called "imperium laws",** see T Daintith, 'The Techniques of Government' in J Jowell and D Oliver (eds), *The Changing Constitution* (Oxford University Press 1994) 213.
[582] Baldwin, Cave and Lodge (2012) 296-297.
[583] Baldwin, Cave and Lodge (2012) 297.
[584] Baldwin, Cave and Lodge (2012) 298.
[585] J Black, M Hopper and C Band, 'Making a success of Principles-based regulation' (2007) 1(3) Law and Financial Markets Review 191, 194; B Burgemeestre, J Hulstijn and Y Tan, 'Rule-based versus Principle-based Regulatory Compliance' in G Governatori (ed), *Legal Knowledge and Information Systems* (IOS Press 2009) 38.

only declare the objective which should be attained, leaving the means to the norm-addressee.[586] In other words, principles are performance standards. This is seen as the main characteristic of principles-based regulation: it uses rules 'to outline regulatory objectives and values' and leaves regulatees free to design systems to achieve these principles.[587] The idea is that organizations and their managers are better placed to determine how to efficiently achieve the desired outcome or goal than the regulator.[588] Principles-based regulation is not typically associated with traditional command-based regulation,[589] but rather with the type of delegation that is central to meta-regulation (discussed below).[590] A principle may seem uncertain but actually become quite clear due to the emergence of a shared understanding as to the meaning of the norm,[591] for example through regulatory conversations or through case law. As principles are given substance through their application, they become more rule-based; best-practices and requirements are formulated.[592]

3.2.1.3 Competition-based regulation

Competition-based regulation uses the competitive forces of the market to regulate through a payment from or to the regulatee.[593] A harmful activity or product may be subject to a charge or a tax, for example.[594] Beneficial actions can be induced by offering subsidies, for example in the form of grants for the purchase of certain equipment, compensation for loss of profit, or tax reductions.[595] According to Ogus, these are incentives; Baldwin, Cave and Lodge call it incentive-based regulation.[596] Incentives are to be contrasted with legal compulsion and can be negative (an action is not prohibited but is subject to a charge) or positive (an action is not mandatory but is subsidized).[597]

Liability can also be seen as competition-based regulation.[598] The idea is that the regulatee, for example a prospective polluter, is deterred from the harmful activity by its potential liability to compensate victims for their damage when sued by the holder of a respective right. The expected cost of the harmful activity – being the quantum of expected damages times the probability that the damages will need to be paid - will thus rise.[599]

3.2.1.4 Consensus-based regulation

Consensus-based regulation regulates behaviour through consensus and co-operation. There needs to be consent of the participants for it to work.[600] This type of regulation is often associated with self-regulation.[601] From the perspective of the regulator, self-regulation in its

---

586 Burgemeestre, Hulstijn and Tan (2009) 39.
587 Baldwin, Cave and Lodge (2012) 302.
588 Black, Hopper and Band (2007) 192-193.
589 Baldwin, Cave and Lodge (2012) 303.
590 J Black, 'Forms and Paradoxes of Principles-based Regulation' (2008) 3(4) Capital Markets Law Journal 425, 432.
591 Black, Hopper and Band (2007) 194.
592 Burgemeestre, Hulstijn and Tan (2009) 37.
593 Morgan and Yeung (2007) 85, 88.
594 A Ogus, *Regulation: Legal Form and Economic Theory* (Hart Publishing 2004) 246-248.
595 Ogus (2004) 249.
596 Baldwin, Cave and Lodge (2012) 111.
597 Ogus (2004) 245.
598 Morgan and Yeung (2007) 85.
599 Baldwin, Cave and Lodge (2012) 126.
600 Morgan and Yeung (2007) 92.
601 Morgan and Yeung (2007) 92.

broad sense means that a group of firms of individuals exerts control over its membership and their behaviour,[602] as any semi-autonomous social field does. The term self-regulation is generally seen as including regulation which is prepared by, deliberated on or formulated by the state, but which employs the self-regulating capacity of social fields.[603] A governmental agency may also be involved with monitoring and enforcement, or public enforcement may be stimulated by the state.[604] There is a spectrum between autonomously formulated and enforced rules and rules which are produced or approved by, or otherwise subject to the oversight of, a state actor.[605] At the less autonomous end of the spectrum, command-based tools can be used to guide the self-regulatory capacity of the regulatee. Command-and-control regulation can be supplemented by self-regulatory mechanisms, such as self-assessment.[606] At the autonomous end, self-regulation consists of rules which are made or enforced in a social field or industry by the stakeholders or their representatives *without imposition from outside or above*.[607]

Ayres and Braithwaite recommend a particular brand of self-regulation which falls somewhere in the middle of the spectrum: enforced self-regulation. This type of regulation occurs if the rules must be approved by the government. Violations of the self-drafted, but government-approved, norms would be punishable by law. Further, internal compliance and enforcement mechanisms are inspected, if they are present: are they carried out by independent parties, and is the system efficient and tough enough? Firms which are too small to have their own compliance program could be subject to traditional government monitoring.[608] The standard-setting, monitoring and enforcement are thus "subcontracted", but remain subject to oversight. The system of binding corporate rules is an example of government-approved self-regulatory standards, although it lacks the oversight on the internal compliance and enforcement mechanisms which Ayres and Braithwaite recommend.

Even in self-regulation in its narrowest sense, the law can function as a threat in the background and as a fall-back mechanism. Firstly, if community rules are not sufficient, the state might intervene.[609] Ayres and Braithwaite accord the threat of state intervention some importance. They argue under the heading of "responsive regulation" that regulators are most likely to achieve their goals if they communicate to the regulatees that self-regulation is preferred, but that enforced self-regulation or command-based regulation are back-up options if the regulatees are not willing. This incentivizes regulatees to make the least burdensome approach of self-regulation work.[610] Secondly, agreements have force by more than social norms alone if they are captured in contracts. Binding arrangements between participants in the social field or industry can be enforced in court.[611]

---

602 Baldwin, Cave and Lodge (2012) 137.
603 M Oude Vrielink, 'Wanneer is zelfregulering een effectieve aanvulling op overheidsregulering?' in M Hertogh and H Weyers (eds), *Recht van onderop: Antwoorden uit de rechtssociologie* (Ars Aequi Libri 2011) 64-65; Baldwin, Cave and Lodge (2012) 138.
604 Baldwin, Cave and Lodge (2012) 138.
605 Ogus (2004) 108-109; Baldwin, Cave and Lodge (2012) 137.
606 Baldwin, Cave and Lodge (2012) 146.
607 W Witteveen, 'Alternatieve regulering: de vele gezichten van de wetgever' in W Witteveen, I Giesen and J de Wijkerslooth de Weerdesteijn, *Alternatieve regulering* (Kluwer 2007) 29, 33.
608 I Ayres and J Braithwaite, *Responsive regulation: Transcending the Deregulation Debate* (Oxford University Press 1992) 106-107.
609 Morgan and Yeung (2007) 96; Baldwin, Cave and Lodge (2012) 138.
610 Ayres and Braithwaite (1992) 38-39.
611 Morgan and Young (2007) 95; Baldwin, Cave and Lodge (2012) 139,

3.2.1.5 Communication-based regulation

Communication-based regulation also employs the force of social norms. It includes attempts to persuade or educate members of the regulated community or those affected by the regulated activity. This can occur through public information campaigns, guidance, or disclosure requirements, for example. While campaigns seek to urge citizens to act in a manner which aligns with government policy objectives,[612] guidance has the goal of providing information or explanations to the public, allowing it to make more informed choices. The government can, for example, provide guidance on legal rights, obligations, and rules about the exercise of specific discretionary powers.[613] The third category of disclosure requirements obliges the regulatee to disclose information to a set of third parties, for example the purchasers of their product. This allows them to make more informed decisions and may work as a deterrent against unlawful or unethical behaviour; "sunlight is the best disinfectant".[614] A fourth category is to publicise compliance performance. The supervisory authority can publish on the initiation of a prosecution or issue press releases following an individual investigation. It can also start a large investigation so as to publish the compliance of multiple members of the regulated community, for example through performance indicators.[615] By praising those who do well, their competitors may be motivated to up their game, while the shaming of those who fall behind regulatory standards may incentivise them to comply. Shaming can punish the offender, harm its reputation, and deter others from engaging in similar behaviour. At the same time, the publicity of this information may facilitate consumers to make more informed choices.[616]

3.2.1.6 Hybrid forms

Clearly, these different modalities overlap and many instruments rely on multiple mechanisms. It was already described above that classical self-regulation may be enforceable on the basis of contract law and may come about under an (implicit) threat of the state to intervene.[617] Moreover, the state can be present in the formulation or enforcement of norms, leading to a mixture of consent-based with command-based regulation – of which enforced self-regulation is an example. Regulatory studies has started to focus not on the regulation as such, but on the governance of regulation.[618] Because the actual dominance of 'law-as-coercion' is no longer assumed, the focus is on how to make the rules work.[619]

While Ayres and Braithwaite's responsive regulation revolves around command- and consensus-based mixes, regulators can also employ a broader mix of regulatory options. Gunningham, Grabosky and Sinclair have argued, under the heading of smart regulation, that different instruments should be used in a complementary manner. They argue that "single instrument" approaches are misguided because none of the instruments are sufficiently flexible and resilient to address the problems which the regulator tries to tackle. However, different techniques

---

612 K Yeung, 'Government by publicity management: Sunlight or spin'? (2005) Public Law 360, 372.
613 Yeung (2005) 373-374.
614 Yeung (2005) 368; Baldwin, Cave and Lodge (2012) 119.
615 Yeung (2005) 374-375..
616 Yeung (2005) 376.
617 Morgan and Yeung (2007) 96, 106.
618 D Levi-Faur, 'Regulation and regulatory governance' in D Levi-Faur (ed), *Handbook on the Politics of Regulation* (Edward Elgar Publishing 2011) 14.
619 M Cohn, 'Law and regulation: the role, form and choice of legal rules' in D Levi-Faur (ed), *Handbook on the Politics of Regulation* (Edward Elgar Publishing 2011) 187. See section 1.3.2.1.

should not be haphazardly combined without any thought of the combined effect. Each instrument has strengths and weaknesses. A smart strategy harnesses the strengths of individual mechanisms while compensating for their weaknesses, if necessary, by using complementary instruments.[620] The regulator must make sure that the different techniques do not cancel each other out, as may be the case if uniform standards are combined with a charge or tax.[621] The appropriate mix of instruments depends on the nature of the problem and the industry.[622] In general, communication-based tools are complementary to other forms of regulation, and command-and-control and self-regulation also do well together.[623] Baldwin and Black also argue that different tools should be used in a complementary manner.[624] For example, deterrent sanctioning may undermine educational approaches because they are based on different assumptions and rationales.[625] Like responsive regulation, smart regulation involves the sequencing of instruments, whereby tools are used if others have failed – starting with the least interventionist ones.[626]

Meta-regulation is a type of self-regulation in the broad sense which mixes a number of modalities. It is similar to enforced self-regulation, as it combines consensus and command, but it can also employ communication or market-based techniques to induce corporations to set appropriate standards. Meta-regulation refers to processes in which the regulator oversees a control or risk management system.[627] According to Parker, 'corporate citizens' need to use self-regulatory mechanisms to determine how to carry out their responsibilities, and also what values to follow in the grey areas, in which there is no consensus yet in the polity on how to act.[628] These systems should be 'permeable': based on dialogue with stakeholders and regulators.[629] The role of the government is double. Firstly, to provide guidance and incentives so corporations set appropriate standards; and secondly, to oversee whether regulatory goals are met by forcing them to evaluate and report on their self-regulation strategies (so-called meta-evaluation).[630]

Parker argues that corporations can and should be incentivized to adopt an appropriate system of self-regulation through the enforcement of commands by regulators and by the public, through tort liability. Next to the enforcement of commands, the government can offer tax breaks, practical guidance and technical assistance.[631] Good risk management systems can be publicly acknowledged and the leash on trusted regulatees may be loosened by minimizing inspections or by offering greater flexibility in the means used to achieve the regulatory goal.[632]

---

620 N Gunningham, P Grabosky and D Sinclair, *Smart regulation: Designing Environmental Policy* (Clarendon Press 1998) ch 6; N Gunningham and D Sinclair, 'Regulatory Pluralism: Designing Policy Mixes for Environmental Protection' (1999) 21(1) Law & Policy 49, 50.
621 Gunningham and Sinclair (1999) 61-64.
622 Gunningham, Grabosky and Sinclair (1998) 15.
623 Gunningham, Grabosky and Sinclair (1998) 438; Gunningham and Sinclair (1999) 55-58.
624 Baldwin and J Black, 'Really Responsive Risk-Based Regulation' (2010) 32(2) Law & Policy 181, 186.
625 Baldwin, Cave and Lodge (2012) 270.
626 Gunningham, Grabosky and Sinclair (1998) 444; Baldwin, Cave and Lodge (2012) 266.
627 Baldwin, Cave and Lodge (2012) 147.
628 C Parker, *The Open Corporation: Effective Self-regulation and democracy* (Cambridge University Press 2002) 245.
629 Parker (2002) 294.
630 Parker (2002) 245.
631 C Coglianese, 'Policies to Promote Systematic Environmental Management' in C Coglianese and J Nash, *Regulating from the Inside: Can Environmental Management Systems Achieve Policy Goals?* (Resources for the Future 2001); Baldwin, Cave and Lodge (2012) 150.
632 Baldwin, Cave and Lodge (2012) 150.

Bad systems can be criticized publicly and enforcement action can be taken.[633] Like Gunningham, Grabosky and Sinclair, Parker thus recommends the use of a large array of modalities: command, consensus, competition and communication. However, her recommendations are specific to getting corporations to take social responsibility even in the absence of (clear) legal norms.

3.2.2 Types of enforcement

Rules do not always translate automatically to the behavioural change they seek to achieve; they need to be enforced. Enforcement can be defined narrowly as the application of rules on the ground,[634] but it can also encompass other actions which are taken to achieve regulatory goals.

3.2.2.1 Timing of the enforcement

Depending on the legal framework, enforcement can take place at several stages. Shavell distinguishes preventative, act-based and harm-based regulatory action. These categories see to interventions 1) to prevent a dangerous act or situation from arising; 2) in response to an act which might lead to harm; and 3) in response to the realization of the harm, after the harm has occurred. A preventative action is, for example, the refusal to issue a license. An example of act-based regulation is the punishment of a failure to keep the sprinkler system in good order. Tort litigation is an example of harm-based action.[635]

3.2.2.2 Public and private enforcement

Regulation can be enforced by public actors and by private actors. Under public enforcement, a state official is responsible for monitoring whether the rules are complied with and for taking action against non-compliance.[636] It is also possible to construct a system in which private actors are allowed to start court proceedings against violations. Generally, the tort system provides the public an enforcement opportunity by allowing victims to seek compensation.[637] Just like financial penalties imposed by an administrative agency can have a deterrent effect, so can the obligation to pay civil damages.[638] Next to civil litigation, private actors can play a number of other roles in monitoring and enforcement. Many complaint mechanisms enrol the capacities of private actors, such as through third-party audit or at the ombudsman.[639] These types of enforcement may co-exist.

Both smart regulation and meta-regulation recommend a mix of public and private enforcement. Gunningham, Grabosky and Sinclair advice the regulator to recruit a range of actors to implement the regulation. Both commercial and non-commercial third parties can be empowered to act as 'surrogate regulators'.[640] This is argued to be more effective and efficient and to reduce the regulatory burden on the government. Parker is optimistic about the mix of public enforcement and tort liability to incentivize corporations to set and enforce appropriate standards when they self-regulate. One option is to make the extent of liability and sanctions

[633] Parker (2002) 267-270; Baldwin, Cave and Lodge (2012) 150.
[634] Baldwin, Cave and Lodge (2012) 227.
[635] S Shavell, 'The Optimal Structure of Law Enforcement' (1993) Journal of Law and Economics 255, 257-258.
[636] Morgan and Yeung (2007) 209.
[637] Morgan and Yeung (2007) 209.
[638] K Yeung, 'Privatising competition regulation' (1998) 18(4) Oxford Journal of Legal Studies 581, 589.
[639] Morgan and Yeung (2007) 215.
[640] Gunningham, Grabosky and Sinclair (1998) 262.

dependent on the existence of an effective self-regulatory system. Alternatively, regulators and courts can oblige corporations who are in breach to set up such a system.[641] Either way, government oversight should be combined with third party oversight and public debate, as the state should facilitate the capacity of third parties to hold the corporation to account. Meanwhile, the regulatee has to evaluate itself and enforce its self-regulatory system, while facilitating oversight on this system of self-evaluation by reporting on the strategies which it employs.[642]

3.2.2.3 Means of public enforcement: sanctions and conversations

Public enforcement does not only consist of handing out fines or issuing other sanctions; it is partly done through 'processes of persuasion, negotiation, advice, education, or promotion';[643] in other words, through regulatory conversations. These conversations take place between regulatory officials and regulatees and may concern the substantive meaning of rules, how rules are monitored and enforced, or the formation of self-regulatory rules. In general, rules are clarified through formal guidance documents, case-specific decisions, and informal mechanisms.[644] Regulatees may seek assurances that a particular activity is not in breach. If a rule is formulated too broadly, the regulator may have the power to waive its application in a particular instance to reduce hostility towards the regulation.[645] Similarly, conversations can take place when a rule needs to be applied or when it has been breached – in other words, during monitoring and enforcement. They may concern the meaning of the rule or the consequences of the breach. [646] Regulatory conversations can also occur during the formulation of a self-regulatory set of rules. If these rules are to give substance to a legal commands which are phrased in general terms, the regulator can give guidance or negotiate on how to tailor the law to the situation of the regulatee.[647]

3.2.2.4 Strategies of public enforcement

Command-based regulation can be enforced in different ways. Early literature makes a distinction between, on the one hand, the compliance approach and, on the other hand, the sanctioning or deterrence approach. In the terminology of Hawkins, a sanctioning approach revolves around 'the application of punishment for breaking a rule and doing harm'.[648] A compliance approach, to the contrary, is concerned with securing conformity rather than punishing evil, which is associated not with sanctions but with negotiating future compliance.[649] Not only current conformity to the rules, but also the willingness to comply and the efforts taken to secure compliance are important. The willing regulatee is treated as compliant so as to ensure a cooperative relationship in which the regulatee seeks to establish substantive compliance, i.e. actual conformity with the underlying regulatory goal.[650] The regulator bargains with the regulatee so that it agrees - perhaps grudgingly but voluntarily - to take certain steps and to report problems. The bargaining process is one of give and take, so the regulator needs

---

641 Parker (2002) 256; Baldwin, Cave and Lodge (2012) 149-150.
642 Parker (2002) 245.
643 Baldwin, Cave and Lodge (2012) 230.
644 J Black, 'Talking about regulation' (1998) 1 Public Law 77, 78-79.
645 Black (1998) 88-90.
646 Black (1998) 86.
647 Black (1998) 85-86.
648 K Hawkins, *Environment and enforcement* (Oxford University Press 1984) 4-5.
649 Hawkins (1984) 4-7.
650 Hawkins (1984) 109.

demanding rules or high fines to give up or to be lenient on.[651] Hutter distinguishes two sub-categories of the compliance approach. With the "insistent strategy", a less flexible attitude towards the law is adopted: officials limit their tolerance and increase pressure to comply if the regulatee is not forthcoming - but with the aim of securing future compliance rather than of punishing wrong.[652] The "persuasive strategy" is more accommodating,; regulatees are coaxed into compliance, the reasonableness of the law is explained, and possible means of achieving compliance are proposed.[653]

In the compliance approach, enforcement is about promoting a willingness to comply.[654] This assumption also underlies the recommendation of Ayres and Braithwaite to play it tit-for-tat, which is part of their normative ideal of "responsive regulation". According to the authors, '[t]he crucial question has become: [w]hen to punish; when to persuade?'.[655] Their answer is: start with a cooperative approach, but punish the regulatee if this is abused.[656] Corporations will sometimes be calculative, but more willing at other times,[657] and it is most efficient to give them the benefit of the doubt.[658] However, if 'the privilege of persuasion' is abused, the regulator should make use of its powers to sanction the regulatee – and it can do so more effectively if a large array of sanctions is available, providing both small and large sticks.[659] Nonetheless, punishment must be accompanied by a breach of the law, and the severity of the punishment should be proportionate to the seriousness of the defence.[660] These legal requirements limit the discretion of regulators to adopt the responsive approach.

An alternative view is that the enforcement strategy should be fully driven by the motivations or characters of the non-complier or the reasons for non-compliance. If a regulatee is probably unresponsive to soft persuasion techniques, it would be wasteful to start so low on the enforcement pyramid.[661] Kagan and Scholz have distinguished three types of regulatees: amoral calculators, who base decisions on cost-benefit analyses; political citizens, who choose not to comply out of civil disobedience; and the organizationally incompetent, who are not able to comply.[662] The incompetent may lack awareness and knowledge of the rules and how to implement them, or the resources to gain such knowledge and alter their organizational processes so as to comply. The organizationally incompetent and the political citizens may benefit from persuasive and educational approaches, while the amoral calculators need to be incentivized by high fines. Hawkins' research into the enforcement of water pollution standards

651 Hawkins (1984) 122.
652 B Hutter, *Compliance: Regulation and Environment* (Oxford University Press 1997) 15-16; Morgan and Yeung (2007) 187.
653 Hutter (1997) 15-16; Baldwin, Cave and Lodge (2012) 239.
654 Black (1998) 88.
655 Ayres and Braithwaite (1992) 21.
656 Ayres and Braithwaite (1992) 21-27.
657 Ayres and Braithwaite (1992) 24-25.
658 Section 3.4.3.3.
659 Ayres and Braithwaite (1992) 26, 36 and 40.
660 K Yeung, *Securing compliance* (Hart Publishing 2004) 169-170.
661 Baldwin, Cave and Lodge (2012) 262.
662 R Kagan and J Scholtz, 'The criminology of the corporation and regulatory enforcement strategies' in J Hawkins and J Thomas, *Enforcing Regulation* (Kluwer 1984) 494.

in the UK show that officials use such typologies to tailor their enforcement strategy to the regulatee.[663]

Baldwin and Black use these insights in their framework of "really responsive regulation". Regulators need to be attentive to a number of factors, including the 'operating and cognitive frameworks' of regulatees, or their 'attitudes and cultures'.[664] The motivations and conceptual frameworks of regulatees influence the regulator's capacity to exert influence and must therefore be taken into account.[665] This includes their general attitude towards the regulatory regime, towards compliance and towards the regulator, their position in the market and their reputation, and their internal power structures.[666] Also their attitude to certain enforcement styles, such as naming and shaming, should be regarded.[667]

3.2.2.5 Risk-based public enforcement

Enforcement action can be prioritized on the basis of the risks that (the activities of) regulatees present in light of the regulatory goals.[668] The aim of such "risk-based" frameworks is principally 'to control relevant risks, not to secure compliance with sets of rules.'[669] As such, they are preventative or act-based. Black explains that regulators constantly need to make decisions regarding which firm or activity to focus on. Risk-based frameworks 'both render the fact of selection explicit and provide a framework of analysis in which they can be made'.[670] The framework must establish the criteria or logic on the basis of which the decision to focus on certain activities is understood. The regulator uses the assessment to assign scores to firms. These scores guide the way its attention, and thus its resources, is divided.[671]

3.3 Characterising the data protection impact assessment

This section will apply the various types of regulation outlined above to see how the data protection impact assessment relates thereto and to assess how the data protection impact assessment can be characterised. The modalities and the enforcement strategies will be discussed consecutively in sections 3.3.1 and 3.3.2.

3.3.1 Modalities harnessed by the DPIA

3.3.1.1 The command to carry out a DPIA

The obligation to conduct a data protection impact assessment is a form of command-based regulation: it is a rule which can be enforced through sanctions. Article 33 of the General Data Protection Regulation requires controllers to describe the processing operation, to assess the

---

663 Hawkins (1984). See also P Mascini and J van Erp, 'Waarom zijn sommige vormen van rechtshandhaving effectiever dan andere?' in M Hertogh and H Weyers (eds), *Recht van onderop: Antwoorden uit de rechtssociologie* (Ars Aequi Libri 2011) 117.
664 Baldwin and Black (2007) 3-4; R Baldwin and J Black, 'Really Responsive Risk-Based Regulation' (2010) 32(2) Law & Policy 181.
665 Baldwin and Black (2010) 186.
666 Baldwin, Cave and Lodge (2012) 269.
667 Baldwin, Cave and Lodge (2012) 275.
668 Baldwin, Cave and Lodge (2012) 281. **See also M Sparrow**, *The Regulatory Craft* (Brookings Institution Press 2000), ch. 10, **which centres regulatory activity around the nomination and solution of problems.**
669 Baldwin, Cave and Lodge (2012) 281.
670 Baldwin and Black (2010) 184.
671 Baldwin and Black (2010) 185; Baldwin, Cave and Lodge (2012) 282.

risks and to identify mitigating measures, and also to document all this.[672] The controller can be fined for failing to carry out a DPIA,[673] and, under the Parliament version, for not doing so in the manner required by Articles 32a-33.[674] The command to assess risks is of quite a general character and could therefore, at first sight, be characterised as principles-based regulation. The Parliament version is more detailed in prescribing what needs to be described or assessed.[675] Nonetheless, in all three versions it is up to regulatees to design a risk assessment process, whereby they can make use of the privacy impact assessment systems described in various guidance documents and studies.[676] However, the DPIA does not unequivocally specify the objectives or values which it aims to serve: compliance, accountability, and/or the mitigation of risks to the rights and freedoms of individuals?[677] Because the underlying principles are not clear, Article 33 is bad principles-based regulation. Moreover, as discussed below, the regulatee needs to make a number of important normative decisions to carry out the risk assessment. The norm-setting involved with the application of Article 33 is more accurately classified as consensus-based regulation.

3.3.1.2 The consensus to set norms and mitigate risks

In order to carry out a risk assessment, the regulatee has to make a number of normative choices which are not prescribed: whether a threat is severe and likely enough to constitute a risk, how much knowledge of this risk is necessary for it to be known rather than imaginary, and what remedies form a suitable response. As explained in section 2.5.2.1, these choices depend on the level of protection and the level of precaution which is strived for. By setting these standards, the regulatee self-regulates. The GDPR provides some handholds for the risk assessment, but these are methodological; the rules are thus partly set by the regulatee. They are not formally subject to the (dis)approval of a government agency, as is the case with enforced self-regulation, but the supervisory authority could negotiate on the content of these norms during a prior consultation.

Moreover, if the DPIA is to ensure risk mitigation beyond what is required by the other requirements of data protection law, regulatees need to cooperate to take actual protective measures. According to the Article 29 Working Party, '[t]he risk-based approach [of the GDPR] requires additional measures when specific risks are identified (e.g. impact assessment, enhanced security, data breach notification)'.[678] However, as discussed throughout section 2, the command of Article 33 does not unequivocally extend to actual risk mitigation, although the supervisory authority may bluff that it does. The compliance review which is required by the Parliament version does entail a duty to demonstrate that the identified measures are taken, but the GDPR does not set any standards on the level of protection which must be reached.[679] Other duties of data protection law do, to some extent, require risk mitigation. The most extensive of these duties is privacy by design and by default. Article 23 requires controllers to implement

672 GDPR, art 33(3).
673 GDPR Commission version, art 79(6)(i); GDPR Council version, art 79a(3)(de); GDPR Parliament version, art 79(2a).
674 GDPR Parliament version, art 79(2a).
675 GDPR Parliament version, art 33(3).
676 Section 2.7.
677 See also section 2.8.
678 Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' (WP2018, 2014) 4.
679 Section 2.5.2.1.

technical and organizational measures so as to ensure compliance with the GDPR and to protect the rights of the data subject.[680] This duty may be constructed as extending to their rights and freedoms rather than only to the data subject rights contained in the GDPR - for example through regulatory conversations and judicial review.[681]

In the terminology laid out above, controllers are expected to set design standards under the heading of privacy by design and by default, which is an output standard. Thus, controllers need to devise the means to avoid harmful situations, such as data breaches or the absence of a system which provides data subjects with information and effective rights of control. The DPIA adds that controllers need to evaluate the design standards they devised by assessing the remaining level of risk to the rights and freedoms of data subjects as part of the DPIA. This evaluation needs to be reported and can be accessed by the supervisory authority. However, the DPIA does not require the controller to ensure that this level of risk is below a certain threshold; it does not specify which level of protection should be aimed for; there is no outcome standard.[682] The command is to conduct a risk assessment which evaluates the controllers' design standards, not to achieve a certain level of protection or avoid certain harms through these design standards. The actual mitigation of risks, above and beyond what is required by the other requirements of the GDPR, is thus left to self-regulation.[683]

3.3.1.3 Possibilities with regard to communication and the market

The last two modalities can also be harnessed through Article 33, although this is not required. The possibility of negotiation during the prior consultation sheds light on the communication-based aspect surrounding the data protection impact assessment. The regulatee can be subject to efforts to educate or persuade him. This is not, however, a general policy inherent to Article 33; it is rather an opportunity created by the system of the DPIA and the regulatory oversight thereon. As such, it should be considered as an enforcement strategy. The same goes for the potential publication of DPIA results by the supervisory authority; Articles 33 and 34 create this opportunity, but do not turn it into a policy. The DPIA is therefore not communication-based regulation proper. This would be different if DPIA reports are required to be made public; it would then be a disclosure requirement.

Secondly, the duty to conduct an impact assessment does not directly harness the competitive forces of the market. It does not give or demand a financial payment to or from the regulatee. It can pose a barrier to the processing of personal data in a risky manner because it requires a costly process to be undertaken, but this is not competition-based regulation proper. It may not even be regulation proper, under Black's definition, if the discouraging effect is not an intended consequence.[684] The tort law on the basis of which liability may attach to controllers if they do not mitigate risks properly does fall within the category of competition-based regulation. The DPIA can help set the standard of the duty of care which controllers are held to and the report can serve an evidentiary function. As such, Article 33 can indirectly contribute to the deterrent effect of tort law.

---

[680] GDPR, art 23(1).
[681] Section 2.5.3.
[682] Section 2.5.2.1. **With regard to public entities, outcome standards can be found in the obligation to respect fundamental rights and freedoms.**
[683] Section 2.6.1.2.
[684] J Black, 'Critical Reflections on Regulation' (2002) 27 Australian Journal of Legal Philosophy 1, 26; J Black, 'What is Regulatory Innovation' in J Black, M Lodge and M Thatcher (eds), *Regulatory Innovation* (Cheltenham 2005), 11.

3.3.1.4 The regulation of self-regulation through meta-regulation

The DPIA has many things in common with meta-regulation. It requires the controller to set up a system in which the risks of envisaged projects are assessed, enabling them to determine how to fill in their legal obligations and what to do with the remaining risks to the rights and freedoms of individuals. It helps them assess whether the envisaged processing would be compliant or in line with their code of conduct.[685] In other words, it is a mandatory system of self-evaluation. The self-regulatory capacity of controllers is called on to ensure that the standards and principles of data protection are applied. Controllers are also forced to confront the grey area, in which there is no democratically determined consensus on how to act. However, only the Parliament version requires controllers to monitor their compliance to the DPIA and to demonstrate that the measures they discern during the assessment are undertaken.[686] Under the Commission and the Council version, they may similarly need to keep an eye on ongoing processing operations to see if any risks remain unaddressed, but this is not clear.[687] As a result, there is not clearly a duty to implement an ongoing risk management system. Moreover, while Parker envisaged a smart mix of modalities to induce self-regulatees to set proper standards, including competition-based tools such as subsidies and technical assistance, the GDPR relies only on command, consensus, and possibly communication-based strategies.

An important part of meta-regulation is meta-evaluation: controllers report on their risk management system so the government agency can evaluate their self-regulation. The prior consultation provides supervisory authorities with this opportunity: they are consulted beforehand to discuss how to mitigate risks if the DPIA shows that the envisaged processing would be highly risky.[688] Moreover, supervisory authorities can oversee the quality of the self-regulatory system by checking if a data protection officer has been appointed and whether he or she meets the requirements, and by assessing whether the impact assessments are conducted in the prescribed manner. However, as stated, only the Parliament version includes a compliance review. The ex post oversight on the implementation of risk mitigation measures is thus limited; supervisory authorities have to make use of their investigatory powers to see how risks are actually mitigated.

3.3.2 Possible types of enforcement of the DPIA

The law does not fully determine which types of enforcement occur or which enforcement strategy is adopted, although legal design factors do play a role. The regulator and the public have to work with the legal powers which they are given. Under the GDPR, the DPIA can be enforced both by private and public entities, whereby public entities can, to some extent, make use of responsive or really responsive strategies. The DPIA can also be used within a framework of risk-based regulation, which will be considered separately.

3.3.2.1 Private enforcement through tort actions and complaints

Private enforcement of the DPIA and subsequent risk mitigation can take place firstly because controllers are liable for pecuniary and non-pecuniary damage arising from conduct which

[685] Section 2.8.1.
[686] Section 2.5.2.1.
[687] Section 2.2.1.
[688] Sections 2.6.1.1. and 2.6.1.2.

breaches the GDPR or, under the Commission and Parliament version, is incompatible with the GDPR, unless they can prove that they are not responsible.[689] A more strict standard of care may apply under national law. Under Dutch law, the question arises whether a tort is committed if there is no breach of the GDPR. A tort is a violation of a right or an act or omission which breaches a duty which is either imposed by law or which arises from what, according to unwritten law, has to be regarded as proper social conduct.[690]

A number of cases indicate that any processing of data which leads to harm could potentially be considered a tort, even if there is no clearly identified violation of the Dutch Data Protection Act. For example, in a 2007 case the Court of Appeal explicitly assumed that the disclosure of information which lead up to a dismissal was in violation of the Dutch Data Protection Act and therefore constituted a tortious act. Strangely enough, the violation was not identified at all. The court simply supposed that the disclosure constituted a violation and proceeded to apply a number of rules of general tort law, especially on the contribution of the claimant to his dismissal (*eigen schuld*).[691] The principle of fair processing could provide a catch-all provision which allows the court to construct a tort when it is faced with unreasonable conduct. In another case, the court simply stated that the principle of fair processing of Article 6 of the Data Protection Act was violated.[692] In the *Alijda*-case, law enforcement employed a blacklist without specifying under what conditions someone would be placed on the list and without specifying which other agencies had access and which did not. The lack of safeguards was considered a violation of fair processing.[693]

The DPIA report - which will generally be accessible through discovery, at least under Dutch civil procedural law -[694] can strongly indicate that the controller had knowledge of a risk but failed to address it. This is harm-based regulatory action: it is a response to the harm which results from the materialization of a risk. It can also have a deterrent effect, which was considered above as market-based regulation.

Secondly, private enforcement can also occur through the complaints mechanisms of supervisory authorities or ombudsmen. The complaints of affected citizens fulfil a monitoring function and may lead to enforcement action taken by these government agencies. Data protection officers may also play a similar signalling function.

3.3.2.2 Public enforcement: more compliance than deterrence

Public enforcement can see to the requirement to carry out a data protection impact assessment and to the actual subsequent mitigation of risk. The command to carry out a data protection impact assessment can be enforced by the supervisory authority through sanctions or through more "compliance-oriented" approaches. With regard to risk mitigation, on the other hand, sanctions are only unequivocally available insofar as the General Data Protection Directive will be or has been breached. Member States could choose to stretch the legality principle by interpreting Articles 34 and 53 as allowing supervisory authorities to prohibit risky, but compliant, data processing operations. During the prior consultation of Article 34, regulatory

689 GDPR Commission and Parliament version, art 77(1); GDPR Council version, art 77(1) and (2); Section 2.6.2.2.
690 Burgerlijk Wetboek, art 6:162.
691 Hof 's-Gravenhage 16 February 2007, ECLI:NL:GHSGR:2007:BA1567.
692 Rb. Amsterdam 4 July 2007, ECLI:NL:RBAMS:2007:BB4555.
693 ABRvS 4 July 2007, ECLI:NL:RVS:2007:BA8742, mt. nt. G Overkleeft-Verburg.
694 Section 2.6.2.2.

conversations may take place in the shadow of the bluff or threat of a prohibition of the processing, whereby the regulator can take a persuasive or an insistent approach. The consultation may lead to agreements on the level of risk mitigation which should be achieved and the measures which should be implemented, adherence to which might, depending on the construction of Article 53(1)(d), be enforceable through sanctions.[695] Only if persuasive and deterrent approaches are available – as is the case if the conduct is in breach of the GDPR or if Articles 34 and 53 are broadly interpreted –[696] can the supervisory authority choose to adopt a tit-for-tat approach, as recommended under the heading of responsive regulation, or tune the employed strategy to the behaviour of the regulatee and the context, as under really responsive regulation. Moreover, the vague norms of the DPIA are more in tune with a compliance-oriented approach. As discussed below, deterrent approaches benefit from precise rules, so that non-compliance can be readily established. However, if the regulator is more keen on promoting good practice, accessibility is more important than precision.[697] Article 33 clearly lends itself better to compliance-oriented enforcement; the boundaries of its legal obligations are far from clear.

Enforcing the duty to carry out a DIA is preventative because the DPIA can help avoid situations of non-compliance or other potentially harmful situations.[698] On the other hand, a conversation, prohibition or sanction relating to a failure to implement adequate risk mitigation measures can be characterised as act-based: the regulatees's conduct brings about a situation which may give rise to harm. These enforcement actions may also be taken after the harm has occurred.

3.3.2.3 Risk-based regulation as part of the risk-based approach

The regulator can use a risk-based framework to guide the decision to focus on particular activities or controllers. According to the Article 29 Working Party, the risk-based approach of the GDPR entails that one of the main roles of supervisory authorities is 'targeting compliance action and enforcement activity on areas of greatest risk'.[699] This appears to be particularly compatible with the DPIA and prior consultation system. If a DPIA report points to high risks, the supervisory authority needs to be consulted. It can decide, on the basis of the DPIA report and other indicators, whether to focus on a particular consultation. The new risk-based approach of the GDPR is, in essence, a partly outsourced version of the current notification duty and prior check, under which every processing operation has to be registered and is subsequently checked by the supervisory authority if they present specific risks.[700] According to Recital 70 of the GDPR, such a indiscriminate notification duty should be abolished and replaced by effective procedures and mechanisms which focus instead on risky types of processing operations.[701]

---

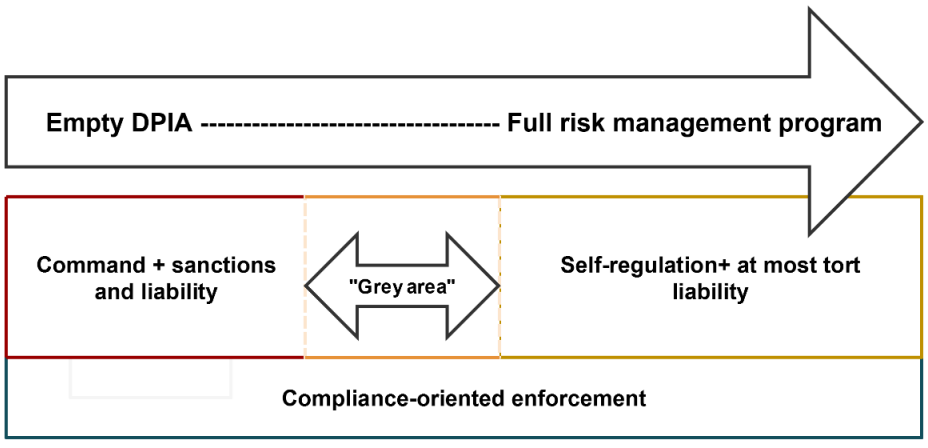
695 Section 2.6.3.
696 **The availability of deterrent approaches depends on how broadly the requirements of data protection are interpreted and on the leeway granted to supervisory authorities to sanction behaviour which is technically compliant.**
697 Baldwin, Cave and Lodge (2012) 230; Section 3.4.1.1.
698 Section 2.8.
699 Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', 4.
700 Data Protection Directive, art 18.
701 GDPR, rec 70.

3.3.3 Conclusion

In conclusion, the DPIA can be characterised as command-based and consensus-based regulation. The command is to carry out a data protection impact assessment, but the controller should self-regulate by determining the level of protection which is strived for during the assessment and by implementing sufficient measures. The level of protection and the measures are, to some extent, commanded by other requirements of data protection, such as privacy by design and by default. Moreover, the DPIA can be used as a communication-based tool and it may interact with the competition-based regulation that is tort law. Such mixing of regulatory tools and actors can be called "smart regulation". However, the regulator is not very responsive and smart in the sense that it probably will not "sequence". While the self-regulatory aspects of the DPIA could be subject to government legislation later, and in that sense take place under an implicit threat of state intervention, the European legislature is not sending out the message that command-based regulation is an option if regulatees are not willing. To the contrary, the lengthy drafting process indicates that they would not quickly attempt to redefine data protection standards. Self-regulation is therefore not clearly incentivized through the threat of strict legislation.

The modalities of command and consensus are combined in a meta-regulatory manner. Regulatees should set up a system of risk management. This is a legal duty under the Parliament version, which also requires controllers to actually implement the risk mitigation measures which they identified during the DPIA and to review their compliance to their self-set standards. The system is overseen by the supervisory agency, particularly during the preventative prior consultation. The duty to carry out a data protection impact assessment and subsequent risk mitigation can be enforced through regulatory conversations of a more or less compliance-oriented character, and – if the conduct breaches the GDPR or if Articles 34 or 53 are widely interpreted -through a deterrent approach. If sanctions are available, public actors can use a responsive or a really responsive style of enforcement, reacting in a persuasive, insistent, or deterrent manner. Moreover, a risk-based framework can be used to prioritize certain controllers or data processing activities. If harm occurs because risks were not sufficiently mitigated, this can also be met with public enforcement on the basis of tort law.

The mix of command and consensus and deterrent, compliance-oriented and civil enforcement is summarized by the figure below.



The figure presents the DPIA as part of a larger risk management program by which regulatees regulate themselves. By regulating how regulatees manage the risks presented by their activity, the EU engages in meta-regulation. This is a way of regulating not only technical legal compliance, but also "grey areas" and unregulated areas such as corporate social responsibility and responsible research and innovation. The figure illustrates that in order to have a full risk management program, controllers need to self-regulate. If they only do the minimum of what is legally required, they do not have a full risk management program; the sanctionable commands of the GDPR do not extent far enough, although they can be extended, for example by extensively interpreting privacy by design and by default. The self-drafted and self-implemented rules which turn the commanded DPIA into a system for the proper management of risks come about under a threat of, at most, tort liability – depending on the standards of care in the country that has jurisdiction. Compliance-oriented approaches, however, are available even if there is no command; supervisory authorities can still negotiate on (un)desirable conduct. It should be added that the data protection officer – if present – can help companies create a full risk management program.

3.4 Strengths and weaknesses

This section will discuss the strengths of these types of regulation and enforcement. It will become clear that the different modalities and enforcement strategies overlap – the conclusion will bring them together.

First, however, a word of caution. Although the description and application of the types of enforcement also entails interpretation and judgment calls which render it subjective, the analysis of the strengths and weaknesses of these types is particularly sensitive to a bias which the author displays. Under the assumption that many corporations value profit over social responsibility and take a calculative attitude towards legal compliance, commands which are enforced through a deterrent approach and high sanctions are deemed more effective overall.[702] Pearce and Tombs, for example, expressed great concern over the persuasive approach. In their opinion, most corporations are amoral calculators because of the inherent tension between 'the profit-making goal of business enterprises with competitive capitalism' on the one hand, and corporate social responsibility on the other.[703] However, this assumption is not necessarily correct. Mascini and van Erp even imply that such a view is outdated by empirical studies which show that sometimes, corporations take expensive measures to comply even though their competitors got away with non-compliance, and which point to other reasons for non-compliance, such as ignorance or political civil disobedience.[704] However, these studies do not discredit that many business managers – perhaps more so within corporations of a particular size and in particular sectors –may not see all of their compliance and CSR duties as moral imperatives. The same may also apply to government departments or agencies. We do not know

[702] Mascini and van Erp (2011) 118-119.
[703] F Pearce and S Tombs, 'Ideology, hegemony, and empiricism' (1990) 30(4) British Journal of Criminology 423; F Pearce and S Tombs, 'Policing corporate "Skid rows": A reply to Keith Hawkins' (1991) 31(4) British Journal of Criminology 415. **This is not to say that public enforcement cannot also contribute to the effectuation of the desired behavioural change. The risk of reputation damage can be considered a reason to comply, also for calculative controllers; the point is that they do not adhere to rules because they *should*, but only if it would be costly not to do so.**
[704] Mascini and van Erp (2011) 119. See also Kagan and Scholz (1984); R Fairman and C Yapp, 'Enforced Self-Regulation, Prescription, and Conceptions of Compliance within Small Businesses: The Impact of Enforcement' (2005) 27(4) Law & Policy 491, 503, 515.

what portion of the regulatees evades the rules under discussion as much as possible as soon as this is better for their bottom line. A useful solution is to presuppose that non-compliance can arise from calculative behaviour, political disagreement or incompetence, as in Kagan and Scholz's typology,[705] without assuming that most regulatees will always[706] fall within the first group.

3.4.1 The command to carry out a DPIA

The requirement to carry out a DPIA is a command. Commands can be valuable in prohibiting dangerous or harmful conduct or in requiring good conduct, rather than "merely" incentivizing for or against it.[707] Commands also serve an important expressive function: they signal behaviour which is expected or unacceptable in our society.[708] This thesis is only concerned with the ability of a type of regulation to effectuate a behavioural change, but the expressive dimension of rules can have a bearing on effectiveness; it may persuade regulatees and the general public of the acceptability or importance of a norm. The requirement to conduct an impact assessment can, as discussed in the last chapter, be beneficial for compliance, accountability and risk mitigation.[709] It also sends a signal: as a controller, you must take the impact of your actions into account. However, commands are never fully effective.[710] Commands have linguistic limits and may not be followed.

3.4.1.1 The limits of rules and creative compliance

Commands depend on rules, and rules tend to be over- or under-inclusive, they are indeterminate, and they need to be interpreted. They intend to cover certain scenario's, which are captured by employing generalizations. These generalizations may not include properties which turn out to be relevant, which makes the rule under-inclusive, or they may include properties which are not necessary, making the rule over-inclusive.[711] An obligation to assess risks to the rights and freedoms of individuals is an example of an over-inclusive rule – assuming that not *all* risks to *all* the rights and freedoms of individuals are considered relevant. Under-inclusion can lead to 'missed targets', while over-inclusion intrudes upon the public sphere more than was necessary and may cause regulatees to experience the rule as unreasonable.[712] Rules are also indeterminate. In Hart's words, they have a 'penumbra of doubt'; there are difficult cases of which it is not sure whether they are captured by the rule. The regulator did not foresee these difficult cases, so they are not clearly included or excluded.[713] Lastly, rules need to be interpreted – and for the rule to be applied as the regulator intended it to be applied, a shared understanding is required. According to Wittgenstein, such shared understandings arise from shared "forms of life", i.e. shared cultural frameworks. As a result, for a rule to be certain it must be interpreted equally by all parties involved, which - following Wittgenstein - requires a common interpretive community.[714]

---

[705] Kagan and Scholtz (1984) 494.
[706] **Regulatees can shift between types.** Ayres and Braithwaite (1992) 24-25.
[707] cf Ogus (2004) 245; Baldwin, Cave and Lodge (2012) 107.
[708] cf Morgan and Yeung (2007) 147.
[709] Section 2.8.
[710] Section 1.2.1.1.
[711] J Black, *Rules and regulators* (Clarendon Press 1997) 6-7.
[712] Black (1997) 6-8.
[713] H.L.A Hart, *The Concept of Law* (Oxford University Press 1961, 2nd ed) 123; Black (1997) 8.
[714] Black (1997). 8-10.

Under-inclusive rules may not be substantively complied with. Creative compliance is possible: the letter of the law is followed, but the spirit is disobeyed.[715] Creative compliance results from a refusal to include situations in the rule which were not technically covered, thus refusing to recognise the 'tacit understanding on which the rule is based'.[716] Regulatees may escape sanctions by adhering to the terms of the law without, however, achieving the regulatory goal.[717] Thus, because there are no clear standards on when a risk is "known", a threat might be argued to not constitute a risk because there is little certainty on the probability with which it will take place. A risk is technically defined as a threat times probability, implying that both must be known.[718] Those in favour of superintelligence could argue, for example, that there is no scientific agreement on whether the computational will escape our control: the probability is not known, so there is no risk. Literal interpretations of rules can be used to circumvent that which the rule is mean to require because 'the letter of the rule may not accord with the spirit in which it was framed' or may have become out of date.[719] This is somewhat alleviated in the case of the DPIA by using vague terms, such as "risks" and "rights". The likelihood of formalistic interpretations is thereby reduced, and the term can be argues to include the behaviour which the regulatee excluded from its scope.

Over-inclusive rules use vague terms. They are not in danger of creative compliance as it was defined above, but the vagueness opens up the problem that the meaning of these terms is less clear or less universally accepted. Do controllers need to assess the impact on the way in which they use data to personalise advertising on the problem of consumer debt in society? Before a court ruling is made, Article 33 is open to debate on this matter. The optimist would remark that the uncertainty attached to rules can be reduced through regulatory conversations, by fostering a shared understanding of what is meant by a rule and by deciding whether the situation at hand is considered to fall within its scope.[720] According to the critic, vague rules or principles allow regulatees 'to do what they want without fear of breaching strict rules'.[721] If there is legal uncertainty, the level of discretion of the involved parties – controllers, data protection officers and judges - is larger.[722] It may take decades before the vague rule gains a workable core of certainty. This can be remedied by appending a list of components – such as the list of risky processing situations. On the other hand, the rule may become less easy to apply or less congruent with the underlying policy objective if the terms are specified. [723] The list of risky data processing operations in the Parliament version may, indeed, overshoot the mark.

3.4.1.2. Other factors which play a role in adherence to rules

Next to a lack of clarity or precision, there are many other reasons why a command is not necessarily obeyed or substantively complied with. Illuminative in this respect is the so-called

[715] Section 2.6.1.2.
[716] Black (1997) 11.
[717] Baldwin, Cave and Lodge (2012) 110.
[718] Section 2.2.3.
[719] D McBarnet and C Whelan, 'The elusive spirit of the law: Formalism and the struggle for legal control' (1991) 52 Modern Law Review 848, 851.
[720] Morgan and Yeung (2007) 176.
[721] Black (2008) 432 and 439; Baldwin, Cave and Lodge (2012) 303.
[722] J Black, 'The Rise, Fall and Fate of Principles Based Regulation' (2010) 17 LSE Law, Society and Economy Working Papers, 8.
[723] C Diver, 'The optimal precision of administrative rules' (1983-1984) 93 Yale Law Journal 65, 71.

Table of Eleven, which was developed for the Dutch Ministry of Justice in 1994. Developed to improve the compliance-friendliness of government regulation, this comprehensive table lists eleven factors which may predict or explain the level of compliance with rules. It to be used during an ex ante or ex post assessment of the enforcement and compliance of a regulation, for example during a regulatory impact assessment.[724] Ideally, the regulatee has knowledge of the rules; the costs of compliance do not outweigh the benefits; the policy and legislation is considered acceptable; the regulatee has respect for government authority and adheres to their own rules and standards; and the rules are enforced through social control or peer control. With regard to government enforcement, the risk of being reported (e.g. by tip-off or complaint) or of being subject to an inspection, and the accompanying chance that they will find something, will play a role. Of importance is whether regulatory agencies succeed in focussing their detection activities on offenders. The risk that a sanction will be imposed and the severity of the sanction are the last two enforcement-related factors.[725] The importance of the different types of social, public and private enforcement is also apparent from a 2007 study on the privacy impact assessment. The study reviewed PIA models and conducted interviews with policy-makers, data protection regulators and a few organizations – all from DPIA's countries of origin, Canada, Australia, the US, New Zealand and Hong Kong. It concludes that 'PIAs appear to be more effective where they are part of a system of incentives, sanctions and review, and/or where they are embedded in project workflow or quality assurance processes [such as] risk assessment'.[726] In particular, the use of external review and external consultants are recommended, and also transparency to enhance trust in the proposed project.[727]

Regulatees can be familiarized with the risk assessment terminology with the help of data protection officers or other compliance experts if they have enough resources to do so. Carrying out a DPIA well is quite a burden, but this may be offset by the benefits for the regulatee, as strongly emphasized in literature and soft law. The impact assessment is "sold' as a tool or method for the risk management of controllers.[728] It helps them demonstrate compliance, helps ensure that the product will be accepted in society and that it will not have to be changed at a later stage, and reduces the risk that the controller will be faced with a privacy breach and the subsequent loss of reputation.[729] According to the 2007 study, companies have recognised that

---

[724] Expertisecentrum Rechtspleging en Rechtshandhaving, 'De 'Tafel van elf': een veelzijdig instrument' (2006) <https://www.kcwj.nl/kennisbank/integraal-afwegingskader-beleid-en-regelgeving/6-wat-het-beste-instrument/61/tafel-van> accessed on 15 September 2015.
[725] Centrum criminaliteitspreventie veiligheid, 'Tafel van Elf' < http://www.it11.nl> accessed 1 September 2015.
[726] A Warren and others, 'Privacy Impact Assessments: international experience as a basis for UK Guidance' (2008) 24(3) Computer Law & Security Report 233, 235.
[727] Warren (2008) 236.
[728] D Wright, 'Should privacy impact assessments be mandatory?' (2011) 54(8) Communications of the ACM 121, 126; R Weber, 'Symposium on EU Data Protection Reform: Privacy management practices in the proposed EU regulation' (2014) 4(4) International Data Privacy Law 290, 290; Commission, 'Impact Assessment. Accompanying the Documents Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation); and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' SEC(2012)72 final, 122-123; Information Commissioner's Office (ICO), 'Conducting privacy impact assessments: code of practice' (2014) < https://ico.org.uk/for- organizations/guide-to-data-protection/privacy-by-design/> accessed 15 August 2015, 23.
[729] D Wright, R Gellert, S Gutwirth and M Friedewald, 'Precaution and privacy impact assessment as modes towards risk governance' in R von Schomberg (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Field* (European Commission 2011) 97; D Wright, 'Making Privacy Impact Assessment More Effective' (2013) 29(5) The Information Society: An International Journal, 313; Weber (2014) 290.

they can use the impact assessment to 'expose and mitigate privacy risks, avoid adverse publicity, save money, develop an organizational culture sensitive to privacy, build trust and assist with legal compliance'.[730] From a systems theory perspective, this can be seen as an attempt of the law to steer subsystems not through its own language and logic, but through channels which are more compatible, channelling the internal management systems of regulatees.[731] The mitigation of risks is not a rule, compliance with which is enforced through sanctions, but something which regulatees should incorporate into their organizational processes for their own benefit. However, the literature fails to note that these benefits are only advantageous if the risks which are supposed to be mitigated, i.e. the cost of non-compliance and of potential reputation damage, are high enough: i.e. they only exist if supervisory authorities and citizens make it so. Apart from fines, other sanctioning mechanisms such as naming and shaming, the threat of stricter and less flexible legislation,[732] or the possibility to conduct stricter audits may also be available.[733] Regulators, scholars and activists are concerned with increasing transparency, for example through symbols and privacy seals,[734] to allow the public to react to non-compliance and privacy-unfriendliness. This increases the benefits of the DPIA and may also lead to a higher acceptance of the command to carry out a data protection impact assessment. Whether the regulatee has respect for authority and is subject to social control or peer control depends on the situation. Again, better transparency and a higher public concern for adherence to data protection law will be beneficial for compliance.

Internal social control is improved if the data protection impact assessment is embedded into the organizational processes. Research indicates that there are possibilities for integrating privacy impact assessments into project and risk management practices, and that, in practice, impact assessments are often part of the general risk management process. However, this study also concludes, on the basis of case studies with interviews, that proper internalisation requires the development of relevant functions or roles within the company and a 'privacy-aware culture' which allows privacy risks to be assessed early on and which sees this as a mandatory 'an organizational requirement'.[735] Similarly, Nokia highlights the importance of targeted personnel training and general awareness campaigns, and seems optimistic of the function of the impact assessments here by stating that '[p]rivacy assessments are in themselves a step towards changing corporate cultures'.[736] It may be that the DPIA itself will help in internalising privacy awareness, but the first step is getting it to be seen as an important requirement in risk management which is not to be glossed over – which the prior consultation and the appointment of data protection officers might encourage. The prior consultation serves as a check whether DPIAs are carried out properly, bringing in transparency and an external review.

---

730 Warren (2008) 235.
731 C Scott, 'Regulation in the age of governance: The rise of the post-regulatory state' in J Jordana and D Levi-Faur, *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance* (Edward Elgar Publishing 2004).
732 Wright (2013) 313.
733 Mascini and van Erp (2011) 125.
734 e.g. GDPR, art 39; GDPR Parliament version, art 13a and amendment 207; R Rodrigues, K Wadhwa and D Wright, 'Developing a privacy seal scheme (that works) (2013) International Data Privacy Law 100; EuroPrise – the European Privacy Seal for IT Products and IT-based Services <https://www.european-privacy-seal.eu/EPS-en/Home> accessed 1 September 2015; Terms of Service; Didn't Read <https://tosdr.org/> accessed 1 September 2015.
735 E Charikane, M Lagazio, C Raab, K Wadhwa, and D Wright, 'Integrating privacy impact assessment in risk management' (2014) 4(2) International Data Privacy Law 155, 155.
736 D Wright and P De Hert, 'Findings and Recommendations' in D Wright and P De Hert, *Privacy Impact Assessment* (Springer 2012) 476.

Whether a controller has carried out a DPIA is quite easy to check superficially, but the quality of the DPIA is much more difficult to control. The regulator would need to ascertain, amongst others, whether the project is adequately described, whether all the relevant risks are identified, and whether the measures are suitable to address these risks. This requires knowledge of the plans of the controller and of its activity, e.g. how to address data security issues. Because the DPIA does not have to be made public, the risk of being reported is very low. The enforcement factors clarify that it is important for the regulator to have enough resources to detect non-compliant behaviour and to impose a sanction, and also to have the power to issue high fines. Article 47(5) of the GDPR requires that each supervisory authority is given enough resources to effectively perform its duties – but whether this will happen depends, of course, on the overall available budget and the political negotiations on its distribution.

The lower the chance of being caught, the higher a fine is necessary to have a deterrent effect. The GDPR sets fines at a maximum 1 million Euros, or, for corporations, at a certain percentage of last year's worldwide turnover. Unfortunately, the Council did not accept the Parliament's increase in the height of the fine from 2 % to 5 %.[737] As a comparison: in competition law, a fine of maximum 1 % of the turnover can be imposed if incorrect information is supplied, while a fine of maximum 10 % can be imposed if the regulatees abuse their dominant position or form cartels.[738] Fines are not always this high, but the Commission does make use of its power: in 2006, 23 out of 314 undertakings were fined between 9-9.99 % of their turnover for participating in a cartel.[739] The fines for data protection violations are bleak in comparison.

3.4.2 The consensus to set norms and mitigate risks

The cooperation of regulatees is needed to set the norms with which to conduct the risk assessment, and again to implement the identified measures. This section will discuss the strengths and weaknesses of a self-regulatory system of self-evaluation. The enforcement aspect will be discussed in section 3.4.3.3.

3.4.2.1 Expertise, flexibility and differentiation

The main advantage of self-regulation is that the regulator makes use of the knowledge and self-regulatory capacity of regulatees. Regulatees have more knowledge and technical expertise relating to the regulated activity than the state.[740] They can work out what, given their context, is the most efficient way to meet regulatory goals.[741] Applying this to the DPIA context, tech companies are probably better able to identify risks to data security, decide how to mitigate them effectively, and estimate when the risks are mitigated enough to prevent data breaches. However, not all controllers will have such expertise; and there is no reason to believe that the legislator knows less about how to protect fundamental rights than data controllers. The resulting rules can, however, be more precise because they do not need to apply in many different contexts.[742] The rules can also be adapted more quickly to changes.[743] Controllers can

[737] GDPR Commission version, art 79; GDPR Parliament version, art 79(2a); GDPR Council version, art 79a.; Section 2.6.2.1.
[738] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, art 23.
[739] European Commission, 'Cartel Statistics' (2015) <http://ec.europa.eu/competition/> accessed 6 September 2015.
[740] Baldwin, Cave and Lodge (2012) 139.
[741] Baldwin, Cave and Lodge (2012) 147.
[742] Baldwin, Cave and Lodge (2012) 148.

indeed identify and update the measures needed to address a risk with more knowledge, or in any case with more swiftness, than the European legislator. Moreover, with regard to enforced self-regulation the possibility of differentiation also enables higher standards to be demanded of actors with lower compliance costs.[744] Multinationals could be treated more strictly than SMEs; supervisory authorities could, for example, try to negotiate a higher level of data security during the prior consultation.

3.4.2.2. Commitment, but a low level of rules

It is argued that self-regulatees are more committed to self-drafted rules.[745] It may be more accurate to say that representatives of the individuals within the regulated group know which regulatory obligations will be accepted as reasonable, which allows them to set rules at a level which is voluntarily complied with -[746] although this might result in standards which are too low. Government intervention may be necessary to set the standards at a high enough level, possibly surpassing that which regulatees find reasonable. Regulatees may be more inclined to set self-drafted standards at a high level if there is a threat that the government might otherwise intervene with enforced self-regulation or commands,[747] but, as stated above, the EU has not clearly signalled that this is a possibility. Moreover, Baldwin, Cave and Lodge note that it is difficult to fix standards at the right level. If a total eradication of risk is aimed for, most activities could not be carried out.[748] It already requires 'a good deal of judgement' for the regulatee to apply principles properly;[749] this is even more so with regard to the data protection impact assessment, which requires the regulatee to set important norms and goals regarding the identification and mitigation of risks. The supervisory authorities will have their work set out for them if they seek to ensure a high enough level of protection and precaution; they would have to engage in negotiations continually.

Regulatees can include democratic processes in their norm-setting procedure, which might help set rules at a desirable level. Parker aims for the "permeable" corporation, which constantly engages in deliberative dialogue with stakeholders and regulators to decide how to approach their legal responsibilities and the potential impacts of their conduct. She admits this is an ideal.[750] The DPIA also includes a stakeholder consultation, which may help controllers approach both their legal compliance and the surrounding grey areas. However, as argued under section 2.5.2.1., the duty to seek the views of data subjects is not a hard one; it will definitely not be carried out for every risky project, especially because it requires substantial resources and staff expertise.[751] Companies may not see themselves as deliberative organizations: '[m]any companies will see themselves in quite different terms—as organizations that sell products and services so as to make a return for shareholders within a framework of discipline by the market. Deliberation, they may think, is not what they are about, and they will be ill-inclined to commit to it.'[752] If the controller does choose to conduct a stakeholder consultation, it might also find

---

743 Black (1998) 88.
744 Ayres and Braithwaite (1992) 108; Baldwin, Cave and Lodge (2012) 147.
745 Black (1998) 88.
746 Baldwin, Cave and Lodge (2012) 139.
747 Ayres and Braithwaite (1992) 38-39.
748 Baldwin, Cave and Lodge (2012) 299.
749 Baldwin, Cave and Lodge (2012) 303.
750 Parker (2002) 294.
751 Badwin, Cave and Lodge (2012) 155.
752 Badwin, Cave and Lodge (2012) 155.

that it is challenging to conduct deliberations in a manner which leads to agreement or to otherwise take the different views into account.[753] Decision-making procedures are therefore likely to suffer from indecisiveness and inaction.[754] Another pitfall is that the deliberations are seen as a way to sell products or policies, as a result of which the consultations are manipulated and the views of the participants distorted 'in favour of private corporate ends'.[755] The shortcoming of the stakeholder consultation is that it is unlikely to be carried out properly, if carried out at all.

3.4.2.3 Would regulatees be able and willing to self-evaluate?

It is argued that informal enforcement mechanisms more efficiently control compliance because self-regulatees have lower monitoring and enforcement costs.[756] Internal compliance staff knows "where the bodies are buried".[757] However, this requires a cultural change whereby the risk assessor 'has to lose the "tick the box" mentality and get used to assessing risk'. [758] With regard to risk-based regulation, the danger in this respect is that the assessor will simply make an assessment of the situation as he did before, and fill in the forms in accordance with this assessment, thus "reverse engineering" the process.[759] Similarly, controllers will be inclined to use a preconceived notion of risk when performing the data protection impact assessment. The implementation of a system for the identification and enforcement of risk mitigation requires a certain amount of knowledge, competence and resource. It also requires an openness to self-evaluate in light of the "right" goals, i.e. the goals which the regular would want to pursue. In the following, it is argued that SMEs often lack the former, while larger corporations and also government departments and agencies may lack the latter.[760]

Research into small and medium enterprises in the UK food safety industry indicates that they would fail to devise appropriate goals and monitoring systems – not due to unwillingness, but because of ignorance or organizational incompetence.[761] They may not know about the risks of their activity and lack the funds to consult experts.[762] The required hazard analysis was often not understood and its terminology incorrectly interpreted: '[t]erms such as "high risk" resulted in a number of businesses ignoring all the requirements because they could not see how their businesses could present "high risk" (all the businesses served what the enforcer would consider high-risk food).'[763] Moreover, SMEs would not engage in self-evaluation and self-monitoring. The researched companies did not educate themselves on the legal requirements and thought of compliance only as doing what the health inspector told them to do during the last inspection.[764] A literature review on the implementation of environmental management systems in SMEs also

---

[753] Badwin, Cave and Lodge (2012) 154.
[754] Badwin, Cave and Lodge (2012) 155.
[755] Badwin, Cave and Lodge (2012) 155.
[756] Baldwin, Cave and Lodge (2012) 140.
[757] Baldwin, Cave and Lodge (2012) 148-149.
[758] **This commonly cited concern was expressed by the Financial Services Authority in an interview with Julia Black.** See J Black, 'The Development of Risk Based Regulation in Financial Services: Canada, the UK and Australia: A Research Report' (2004) ESRC Centre for the Analysis of Risk and Regulation, 28.
[759] Black (2004) 28; Baldwin, Cave and Lodge (2012) 286.
[760] **Of course, SMEs may also pose problems of capture and larger companies or governments may also lack the knowledge and resources. The author does not intend to exclude these arguments.**
[761] Fairman and Yapp (2005) 515.
[762] Fairman and Yapp (2005) 494.
[763] Fairman and Yapp (2005) 507.
[764] Fairman and Yapp (2005) 503-506.

points to ignorance on legal requirements and to the same reactive attitude of regulatees.[765]

Larger corporations or government agencies may have the knowledge and, perhaps, the resources, but, from a systems theory perspective, the fear remains that business managers and regulators have different visions on their regulatory responsibilities.[766] For example, the liabilities attached to legal requirements can be seen as risks which should be managed rather than as 'ethically reinforced prescriptions'.[767] This lends a whole different character to "compliance control", as is evidenced by the business of tax lawyers. The DPIA is even presented as a system for the management of "compliance risks".[768] A similar incongruity could also be expected between government regulators and other government departments or agencies. In Kagan's typology of the way in which government officials apply rules, two variables can be distinguished: emphasis on adherence to rules and emphasis on the realization of organizational ends.[769] Research indicates that the formalistic rule-application which Montesquieu expected is not found in practice; in many government departments or agencies, the interests of the department or agency or of its clients or the citizens are leading.[770] This may be at odds with the rationale of the rules which the regulator wants to enforce. Prime examples are national security agencies, whose organizational end is fostered by the large-scale collection of data, and law enforcement agencies, who may seek redress for victims by loosely applying the conditions for monitoring, vis-à-vis data protection law. For these reasons, regulatees could be called "amoral" or "political",[771] which just goes to say that protection of the public good is never the sole aim of a company or a government department or agency. This affects their capacity to self-regulate for the public interest.[772]

3.4.3 Meta-regulation and enforcement

3.4.3.1 Meta-regulation: an ideal?

Meta-regulation is an attempt to steer regulatees to be both compliant and socially responsible by overseeing the standard-setting and compliance processes of regulatees through meta-evaluation. Under this system, firms are incentivized to carry out rigorous risk management systems. The idea is that regulatees will benefit from dealing with their infringements adequately, instead of concealing them.[773] Meta-regulation has been praised as increasing inspection coverage.[774] Ideally, not only compliance but also "grey areas" such as corporate

---

765 H Aisenberg Ferenhof and others, 'Environmental management systems in small and medium-sized enterprises: an analysis and systematic review' (2014) 74(1) Journal of Cleaner Production 44, 47. See also P Rao and others, 'A metric for corporate environmental indicators for Small and Medium Enterprises in the Philippines: an empirical research'2006 14(5) Journal of Cleaner Production 505; S Burge and W Gaughran, 'Intelligent environmental management for SMEs in manufacturing' (2006) 22 Robotics and Computer-Integrated Manufacturing 566.
766 Baldwin, Cave and Lodge (2012) 152-153.
767 Baldwin, Cave and Lodge (2012) 153.
768 See at footnote 728.
769 R Kagan, *Regulatory Justice: Implementing a Wage-Price Freeze* (Russell Sage Foundation 1978) 6.
770 S Maynard-Moody and M Musheno, *Cops, Teachers, Counselors: Stories from the Front Lines of Public Service* (University of Michigan Press 2003) 9; N Doornbos, 'Wat doen ambtenaren als ze regels toepassen?' in M Hertogh and H Weyers (eds), *Recht van onderop: Antwoorden uit de rechtssociologie* (Ars Aequi Libri 2011) 102-104.
771 cf Kagan and Scholz (1984) 494.
772 See differently Parker (2002) 294. **Parker is optimistic about the capacity of top managers and compliance officers to bring social and business values in alignment. However, it cannot be assumed that a win-win is always possible.**
773 Baldwin, Cave and Lodge (2012) 148-149.
774 Baldwin, Cave and Lodge (2012) 148.

social responsibility and responsible research and innovation can be overseen at a distance. As a result, areas which the legislator could not regulate extensively enough – possibly due to a lack of democratic consensus or due to strong lobbying – can still be subject to government regulation. But will it work?

Parker envisages a mixture of techniques, such as commands, tax breaks, technical assistance, naming, shaming and faming, and the reward of less government inspections or more leeway.[775] Clear rules on what is required and what will be enforced help build commitment amongst regulatees.[776] She also calls for both public and private enforcement.[777] A robust enforcement system is indeed necessary to make meta-regulation successful. The General Data Protection Regulation includes a command to adopt a risk management system, although the Commission and the Council versions do not include the compliance review. The rules lack clarity, but this can be remedied through guidance documents and regulatory conversations. The GDPR does not provide for market-based incentives such as tax breaks and technical assistance, but the other techniques Parker relies on could be adopted during public enforcement: the regulator can make compliance performance public and can also bargain by conceding on the potentially extensive command of Article 33.[778] The available types of enforcement are further discussed below.

3.4.3.2 Private enforcement as a second-best solution but useful supplement

The GDPR allows for a mixture of public and private enforcement of the data protection impact assessment and subsequent risk mitigation. Economic analyses indicate that the combination of both types is likely more efficient in reaching an optimal level of enforcement, under which the cost of enforcement is equal to the overall public benefit, than sole reliance on one or the other.[779] Administrative agencies are often limited by insufficient funding, which generates an 'enforcement gap'. Private enforcement can function as a much needed supplement.[780] Because private enforcement is difficult to set at an optimum level, it is a second-best solution. In a system of public enforcement, the fines can be set above the social cost of the activity to make up for the fact that the probability of apprehension and conviction is not 100 %.[781] However, Yeung argues that this same mechanism to achieve deterrence has an unwanted side-effect in a system of private enforcement. This is firstly because victims may be too eager to sue if the courts award damages which are higher than the social cost of the activity, leading to over-enforcement. As a result, 'the total cost of litigation may not justify the overall public benefit'.[782] Secondly, the free rider problem may lead to under-enforcement. A court ruling condemning a certain activity offers a useful court precedent for those who did not litigate. It can be used to negotiate a payment out of court. As a result, individuals are incentivized to wait for someone else to take the costs and risks involved with litigation.[783]

In practice, tort liability is surely more likely to have an under-deterrent than an over-deterrent effect, especially in the absence of punitive damages. A victim needs to start judicial proceedings,

[775] Parker (2002) 245, 256, 267-270; Baldwin, Cave and Lodge (2012) 149-150.
[776] Parker (2002) 248.
[777] Parker (2002) 245, 256, 267-270; Baldwin, Cave and Lodge (2012) 149-150.
[778] Hawkins (1984) 122; Section 3.2.2.4. **Hawkins already remarked that if the regulator wants to bargain, he needs strict rules to bargain with.**
[779] Yeung (1998) 591-692.
[780] Yeung (1998) 590.
[781] W Landes and R Posner, 'The Private Enforcement of Law' (1975) 4(1) Journal of Legal Studies.
[782] Yeung (1998) 592.
[783] Yeung (1998) 591.

the damage must be estimated at a deterrent level, and the courts must develop a standard of conduct which needs to be violated for the payment to take place. For similar reasons, court-enforced liability rules were not sufficient to address pollution.[784] The enforcement costs for individuals may be high, as a result of which many victims may not seek compensation: there may be evidential difficulties, victims may lack the resources to start legal proceedings, and, while class actions may offer a solution if individual damages are low, this might not be provided for by the law of a Member State and may also present difficulties in coordinating between the victims.[785] The attempt of Austrian law graduate Max Schrems to sue Facebook is exemplary of the shortcomings of enforcement through tort liability in the area of data protection. Schrems started to pursue Facebook in 2011. He was able to secure financial backing for his attempt to hold Facebook to account for its violations of EU data protection law through a class action, seeking 500 Euros in damages per user. Even as a class action lawsuit of over 25.000 participants, the total amount of damages can hardly be called deterrent. On the 30th of June 2015, the Viennese court of first instance denied the class action for lack of jurisdiction by finding that Schrems is not acting as a consumer. This ruling implies that Schrems needs to file charges against Facebook at its European headquarter in Ireland.[786] He sees the lawsuit as an experiment to see whether the right to the protection of personal data can be enforced: 'While it is clear by now, that no normal citizen is able to follow through with such a proceeding, we are still working to get our final decision today. We want to know if our fundamental rights are respected and enforced against tech giants like Facebook, or if our rights are only existing on the paper'.[787]

The insurance system could further lower the deterrent effect of liability rules, although this can also be avoided. The availability of insurance may spread risks widely and thereby undermine the deterrent effect of the tort system.[788] However, if activities which are inherently risky are only covered under high premiums, this would make these activities less attractive. Moreover, insurance companies can influence the degree of care or recklessness exerted by their clients through deductibles or by differentiating premiums on the basis of the claims record of the insured.[789]

3.4.3.3 The strengths and weaknesses of deterrence- and compliance-oriented public enforcement

The duty to conduct a data protection impact assessment and to carry out risk mitigation cannot always be enforced through sanctions. Deterrent enforcement strategies are only available to supervisory authorities if the conduct is in breach of the GDPR of if the power to prohibit processing operations during or after a prior consultation is broadly interpreted. Moreover, the vague norms of the DPIA are more in tune with a compliance-oriented approach. In short, this

---

[784] S Breyer, *Regulation and its reform* (Harvard University Press 1982) 177.
[785] Baldwin, Cave and Lodge (2012) 127.
[786] Europe versus facebook, 'Privacy Class Action against Facebook: Viennese Court forwards "hot potato' <http://www.europe-v-facebook.org/sk/PR_LG_en.pdf> accessed 15 September 2015.
[787] Europe versus facebook, 'Objectives' < http://europe-v-facebook.org/EN/Objectives/objectives.html> accessed 15 September 2015.
[788] M Trebilcock, 'The Social Insurance–Deterrence Dilemma of Modern North American Tort Law: A Canadian Perspective on the Liability Insurance Crisis?' (1987) 24 San Diego Law Review 929; Baldwin, Cave and Lodge (2012) 127-128. **It does help compensate the victims of offenders with shallow pockets.**
[789] R Schwitters, 'Wat zijn de maatschappelijke gevolgen van een instrumenteel aansprakelijkheidsrecht?' in M Hertogh and H Weyers (eds), *Recht van onderop: Antwoorden uit de rechtssociologie* (Ars Aequi Libri 2011).

means that the DPIA is not very suitable to induce calculative regulatees to be compliant and mitigate risks.

According to the proponents of the deterrent approach, strict sanctioning is the best way to effectuate the desired behavioural change in calculative regulatees. The bounded rationality of individuals means that top management cannot make rational cost-benefit analyses about everything, so the risk of non-compliance will need to be brought to their attention.[790] Tougher enforcement strategies have led larger corporations to 'hire full-time experts to keep up with the regulations and to devise programs to "keep the company out of trouble"'.[791] The probability that a sanction will be imposed and the severity of the sanction will influence analyses of the costs and benefits of compliance.[792] Not every instance of non-compliance can be traced back to a cost-benefit analysis, though; it may also be 'the result of 'irrationalities' from sources such as poor training and ill-organization'.[793] SMEs in particular may simply be ignorant or organizationally incompetent, which should be met with education rather than fines.[794] Ayres and Braithwaite argue that a deterrent approach must be available as a back-up option for when corporations turn out to be motivated by profit and seek to avoid regulation.[795] It is also in line with really responsive regulation for regulators to be able to adapt the enforcement strategy to the attitude they are confronted with.[796]

However, precise rules which are enforced by a deterrent hand overshoot the mark if they lead to creative compliance and evasion. They may cause regulatees to devise ways to escape substantive compliance,[797] to shift responsibility to other actors, or to evade the reach of the regulation.[798] The GDPR attempts to avoid these pitfalls. It clearly ascribes responsibility to any entity which determines the purposes, conditions and means of the processing operation,[799] and makes jurisdictional evasion very difficult.[800] Many of its norms are vague so as to avoid creative compliance, while other rules (such as purpose specification) are specific and can easily be enforced. The DPIA is one of the vague norms. This means that it is more difficult to evade, but that it cannot be enforced as strictly.[801] Regulatees will find it unreasonable if vague principles are strictly enforced and there is more room for debate and negotiation, so supervisory authorities will have less leverage during the regulatory conversations in the face of recalcitrant regulatees. The boundaries may need to be set through lengthy and costly judicial review.[802] Precise rules lend themselves better to deterrent enforcement, but they can be evaded through creative compliance, which is met by writing more specific rules, which quickly become

---

790 Parker (2002) 69-70.
791 E Bardach and R Kagan, *Going by the Book: the problem of regulatory unreasonableness* (Temple University Press 1982, 5th ed) 95. See also Baldwin, Cave and Lodge (2012) 240.
792 Centrum criminaliteitspreventie veiligheid, 'Tafel van Elf' < http://www.it11.nl> accessed 1 September 2015. See also Baldwin, Cave and Lodge (2012) 240.
793 Baldwin, Cave and Lodge (2012) 240-241.
794 Fairman and Yapp (2005) 503, 515.
795 Ayres and Braithwaite (1992) 24-25. **Sometimes firms are 'motivated by a sense of social responsibility', which would be undermined by punitive enforcement. This is one of the reasons why the regulator should start with a persuasive approach.**
796 Baldwin and Black (2007) 3-4; Baldwin and Black (2010) 181. See also Kagan and Scholz (1984).
797 Section 3.4.1.1.
798 Baldwin, Cave and Lodge (2012) 241.
799 GDPR, art 4(5); GDPR Commission and Parliament version, arts 26(4) and 24. See also section 2.3.
800 GDPR, art 3.
801 Black (2008) 432 and 439; Black (2010) 8; Baldwin, Cave and Lodge (2012) 303.
802 Black, Hopper and Band (2007) 194-200.

outdated.[803] This is a dilemma for the deterrent regulator which compliance approaches try to avoid. Ayres and Braithwaite hope that if the regulator starts with a persuasive approach, the game of cat-and-mouse can be circumvented.[804]

According to the proponents of compliance approaches, compliance strategies are better at fostering information flows between regulators and regulatees, at educating regulatees to think constructively about how to comply, and at encouraging firms to achieve substantive compliance.[805] It is particularly important to nurture the compliance capacity and the compliance professionalism of regulatees by targeting their in-house corporate compliance systems and by developing standards for compliance officers.[806] The GDPR provides a framework to achieve these aims through the data protection impact assessment and other reporting requirements, the prior consultation, and the presence of data protection officers. The DPIA can be seen as a way to avoid minimal compliance by stimulating controllers to think about the grey areas in terms of risk mitigation. This leads to a system to address risks which is not always enforceable through fines, but which does nudge in the direction of substantive compliance through education and persuasion.

However, this would not have the desired effect on regulatees who simply do not have the capacity to self-evaluate, nor on regulatees who need to be incentivized by a high cost of non-compliance. It would have been preferred if the regulator could also offer subsidies such as tax breaks or technological assistance to help regulatees which do not have the resources to comply. Further, Ayres and Braithwaite already note that if 'the privilege of persuasion' is abused, the regulator should make use of its powers to sanction the regulatee.[807] The DPIA does not always afford supervisory authorities with this option.

At the same time, though, it is not at all clear if calculative regulatees could be induced to mitigate risks if the DPIA was drafted differently. A duty to address risks to the rights and freedoms of individuals would only be able to effectuate a change in the calculative if it is remarkably well-drafted. The duty would need to avoid the under-inclusiveness which allows for creative compliance and be resistant to technological turbulence, while being detailed enough to be monitored and enforced in an affordable manner. The power to enforce agreements on the level of risk mitigation during the prior consultation might be a way out of the regulatory dilemma regarding rule precision. Although Article 33 is vague, the level of discretion of regulatees can be diminished through regulatory conversations; and if these take place during the prior consultation, the Commission and the Parliament version might allow them to be enforced. Indeed, they empower the supervisory authority to ensure compliance with prior consultations.[808] If the final version of the General Data Protection Regulation would clarify that this includes not only compliance with a prohibition made during a prior consultation, but also sees to agreements struck with the regulatee, a solution is offered: open norms which can be enforced, if necessary, by a deterrent hand. However, the supervisory authority would need to bluff, and a calculative and informed controller, aware that the reach of the command does not extend so far, might call his hand.

---

[803] Ayres and Braithwaite (1992) 26.
[804] Ayres and Braithwaite (1992) 26.
[805] Baldwin, Cave and Lodge (2012) 240.
[806] C Parker, 'Reinventing Regulation within the Corporation: Compliance-Oriented Regulatory Innovation''(2000) 32(5) Administration & Society 529.
[807] Ayres and Braithwaite (1992) 26, 36 and 40.
[808] GDPR Commission and Parliament version, art 53(1)(d); Section 2.6.2.1.

Moreover, the resources and fines which are available to supervisory authorities[809] may not allow a deterrent approach, nor the mix of enforceable negotiations. Given that the value of the data of EU consumers has been estimated at 315 billion Euros in 2011,[810] non-compliant controllers should face substantial fines or other sanctions. The regulator needs sufficient resources to detect undesirable or non-compliant behaviour, to engage in negotiations, and to impose the penalty. It also has to be empowered to issue sanctions which are high enough.[811] Unfortunately, the European legislature was unable to provide the supervisory authority with either. Given the difficulties with rule precision and the allocation of sufficient resources and sanctions, the regret about the limits of the DPIA to change the behaviour of calculative regulatees should not overshadow the celebration of its capacity to induce more willing regulatees to reach substantive compliance.

2.4.3.4 Basing risk-based regulation on DPIA reports

Risk-based frameworks can help regulators allocate their resources effectively by focussing on risky controllers or risky processing operations. Any risk-based framework must clearly articulate the objectives to which risks may be posed and the types of risks that the regulated activity may present thereto.[812] It requires a scheme for detecting and identifying key risks to the regulatory objectives and for pinpointing the causes or creators of those risks. Only then can important problems be picked up.[813] The regulator needs to determine what type of risks it is prepared to tolerate and at what level – a difficult exercise, as these decisions are often driven by political considerations.[814] Further, the regulator must develop a system for assessing and scoring the risks.[815] The envisaged function of the DPIA in this context is that it could help indicate which operations are risky. The fact that controllers will conduct a risk assessment themselves and only need to do a prior check if their assessment points to high risks, is considered more effective than the current notification system because the regulatees's self-assessment can be used by the regulator as an indication of the level of riskiness. However, this implies a trust in their capability to self-assess and in the comparability of the subsequent reports.

The Article 29 Working Party wants supervisory authorities to target the areas of greatest risk, but also states that enforcement 'may imply challenging risk analysis, impact assessments as well as any other measures carried out by data controllers'.[816] Indeed, the DPIA reports should not be taken at face value. Self-reported performance data may not be robust and should therefore be audited; it may "hit the target but miss the point".[817] More fundamentally, the reports will not be comparable because there is no clear framework for the assessment and

---

[809] Section 3.4.1.2.
[810] European Data Protection Supervisor, 'Preliminary Opinion of the European Data Protection Supervisor: privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' (March 2014) <https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/big_data> accessed 6 September 2015, 8-9. See also V Monga, 'The Big Mistery: What's Big Data Really Worth?' (12 October 2014, The Wall Street Journal) <http://www.wsj.com/articles/whats-all-that-data-worth-1413157156> 6 September 2015.
[811] Baldwin, Cave and Lodge (2012) 239-240.
[812] Baldwin, Cave and Lodge (2012) 281-282.
[813] Sparrow (2000) 133.
[814] Baldwin and Black (2010) 184.
[815] Baldwin, Cave and Lodge (2012) 282.
[816] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', 4.
[817] G Bevan and C Hood, 'What's measured is what matters: Targets and gaming in the English public health care system' (2006) 84(3) Public Administration 517.

because, in any case, the assessment is not objective. The supervisory authority could communicate the system it uses to assess and score risk, requiring DPIAs to be conducted under the same format. However, even if a uniform system for assessing and scoring the risks is provided through later guidance, the DPIA reports cannot be comparable. Because the assessments are qualitative – risks to rights and freedoms are not quantifiable – the outcome depends greatly on the subjective judgments made during the assessment.[818] To assess risks properly, controllers need to have in mind a level of protection and a level of precaution.[819] But these levels are not determined by the GDPR and will be difficult to fix by supervisory authorities. It may not even be desirable to require a static understanding of risk which cannot readily respond to changes in risk perception in society.[820] If a report points to high risks, it could present a case which needs to be prioritized, but in general, the reports should not be treated as a reliable and comparable indicator of the level of riskiness of a project.

Data protection officers could be trained to assess risks in the way the regulator thinks is best. The Parliament and the Council require them to be involved in the data protection impact assessment.[821] Note, though, that not every controller is required to have a data protection officer. The requirements differ in each version of the GDPR, whereby the Council leaves it to other EU or national laws to regulate.[822] The success of the DPIA's role in risk-based regulation thus depends not only on the ability of data protection officers to assess risks properly and uniformly, but also on their appointment and actual involvement in the DPIAs. It is highly unlikely that data protection officers would succeed in making DPIA reports reliable and comparable.

Moreover, while risk-based regulation can help allocate resources, it suffers from a number of difficulties. Firstly, it is not at all clear whether it is helpful to focus on a particular risk and define it as the problem.[823] What types of risks are targeted? Is the conduct of a firm considered in isolation or are the risks better viewed in conjunction with each other?[824] Judgments have to be made on how risks are designed and grouped.[825] The concern is that the focus is on individual silos of risk, as a result of which systemic and cumulating risks are neglected.[826] The risk framework may also make regulators resistant to changing perceptions of risk in society because it has become difficult to adapt.[827] Another weak point of risk-based regulation ties in to the criticism of DPIA reports as incomparable and possibly unreliable. Risk assessment systems require 'politically contentious judgments' to be made, but these are 'hidden away behind the apparently neutral language of the risk assessment model'.[828] The result is an illusion of transparency and neutrality.

---

818 Baldwin and Black (2010) 185.
819 Section 2.5.2.1.
820 **Baldwin, Cave and Lodge make this argument with regard to the risk framework of the regulator**. Baldwin, Cave and Lodge (2012) 291.
821 GDPR Parliament version, art 33(3a); GDPR Council version, art 33(1a).
822 GDPR, art 35.
823 Baldwin, Cave and Lodge (2012) 268.
824 Baldwin, Cave and Lodge (2012) 268.
825 Baldwin, Cave and Lodge (2012) 283.
826 Baldwin, Cave and Lodge (2012) 283.
827 Baldwin, Cave and Lodge (2012) 291.
828 Baldwin, Cave and Lodge (2012) 293-294.

2.4.3.5 A good mix of preventative, act-based and harm-based regulation

The enforcement possibilities surrounding the DPIA include preventative, act-based and harm-based actions. The duty to carry out a DPIA and its enforcement should prevent non-compliance or potentially harmful situations. However, if this fails, enforcement action can focus on the implementation of risk mitigation measures or follow the occurrence of harm, as is the case with private enforcement on the basis of tort law.

Preventative measures sometimes offer a "lighter" way of regulating conduct.[829] Indeed, if controllers avoid dangerous situations or harm by assessing and mitigating risks, serious regulatory intervention and litigation is also be avoided. At the same time, the occurrence of harm is prevented. It can also be less costly for the regulatee to prevent harm. The DPIA helps controllers ensure that there is still time to adjust the outcome; they can get it right from the start.[830] This avoids the situation in which a new product or project is developed, only to be criticized by the legal department or sanctioned by the supervisory authority. Act-based intervention may be more suitable if prevention would be so expensive that it does not weigh up to the benefits. The DPIA system largely avoids this inefficiency, though: in these situations, calculative controllers would not actually carry out and implement the DPIA, so the supervisory authority is left to intervene at the act stage.

Harm-based intervention is generally less useful. There may be difficulties in holding individuals or controllers to account for the harm they caused. This is particularly so if the harm is the result of cumulative actions or if the act is easier to identify than the harm.[831] In the case of data protection, harm can indeed be diffuse – for example, detailed profiles are based on many separate instances of data processing – and difficult to identify – the data security practices of a company are more easily ascertained than whether a security breach has taken place. As a result, private enforcement through tort law again turns out to be a second-best option.

3.4.4 Conclusion

Throughout the above sections, a distinction was made between the modality harnessed by a piece of regulation and its enforcement, and between the law's command and self-regulation. However, these distinctions are not absolute. Rules have to be interpreted, applied and enforced; commands need to be translated to a given situation in a manner reminiscent of self-regulation, and the distinction between command and self-regulation has a bearing on the available methods of enforcement. In other words, the limits of the use of these categories as heuristic devices have become apparent. This conclusion attempts to combine the various categories to give an overall picture of the strengths and weaknesses of the DPIA as a regulatory tool.

The DPIA should be seen as part of a larger risk management program by which regulatees regulate themselves. It is meta-regulation: it regulates the way in which controllers manage risk, and as such extends beyond technical legal compliance into "grey areas" such as corporate social responsibility. Article 33 is over-inclusive rather than under-inclusive, and vague rather than

[829] Baldwin, Cave and Lodge (2012) 244.
[830] D Wright, 'The state of the art in privacy impact assessment' (2012) 28(1) Computer Law & Security Review 54, 55; D Wright and P De Hert, 'Introduction to Privacy Impact Assessment' in D Wright and P De Hert (eds), *Privacy Impact Assessment* (Springer 2012) 5-6; Article 29 Working Party, 'Opinion 01/2012 on the data protection reform proposals' (WP191, 2012), 4.
[831] Baldwin, Cave and Lodge (2012) 245-246.

specific. As a result, creative compliance is not a problem, but regulatees may not understand what Article 33 asks of them because there is no shared meaning. Moreover, it is difficult to enforce, precisely because vague norms are open to debate. The drawbacks of over-inclusiveness can be alleviated through regulatory conversations, which can also be used to foster a shared understanding. However, if the regulatees are not willing to participate in these conversations, they can abuse the vagueness of Article 33 by doing 'what they want without fear of breaching strict rules', in the knowledge that enforcement would be expensive.[832] It is a regulatory dilemma: precise rules are more suitable for deterrent enforcement, but they can be evaded through creative compliance. Ayres and Braithwaite hope that if the regulator starts with a persuasive approach, the game of cat-and-mouse can be avoided – but a deterrent option should be available if the regulatee turns out to be calculative and does not respond in kind. As explained in the following, supervisory authorities cannot make use of an effective deterrent strategy to induce controllers to implement a full risk management program.

Because Article 33 is a vague norm, it must be filled in by the regulatee. To carry out a data protection impact assessment properly, the assessor must envisage an acceptable level of protection and precaution while conducting the assessment. This is the self-regulatory part of the command of Article 33. Moreover, to implement the DPIA, that is, to take adequate mitigating measures, the regulatee must also go beyond what is technically required by the GDPR. The strengths of this self-regulatory approach are that the regulatee may have more knowledge of the risks and how to mitigate them sufficiently, at least tech companies will do with regard to data security; the regulatee can make precise rules which apply to his or her context and can update them swiftly; and the supervisory authority can differentiate between regulatees, holding controllers with lower compliance costs, such as tech-savvy multinationals, to higher standards. The self-regulatee may also be more committed to the self-drafted rules, although this has little value if the rules are set too low. In the case of big data analysis, self-regulated standards would probably be at an unacceptably low level precisely because companies are incentivized to collect, process and re-use data as much as possible. Supervisory authorities will probably need to negotiate continually to prevent this. The other side of the coin is that the DPIA provides a framework in which negotiations can take place about legal requirements and the "grey areas", thereby stimulating controllers to go beyond minimum compliance by reaching a proper level of risk mitigation, even if this is not technically required. This is just what the supervisory authority needs to get willing and somewhat competent controllers to achieve substantive compliance, but it is much less likely to work for calculative controllers.

A stakeholder consultation would add a deliberative component to the drafting of self-regulatory standards and may raise the level of protection which is aimed for. However, one can be sceptical as to whether a consultation will be conducted at all, since the legal requirement is easily avoided. If a controller does decide to seek the views of data subjects, it may take this as an opportunity to engage in reputational management. The plurality of views and interests may also lead to indecisiveness. Nonetheless, the existence of self-regulatory standards is better than no standards, especially if they are the result of more or less deliberative processes. From this perspective, self-regulation is a supplement which has added value in those areas in which the democratic and political processes could not provide durable and precise legal standards.

The implementation of a system for the assessment of risks and the implementation of risk

[832] Black (2008) 432 and 439; Baldwin, Cave and Lodge (2012) 303.

mitigating measures does require a certain amount of knowledge, organizational competence and openness, and the enforcement options are limited. In other words, it requires a certain faith 'in the capacity and commitment of the corporation to self-regulate in the public interest'.[833] SMEs have been found to be ignorant on legal requirements and to display a reactive attitude, under which precise directions are followed, but an ongoing system of self-evaluation is not properly implemented. Moreover, many if not all controllers, both public and private, will not be open or willing to self-evaluate only in light of the "right" goals, i.e. the goals which the regular would want to pursue, because the controller has its own interests to fulfil. Privacy, in particular, may not be one of the values which data-driven corporations want to pursue. Mark Zuckerberg famously asserted in 2010 that privacy is no longer a social norm.[834] If regulatees cannot set proper goals and evaluate their compliance in accordance with these goals, there is no point to meta-evaluation.

Strict sanctioning could incentivize controllers to reconsider their respect for data protection law and to consult compliance officers, but supervisory authorities cannot use deterrent enforcement strategies to induce controllers to implement a full risk mitigation program; the command does not extend far enough. The compliance approach which *is* available is unlikely to incentivize calculative controllers to conduct proper risk management. Private enforcement through tort law might somewhat alleviate this problem, but suffers from limitations; it is probably only viable as a supplement to fill in a public enforcement gap. If the reach of the command and the accompanying sanctions is extended far enough, deterrent enforcement does become an option across the board. The requirement of privacy by design and by default can be constructed to require mitigation of the risks to the rights and freedoms of individuals. The duty would need to avoid the under-inclusiveness which allows for creative compliance and be resistant to technological turbulence, while being detailed enough to be monitored and enforced in an affordable manner. However, even if the courts and authorities of the Member States would succeed in constructing a well-formulated duty to mitigate risks to the rights and freedoms of individuals, supervisory authorities are limited in their enforcement options by the available resources and moderate sanctions.

Data protection officers can fulfil a valuable role in familiarizing the regulatee with the terminology and the requirements of a risk mitigation system. They can also help generate a "privacy-aware culture" in which the DPIA is regarded as an important part of overall risk management. However, in the absence of severe enough sanctions, the importance of data protection, and the protection of the rights and freedoms of individuals, may not be absorbed by the bounded rationality of top management. It is quite a burden to fully implement a risk management program, and it is only beneficial to controllers if non-compliance and reputation damage are real risks. Unfortunately, given that the fines available for violations of competition law are two to five times higher than those provided for in the different versions of the GDPR, companies whose business model revolves around the collection of data are unlikely to be deterred. Without high enough fines, the threat of stricter audits or more interventionist regulation is quite empty – they would be mere inconveniences. Parker also envisaged a number of competition-based techniques, such a tax breaks and technical assistance, and

[833] Badwin, Cave and Lodge (2012) 152. See also R Baldwin, 'Why Rules Don't Work' (1990) 53 Modern Law Review 321.
[834] B Johnson, 'Privacy no longer a social norm, says Facebook founder' (11 January 2010, The Guardian) <http://www.theguardian.com/technology/2010/jan/11/facebook-privacy> accessed 16 September 2015.

communication-based techniques such as naming, shaming and faming.[835] The GDPR does not provide for the former category of incentives, but the regulator could opt for a policy of making certain compliance performance public, as was done, for example, after the Article 29 Working Party Cookie Sweep.[836] However, naming and shaming or other mechanisms of disclosure to the public only work if the public cares enough *and* has the possibility to vote with their feet by switching to a more privacy-friendly competitor. Calculative controllers will probably find that the cost of implementing a risk management program is not worth the benefit, especially if they have a secure position on the market.

As indicated by the Table of Eleven, not only the severity of the sanction is important, but also the probability that the regulatee is checked and that non-compliant behaviour is detected and the probability that a sanction will be imposed.[837] These factors require that supervisory agencies are allocated enough resources and manage their resources wisely. Supervisory authorities need to be able to conduct investigations and pursue infringements, even though the quality of DPIA's is difficult to check and even though the rules are not clear-cut and can be disputed through lengthy judicial proceedings. The preventative approach which is central to the DPIA can be a smart approach to limited funds: with regard to the controllers which take it seriously, it can prevent enforcement actions and litigation at a later stage. The DPIA has also been presented as facilitating a risk-based approach, under which supervisory authorities focus on risky cases. However, supervisory authorities cannot rely too much on the DPIA reports as an indicator of the actual riskiness of the activity. They may not be robust. They will also lack comparability because the outcomes depend on normative judgments made by the assessor. Data protection officers could play a valuable rule if they can be relied on to provide accurate and somewhat comparable information, but not all controllers need to appoint a DPO, and if they are appointed, they would need to take a central role in the DPIA process in practice. The risk-based approach also suffers from a number of weaknesses more generally. Most importantly, the focus on risk may cause systemic and cumulating effects to be neglected, the bureaucratisation of risk frameworks may make regulators less responsive to the ever-changing levels of risk perception in society, and the language of the risk assessment model can result in an illusion of transparency and neutrality. It is therefore highly uncertain whether the DPIA report can play a role in a risk-based approach, nor whether the risk-based approach should be adopted in the first place.

To conclude, the main strength of the DPIA is that is offers a framework within which regulatory conversations on substantive compliance and additional protection can take place. It can inspire a self-regulatory system of risk mitigation, although this requires a certain level of knowledge and organizational competence, of openness to protect the public good, and a willingness to cooperate. Supervisory authorities will have to engage in constant conversation and negotiation to make sure regulatees understand what to do and aim for high enough standards. This will probably not effectuate the desired behavioural change in calculative controllers: enforcement of the fuzzy norms would be costly, sanctions are not always available, and the fines may not be deterrent with regard to data-driven corporations. More willing regulatees can, however, be educated and bargained with to protect the rights and freedoms of individuals beyond what the law strictly requires, if they are not wholly incompetent. The DPIA should not be celebrated as a

[835] Parker (2002) 245, 256, 267-270; Baldwin, Cave and Lodge (2012) 149-150.
[836] Article 29 Working Party, 'Cookie sweep combined analysis – report' (WP 229 2015), 16.
[837] Section 3.4.1.2.

great achievement of the European legislator in face of the large tech lobby, but its value – however limited – should be recognised. Its meta-regulatory and largely self-regulatory form allows the regulator to negotiate on the risks which democratic and political processes could not address. Controllers who do not calculate the costs and benefits of implementing a risk management system can be guided to do so. While the scepticist will say: 'Which controllers are those?', lamenting the escape of the notorious multinationals, the optimist will point to managers and officials who are more open to persuasion (however many they are).

3.5 Conclusion: functions of the DPIA in light of the regulatory analysis

This section will extrapolate what the above means for the functions identified in section 2.8. Some functions can be readily dismissed as unlikely, but others are revalued or expanded. The strengths identified above can be translated to the previously identified functions. New functions were also considered. Only the DPIA's possible role in risk-based regulation is of a new category, but given the difficulties with the reliability and comparability of DPIA reports, they are unlikely to be able to function as an indicator of risky activity.

3.5.1. Achieving compliance and preventing non-compliance

The application of rules on the ground is not straightforward. They have to be interpreted and applied to the situation at hand. This means that DPIA's function of helping regulatees establish whether their activities will be compliant and what measures should be taken to remedy non-compliance can be highly valuable, especially with regard to the more fuzzy requirements of data protection law. Nonetheless, it was also explained above that vague norms are more expensive and more difficult to enforce; calculative controllers might not be interested in what they are supposed to mean if there is a low chance that it will come to sanctions.

The DPIA and the prior consultation provide a conceptual and organizational framework from which substantive compliance can be negotiated preventatively. The DPIA assumes the conceptual framework of risk management, which can be used to negotiate on the conduct of regulatees. This is accompanied by the prior consultation and the Parliament's compliance review: during these moments of meta-evaluation, negotiations on risk management can take place. Systems theorists would be critical as to whether the DPIA can provide a shared conceptual framework, and some misunderstanding indeed cannot be avoided, but a common understanding among porous semi-autonomous social fields can be fostered through the terminology and the process of the risk assessment.

If the DPIA is embedded in the general risk management processes within the organization, there is a central framework from which possible infringements can be identified and assessed. This may give the data protection officer more of a foothold within the organization to promote compliance, and it might even foster an organizational culture in which the mitigation of risks to the rights and freedoms of individuals is considered an 'organizational requirement'.[838] However, the framework also induces the kind of cost-benefit analysis with regard to compliance that characterises the calculative regulatee. Infringements are seen as risks which can be prevented, mitigated, or accepted, if the cost of addressing them is too high. The Article 29 Working Party has clarified that the interests of the controller do not weigh in during the data

[838] Charikane and others (2014) 155; Wright and De Hert (2012) 'Findings and Recommendations' 476.

protection impact assessment –[839] but this will not prevent that such a cost-benefit analysis will take place.

Perhaps the most obvious characteristic of the DPIA and risk management in general is that it is preventative. The analysis of preventative, act-based and harm-based enforcement clarifies that preventative action can prevent further enforcement action down the line and may be cheaper and more effective than addressing non-compliance and harm after it has materialized.

3.5.2 Enforcement and accountability

It was argued in section 2.8, firstly, that the DPIA provides a framework for controllers to identify measures to demonstrate their compliance. Again, the calculative regulatee might not be sufficiently incentivized to adhere to such a vague norm. DPIA reports were also argued to facilitate supervisory authorities and members of the public to hold controllers to account, However, DPIA reports may not help supervisory authorities to detect instances of non-compliance: they might present the envisaged processing as unproblematic, hiding any issues that could arise. This also affects their use as evidence of wrongdoing during civil proceedings. However, in the rare occasions when a DPIA report is reliable enough to point to undesirable or non-compliant behaviour, it can be used for public and private enforcement. Moreover, DPIA reports can still have an evidentiary function. if the DPIA clearly was not conducted thoroughly enough, the superficial report is evidence that the assessor botched the impact assessment. Finn, Rodrigues and Wright recommend that PIA reports are signed off by senior management to enable individual accountability.[840]

3.5.3 Additional risk mitigation

Compliant data processing operations can still pose risks to the rights and freedoms of data subjects or individuals. The advantage of the DPIA framework is that these risks are not necessarily considered in terms of compliance; in other words, next to "compliance risks" also other risks are considered; regulatees are steered to assess risks, not only to check compliance. This could bring awareness that such risks exist – although they may use preconceived notions of what is risky, so that little to no new knowledge is gained unless the supervisory authority takes an educative role. The awareness might incentivise them to act, especially if the risks might lead to reputation damage. Risk-based regulation can be criticised as focussing only on "silos of risk", which obscures systemic or cumulating problems. In this context, however, the focus on risk does not have a narrowing effect; it enables controllers and regulators to look beyond what the law requires.

The DPIA, together with the prior consultation and the compliance review of the Parliament version of the GDPR, not only provides a framework for communication on compliance, but also on additional risk mitigation. The controller must decide, when assessing risks, what level of protection and precaution to aim for. These standards are not provided by the European legislator – and that may not be so bad, because the risk management of controllers should be responsive to the perception of risk in society. By regulating them through regulatory

[839] Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', 4.
[840] R Finn, R Rodrigues and D Wright, 'A Comparative Analysis of Privacy Impact Assessment in Six Countries', (2013) 9(1) Journal of Contemporary European Research 161, 164.

conversations, they remain flexible. The supervisory authorities can use fundamental rights and data protection requirements such as privacy by design and by default as benchmarks during the negotiations. Also the vague duty to conduct a data protection impact assessment can be used to bargain with. While fundamental rights have a moral appeal but lack practical enforcement possibilities, especially with regard to private entities, the data protection requirements are punishable by moderate fines. During these regulatory conversations, the supervisory authority can also negotiate the actual implementation of measures to mitigate risks above and beyond what compliance strictly requires.

However, a compliance approach to enforcement will have to suffice, unless the courts of the Member States allow the supervisory authorities to interpret the GDPR extensively and stretch the principle of legality.[841] Member States need to decide how much room to give their enforcement agencies. To what extent will they let go of the principle of legality in favour of more effective new governance? The GDPR provides space to allow the "rise of the administrative state" through the DPIA and the prior consultation. This is not necessarily non-legal; following Hart and Tamanaha, law is what is recognised or labelled as law.[842] Moreover, the principle of legality can be supplemented by other values, such as transparency, participation, and accountability.[843] In the meantime, the deterrent effect of public enforcement through tort litigation might throw some weight in the balance.

Even if only willing and able controllers are steered to conduct and implement proper data protection impact assessments, the DPIA system has real added value. It can be regarded as a supplement to the law. As such, it alleviates the limits of the legislative process: concessions to large lobby groups may lead to lower standards, and a lack of consensus on moral issues may lead to indecisiveness. It also provides a way to cope with the limits to the ability of legal rules to regulate under ever-changing circumstances. New risks may pop up which more precise instruments would not have covered and new ideas may arise on what is acceptable and what is not. Although stakeholder consultations are unlikely to be carried out properly, if at all, any protection achieved in the "grey areas" which the law could not reach adds to the realization of the rights and freedoms of individuals.

A meta-regulatory system, through which the government regulates at a distance, could even be speculated to be the only viable form of risk governance the state can undertake in the risk society – if that.[844] The proliferation of man-made risks can hardly be met by a similar proliferation in command-and-control regulation;[845] already the amount of regulation in some regulated areas renders the requirements incomprehensible and resources at government agencies and courts are spread thin. Black argues that for government regulation to be effective, a decentred strategy must be adopted: state actors must make use of the self-regulatory capacity of private actors and regulate through a number of different modalities.[846] However, if we are

---

841 See end of section 2.6.1.2.
842 Hart (1961); B Tamanaha, *A General Jurisprudence of Law and Society* (Oxford University Press 2001).
843 K Van Aeken, 'Regulation & governance-onderzoek in het rechtenonderwijs in Nederland: Stranger in a strange land?' 2015(2) RegelMaat 95, 104.
844 cf U Beck, *Risk society: Towards a new modernity* (Sage 1992).
845 **This assumes that risks should be managed. Risk management can also be criticized as a futile attempt to control the uncontrollable, because risks cannot be fully governed.** See also P O'Malley, *Risk, Uncertainty and Government* (Glasshouse Press 2004), ch 1.
846 Black (2002) 8-9. See also Van Aeken (2015) 100, **who postulates that the need to govern a complex society gave rise to the transformation from government to governance.**

indeed at the point in which consensus-based regulation is needed to achieve regulatory goals, one may wonder if the threat of state intervention – which functions as an important incentive for regulatees to self-regulate properly – is still present. It remains to be seen whether there will be enough pressure for private actors to align their behaviour to the needs of the public interest if the state does not even have the option of introducing command-based regulation which can be enforced with a deterrent hand.

Sources

Van Aeken K, 'Regulation & governance-onderzoek in het rechtenonderwijs in Nederland: Stranger in a strange land?' 2015(2) RegelMaat 95

Aisenberg Ferenhof H and others, 'Environmental management systems in small and medium-sized enterprises: an analysis and systematic review' (2014) 74(1) Journal of Cleaner Production 44

Article 29 Working Party, 'Opinion 01/2012 on the data protection reform proposals' (WP191, 2012)

——, 'Statement on the role of a risk-based approach in data protection legal frameworks' (WP2018, 2014)

Ayres I and Braithwaite J, *Responsive regulation: Transcending the Deregulation Debate* (Oxford University Press 1992)

Baldwin R, 'Why Rules Don't Work' (1990) 53 Modern Law Review 321

Baldwin R and Black J, 'Really Responsive Regulation' (2007) LSE Legal Studies Working Paper No. 15/2007

——, 'Really Responsive Risk-Based Regulation' (2010) 32(2) Law & Policy 181

Baldwin R; Cave M and Lodge M, *Understanding Regulation: Theory, Strategy and Practice* (Oxford University Press 2012)

Bardach E and Kagan R, *Going by the Book: the problem of regulatory unreasonableness* (Temple University Press 1982, 5th ed)

Beck U, *Risk society: Towards a new modernity* (Sage 1992)

Bevan G and Hood C, 'What's measured is what matters: Targets and gaming in the English public health care system' (2006) 84(3) Public Administration 517

Black J, *Rules and regulators* (Clarendon Press 1997)

——, 'Talking about regulation' (1998) 1 Public Law 77

——, 'Critical Reflections on Regulation' (2002) 27 Australian Journal of Legal Philosophy 1

——, 'The Development of Risk Based Regulation in Financial Services: Canada, the UK and Australia: A Research Report' (2004) ESRC Centre for the Analysis of Risk and Regulation

——, 'The Rise, Fall and Fate of Principles Based Regulation' (2010) 17 LSE Law, Society and Economy Working Papers

——, 'What is Regulatory Innovation' in Black J, Lodge M and Thatcher M (eds), *Regulatory Innovation* (Cheltenham 2005)

——, Hopper M and Band C, 'Making a success of Principles-based regulation' (2007) 1(3) Law and Financial Markets Review 191

——, 'Forms and Paradoxes of Principles-based Regulation' (2008) 3(4) Capital Markets Law Journal 425

Breyer S, *Regulation and its reform* (Harvard University Press 1982)

Burge S and Gaughran W, 'Intelligent environmental management for SMEs in manufacturing' (2006) 22 Robotics and Computer-Integrated Manufacturing 566

Burgemeestre B, Hulstijn J and Tan Y, 'Rule-based versus Principle-based Regulatory Compliance' in Governatori G (ed), *Legal Knowledge and Information Systems* (IOS Press 2009)

Centrum criminaliteitspreventie veiligheid, 'Tafel van Elf' < http://www.it11.nl> accessed 1 September 2015

Charikane E, Lagazio M, Raab C, Wadhwa K, and Wright D, 'Integrating privacy impact assessment in risk management' (2014) 4(2) International Data Privacy Law 155

Coglianese C, 'Policies to Promote Systematic Environmental Management' in Coglianese C and Nash J, *Regulating from the Inside: Can Environmental Management Systems Achieve Policy Goals?* (Resources for the Future 2001)

Cohn M, 'Law and regulation: the role, form and choice of legal rules' in Levi-Faur D (ed), *Handbook on the Politics of Regulation* (Edward Elgar Publishing 2011)

Commission, 'Impact Assessment. Accompanying the Documents Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation); and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' SEC(2012)72 final

Daintith T, 'The Techniques of Government' in Jowell J and Oliver D (eds), *The Changing Constitution* (Oxford University Press 1994)

Diver C, 'The optimal precision of administrative rules' (1983-1984) 93 Yale Law Journal 65

Doornbos N, 'Wat doen ambtenaren als ze regels toepassen?' in Hertogh M and Weyers H (eds), *Recht van onderop: Antwoorden uit de rechtssociologie* (Ars Aequi Libri 2011)

Expertisecentrum Rechtspleging en Rechtshandhaving, 'De 'Tafel van elf': een veelzijdig instrument' (2006) <https://www.kcwj.nl/kennisbank/integraal-afwegingskader-beleid-en-regelgeving/6-wat-het-beste-instrument/61/tafel-van> accessed on 15 September 2015

European Commission, 'Cartel Statistics' (2015) <http://ec.europa.eu/competition/> accessed 6 September 2015

European Data Protection Supervisor, 'Preliminary Opinion of the European Data Protection Supervisor: privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' (March 2014) <https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/big_data> accessed 6 September 2015

EuroPrise – the European Privacy Seal for IT Products and IT-based Services <https://www.european-privacy-seal.eu/EPS-en/Home> accessed 1 September 2015

Fairman R and Yapp C, 'Enforced Self-Regulation, Prescription, and Conceptions of Compliance within Small Businesses: The Impact of Enforcement' (2005) 27(4) Law & Policy 491

Finn R, Rodrigues R and Wright D, 'A Comparative Analysis of Privacy Impact Assessment in Six Countries', (2013) 9(1) Journal of Contemporary European Research 161

Gunningham N and Sinclair D, 'Regulatory Pluralism: Designing Policy Mixes for Environmental Protection' (1999) 21(1) Law & Policy 49

Gunningham N, Grabosky P and Sinclair D, *Smart regulation: Designing Environmental Policy* (Clarendon Press 1998)

Hart H.L.A., *The Concept of Law* (Oxford University Press 1961, 2nd ed)

Hawkins K, *Environment and enforcement* (Oxford University Press 1984)

Hutter B, *Compliance: Regulation and Environment* (Oxford University Press 1997)

Johnson B, 'Privacy no longer a social norm, says Facebook founder' (11 January 2010, The Guardian) <http://www.theguardian.com/technology/2010/jan/11/facebook-privacy> accessed 16 September 2015

Kagan R, *Regulatory Justice: Implementing a Wage-Price Freeze* (Russell Sage Foundation 1978)

Kagan R and Scholtz J, 'The criminology of the corporation and regulatory enforcement strategies' in Hawkins J and Thomas J, *Enforcing Regulation* (Kluwer 1984)

Landes W and Posner R, 'The Private Enforcement of Law' (1975) 4(1) Journal of Legal Studies

Lessig L, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harvard Law Review 501

Levi-Faur D, 'Regulation and regulatory governance' in Levi-Faur D (ed), *Handbook on the Politics of Regulation* (Edward Elgar Publishing 2011)

Mascini P and van Erp J, 'Waarom zijn sommige vormen van rechtshandhaving effectiever dan andere?' in Hertogh M and Weyers H (eds), *Recht van onderop: Antwoorden uit de rechtssociologie* (Ars Aequi Libri 2011)

Maynard-Moody S and Musheno M, *Cops, Teachers, Counselors: Stories from the Front Lines of Public Service* (University of Michigan Press 2003)

McBarnet D and Whelan C, 'The elusive spirit of the law: Formalism and the struggle for legal control' (1991) 52 Modern Law Review 848

Monga V, 'The Big Mistery: What's Big Data Really Worth?' (12 October 2014, The Wall Street Journal) <http://www.wsj.com/articles/whats-all-that-data-worth-1413157156> 6 September 2015

Morgan B and Yeung K, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press 2007)

O'Malley P, *Risk, Uncertainty and Government* (Glasshouse Press 2004)

Ogus A, 'Rethinking Self-Regulation' (1995) 15(1) Oxford Journal of Legal Studies 97

Ogus A, *Regulation: Legal Form and Economic Theory* (Hart Publishing 2004)

Oude Vrielink M, 'Wanneer is zelfregulering een effectieve aanvulling op overheidsregulering?' in Hertogh M and Weyers H (eds), *Recht van onderop: Antwoorden uit de rechtssociologie* (Ars Aequi Libri 2011)

Parker C, 'Reinventing Regulation within the Corporation: Compliance-Oriented Regulatory Innovation''(2000) 32(5) Administration & Society 529

Parker C, *The Open Corporation: Effective Self-regulation and democracy* (Cambridge University Press 2002)

Pearce F and Tombs S, 'Ideology, hegemony, and empiricism' (1990) 30(4) British Journal of Criminology 423

Pearce F and Tombs S, 'Policing corporate "Skid rows": A reply to Keith Hawkins' (1991) 31(4) British Journal of Criminology 415

Rao P and others, 'A metric for corporate environmental indicators for Small and Medium Enterprises in the Philippines: an empirical research'2006 14(5) Journal of Cleaner Production 505

Rodrigues R, Wadhwa K and Wright D, 'Developing a privacy seal scheme (that works) (2013) International Data Privacy Law 100

Schwitters R, ‘Wat zijn de maatschappelijke gevolgen van een instrumenteel aansprakelijkheidsrecht?’ in Hertogh M and Weyers H (eds), *Recht van onderop: Antwoorden uit de rechtssociologie* (Ars Aequi Libri 2011)

Scott C, ‘Regulation in the age of governance: The rise of the post-regulatory state’ in Jordana J and Levi-Faur D, *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance* (Edward Elgar Publishing 2004)

Shavell S, ‘The Optimal Structure of Law Enforcement’ (1993) Journal of Law and Economics 255

Sparrow M, *The Regulatory Craft* (Brookings Institution Press 2000)

Tamanaha B, *A General Jurisprudence of Law and Society* (Oxford University Press 2001)

Terms of Service; Didn’t Read <https://tosdr.org/> accessed 1 September 2015.

Trebilcock M, ‘The Social Insurance–Deterrence Dilemma of Modern North American Tort Law: A Canadian Perspective on the Liability Insurance Crisis?’ (1987) 24 San Diego Law Review 929

Warren A and others, ‘Privacy Impact Assessments: international experience as a basis for UK Guidance’ (2008) 24(3) Computer Law & Security Report 233

Weber R, 'Symposium on EU Data Protection Reform: Privacy management practices in the proposed EU regulation' (2014) 4(4) International Data Privacy Law 290

Witteveen W, ‘Alternatieve regulering: de vele gezichten van de wetgever’ in Witteveen W, Giesen I and de Wijkerslooth de Weerdesteijn J, *Alternatieve regulering* (Kluwer 2007)

Wright D, 'Should privacy impact assessments be mandatory?' (2011) 54(8) Communications of the ACM 121

——, 'The state of the art in privacy impact assessment' (2012) 28(1) Computer Law & Security Review 54

——, 'Making Privacy Impact Assessment More Effective' (2013) 29(5) The Information Society: An International Journal, 313

Wright D and De Hert P, ‘Introduction to Privacy Impact Assessment’ in Wright D and De Hert P (eds), *Privacy Impact Assessment* (Springer 2012)

——, ‘Findings and Recommendations’ in Wright D and De Hert P, *Privacy Impact Assessment* (Springer 2012)

Wright D, Gellert R, Gutwirth S and Friedewald M, ‘Precaution and privacy impact assessment as modes towards risk governance’ in von Schomberg R (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Field* (European Commission 2011)

Yeung K, ‘Privatising competition regulation’ (1998) 18(4) Oxford Journal of Legal Studies 581

——, *Securing compliance* (Hart Publishing 2004)

——, ‘Government by publicity management: Sunlight or spin’? (2005) Public Law 360

4 Conclusion

This conclusion combines the insights from the legal analysis with those from the regulatory analysis. In the preceding two chapters, a number of potential functions of the data protection impact assessment were discerned, which are first presented here. Consecutively, their contribution to data protection regulation will be assessed in light of the aims of the data protection reform and the context of big data.

4.1 The functions of the data protection impact assessment from a legal and a regulatory perspective

The DPIA can help controllers to establish whether an envisaged processing operation would be compliant with data protection law and what they should do to adhere to the GDPR. Conducting a DPIA provides them with a description of the project and requires them to assess compliance. Article 33 also requires controllers to identify measures to ensure the protection of personal data, requiring them to translate data protection law to the situation at hand. This can help controllers establish what they should do to achieve compliance, which is particularly valuable with regard to the vaguer principles of data protection. Moreover, by conducting a risk assessment, the DPIA brings controllers one step closer to achieving compliance; data protection requirements such as the compatibility test need controllers to understand and weigh the possible impact of their operation. It is a preventative measure: if compliance risks are identified and mitigated, non-compliance and the harm which can arise therefrom is prevented.

Supervisory authorities can use the organizational and conceptual risk management framework provided by the DPIA to negotiate on the conduct of regulatees, whereby the prior consultation and the compliance review provide moments of (meta-)evaluation. The review by the supervisory authority will incentivize also less willing controllers to use the DPIA to establish compliance; processing which would not be compliant can be prohibited during the prior consultation. However, unless the supervisory authority receives notice that a processing operation poses risks, it will have to gain knowledge that a controller is planning a risky project. If the processing stays under the radar of the authority, it is not afforded the opportunity to use the framework provided by the DPIA and the prior consultation.

Similarly, the process of conducting a data protection impact assessment may provide an organizational setting within which the data protection officer can review compliance and from which a switch in organizational culture towards data protection-friendliness can take place. The DPIA is more effective if it is embedded in the general risk management processes. However, the conceptual framework of risk management may also induce the regulatee to engage in a cost-benefit analysis: if the cost of mitigation of a compliance risk outweighs the risk itself, then the assessment may lead the regulatee to choose not to be compliant.

The DPIA can also aid accountability by rendering the conduct of controllers more transparent. Firstly, the DPIA asks controllers to identify measures through which they can demonstrate their compliance. A willing controller could take the opportunity to ascertain how to reach the required transparency – but this vague duty can be more easily avoided, as it is hard to check

and difficult to enforce. Further, a reliable DPIA report also provides insight into the (planned) conduct of the regulatee, helping supervisory authorities find instances of non-compliance both before and after they occur. This function is not available under the Council version, though, because it contains a loophole. The DPIA report only needs to be provided once a prior consultation has been started, which the supervisory authority can only do if (it knows that) the DPIA report points to high risks. Nonetheless, the DPIA report can also serve as evidence during tort litigation, helping victims to hold controllers to account after harm has occurred. Both of these functions only occur if the DPIA report does not hide the issues which could arise. On the other hand, if the report presents a risky processing operation as unproblematic, this is evidence that the data protection impact assessment was blotched – and the assessor can be held to account for failing to conduct a proper DPIA.[847]

The framework of the DPIA not only induces controllers to establish compliance and provides a channel to communicate on their adherence to the GDPR, but also helps them gain awareness of the risks posed by the processing and offers a framework through which the supervisory authority can bargain on additional risk mitigation. Compliant processing can still pose risks to the rights and freedoms of individuals. The DPIA makes controllers aware of these risks and of how to mitigate them – although they must identify the risks and their remedies themselves, which requires them to set important benchmarks: when is a threat so severe and likely that it needs to be assessed as a risk, what level of knowledge is necessary to say that a threat has a certain probability and severity, and what level of protection should the measures achieve, i.e. what level of residual risk is acceptable. Only the Parliament version requires controllers to implement the measures which they identify. However, because there is no set level of protection, even the Parliament version does not contain a legal requirement for the measures to actually mitigate risks to the rights and freedoms of individuals. The public enforcement options are limited. The power to prohibit risky processing could be stretched to encompass situations in which the GDPR is not technically violated, but this is a balancing act between the principle of legality and rights protection which Member States will need to make. Controllers face liability for harm arising from compliant conduct under the Commission or Parliament version or under national tort law, if victims like Schrems choose to take the lengthy and costly path of pursuing their claim, but only acts of non-compliance can be sanctioned by a supervisory authority. Supervisory authorities may be left only with the power to persuade and negotiate. They can bargain for additional protection more successfully, though, in terms of risk instead of compliance. The DPIA enables controllers and regulators to look beyond what the law technically requires. Nonetheless, in the absence of deterrent sanctions or liability damages, calculative controllers are very unlikely to be induced to provide additional rights protection – especially if the risk of reputation damage is low.

By regulating the regulation of risk, the DPIA also helps the legislator cope with creative compliance and technological turbulence. As society and the technology are in constant flux, laws can become outdated quickly; technical compliance may no longer meet the regulatory goals of the current legislator. While the legislative process is lengthy and produces laws which may not connect to a particular situation, self-regulation allows for standards which are tailored to the context and which can be swiftly updated. Meanwhile, the regulator can issue guidance

[847] **While the Parliament version empowers supervisory authorities to sanction controllers for not carrying out a DPIA properly, the Commission and the Council version only allow sanctions if a DPIA is not carried out at all.**

and negotiate on the standards which are set. A stakeholder assessment can also lend legitimacy to the political choices made by controllers. Such a meta-regulatory system can also supplement the law where its standards are too vague or too low, perhaps because of regulatory capture or due to a lack of consensus on moral issues.

Lastly, the DPIA can also fulfil a function in light of the free flow of information. Its risk evaluation indicates how extensive the accountability and compliance mechanisms of controllers should be, helping controllers assess how extensive the GDPR's constraints on the free flow of information are in their particular situation. Moreover, by helping controllers get things right from the start, violations are prevented; this also prevents that the processing must be abandoned at a later point in time. Adequate risk mitigation can also prevent more extensive EU legislation – assuming that the EU could intervene with stricter rules to regulate the multitude of threats in the risk society.

4.2 The potential contribution of the DPIA in light of the aims of the data protection reform and the context of big data

The data protection reform aims to meet the challenges posed to data protection law by new technologies.[848] New technologies have made it possible for individuals to easily share information about their behaviour and their preferences, while also giving rise to more elaborate and less easily detectable ways of collecting personal data.[849] It is now possible for 'both private companies and public authorities' to process personal data easily and on an unprecedented scale, which 'increases the risks for individuals' rights and challenges their capacity of keeping control over their own data'.[850] The main concern throughout the Commission's Communication is the effectiveness of data protection law, whereby change is considered the main enemy: '[l]ike technology, the way our personal data is used and shared in our society is changing all the time. The challenge this poses to legislators is to establish a legislative framework that will stand the test of time. [Further,] clarity must exist on the applicable rules and standards that national authorities have to enforce and that businesses and technology developers must comply with. Individuals should also have clarity about the rights they enjoy'.[851]

The Commission and the Parliament are particularly concerned about a lack of transparency towards individuals about how their data is used and about a lack of control of individuals over their data. This undermines trust and confidence of individuals in the online environment, which

[848] Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union' COM(2010) 609 final, 5.
[849] COM(2010) 609, 2; Commission, 'Impact Assessment. Accompanying the Documents Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation); and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' SEC(2012)72 final, 7.
[850] SEC(2012)72, 11. See also Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final, 1.
[851] COM(2010) 609, 18.

harms the digital single market.[852] Individuals should be empowered through the effective enjoyment of data subject rights.[853] However, the realization of these rights 'has become particularly challenging in the online environment, where data are often retained without the person concerned being informed and/or having given his or her agreement to it'.[854] According to the Impact Assessment, this is because data subject rights are expressed in general terms, so the way they should be given effect is not clearly specified.[855] The conditions for consent should also be clarified to ensure that 'the individual is fully aware that he or she is consenting, and to what data processing'.[856] The Parliament also calls for further clarification and specification of the data protection principles. The information obligations, in particular, should be enhanced.[857] If the problem is indeed the lack of specificity of data subject rights, then the DPIA can provide a solution. It requires controllers to ascertain how to apply vague norms, with their data protection officer if there is one, and provides a channel through which its boundaries can be negotiated. Processing operations which are deemed to violate data subject rights can be prohibited. The function of achieving compliance and additional protection of rights, in this case data subject rights, can contribute to data protection regulation by inducing controllers to actually empower users in practice. This would make data protection law more effective without requiring very detailed and specified rules, making data protection law more resistant to technological turbulence.

In the context of big data it is especially important for controllers to analyse what the GDPR requires of them. Big data may challenge or conflict with some of the provisions of data protection law, most notably data minimisation, purpose limitation, and the effective exercise of data subject rights.[858] Rather than finding a statistically representative sample as is needed to test a certain hypothesis, it allows controllers to collect and analyse large amounts of data .[859] However, the GDPR requires them to limit personal data collection to what is necessary for the purposes of the processing and to design products so as to comply with this principle of data minimisation.[860] Controllers also need to effectively anonymize or delete the data when is it no longer necessary to keep it for the specified purposes.[861] Further, purpose limitation constrains the space which is available to look for and act on unanticipated discoveries and predictions.[862] Personal data has to be collected for a specified purpose which is made explicit and prohibits the use of the data for purposes which are incompatible with the specified purpose.[863]

---

[852] European Parliament, 'Personal data protection in the European Union: European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union' P7_TA(2011)0323, paras 11-24; SEC(2012)72, 23-26; COM (2012) 11, 2.
[853] COM(2010) 609, 6-7.
[854] COM(2010) 609, 7.
[855] SEC(2012)72, 32.
[856] COM(2010) 609, 9.
[857] P7_TA(2011)0323, paras 8-9 and 19.
[858] P Leonard, 'Costumer data analytics: privacy settings for 'Big Data' business' (2014) 4(1) International Data Privacy Law 53, 57. cf Information Commissioner's Office (ICO), 'Conducting privacy impact assessments: code of practice' (2014) < https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/> accessed 15 August 2015, 8-9; L Moerel, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof?' (inaugural lecture 2014) 53-54.
[859] Leonard (2014) 57.
[860] GDPR, rec 61 and arts 5(1)(c) and 23.
[861] GDPR, art 5(1)(e).
[862] Leonard (2014) 57.
[863] GDPR, art 5(1)(b).

Moreover, as the number of processing operations increases and as new information can be inferred it becomes more and more difficult for data subjects to stay informed about the ways in which his data is collected and used, let alone to express meaningful consent regarding these processing operations.[864] Even though processing must occur in such a way as to allow an effective exercise of the rights of individuals, including rights of information, access, and erasure and the right to object, the ubiquity of processing operations makes it difficult to use these rights effectively. Further, big data analysis may reveal patterns relating to specific individuals which they could not have foreseen.[865] In the famous Target example, statisticians "guessed", with great accuracy, which of their costumers were pregnant on the basis of changes in purchasing behaviour such as a sudden preference for non-fragranced lotions.[866] Even a refusal to consent can reveal information.[867] Also the complexity of big data analyses makes it difficult to render processing transparent.[868] A lack of transparency prevents individuals from exercising control over their data or from holding controllers to account, as they do not know if their data is being collected or if decisions are being made about them.[869] Transparency towards supervisory authorities is also important; they need to be able to detect non-compliance. Article 22 therefore requires controllers to be able to demonstrate that they are compliant.

Recognising the tension between big data and the principles of data protection, the Article 29 Working Party has even found it necessary to confirm that data protection principles apply to big data processing without limitation.[870] Controllers should take care to ensure that their big data processing operations do not violate the GDPR.

The question is whether the data protection impact assessment would indeed induce controllers to achieve substantive compliance and actually empower data subjects. The data protection impact assessment was intended to stimulate the responsibility of controllers to comply with data protection rules in a proactive manner.[871] However, in all likelihood the main offenders are non-compliant not because of ignorance of what the law requires, but because the rules are not accepted and because the costs of compliance outweigh the benefits. Applying the Table of Eleven, a lack of clarity of the rules is not the problem; the problem most likely lies in the enforcement factors and the cost-benefit ratio. Particularly multinationals may also lack

---

[864] C Kuner and others, 'The challenge of 'Big Data' for data protection' (2012) 2 International Data Privacy Law 47, 48. See also M Hildebrandt, 'Who is Profiling Who? Invisible Visibility' in S Gutwirth, Y Poullet, P De Hert, C De Terwangne and S Nouwt (eds), *Reinventing Data Protection?* (Springer 2009) 243; D Le Métayer and J Le Clainche, 'From the Protection of Data to the Protection of Individuals: Extending the Application of Non-discrimination Principles' in S Gutwirth, R Leenes, P De Hert and S Poullet (eds), *European Data Protection: In Good Health?* (Springer 2012) 323; D Solove, 'Introduction Privacy self-management and the consent dilemma' (2013) 126 Harvard Law Review 1880, 1889-1891.

[865] Article 29 Working Party, 'Statement of the WP29 on the impact of the development of Big Data on the protection of individuals with regard to the processing of their personal data in the EU' (WP221, 2014) 3.

[866] K Crawford and J Schulz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55(1) Boston College Law Review 93, 94-95.

[867] Y Hermstrüwer and S Dickert, 'Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten' (2013)15 Preprints of the Max Planck Institute for Research on Collective Goods, 24.

[868] Leonard (2014) 60.

[869] Information Commissioner's Office, 'Big data and data protection' (2014) <http://ico.org.uk/for_organisations/data_protection/topic_guides/big_data> accessed 26 July 2015, 33.

[870] Article 29 Working Party, 'Statement of the WP29 on the impact of the development of Big Data on the protection of individuals with regard to the processing of their personal data in the EU'.

[871] COM(2010) 609, 7, 11-12. See also P7_TA(2011)0323, paras 26 and 31.

respect for the authority of the enforcement agencies of Member States and find the rules unreasonable. Supervisory authorities can prohibit or limit processing operations, but they need the resources to detect and sanction non-compliant behaviour. Because the norms are vague, their meaning is open to debate and enforcement can be costly and lengthy. Calculative controllers might wager a prohibition in the hope that their conduct will not be detected or that the prohibition will be overturned during judicial review. It would have been valuable if the DPIA could help supervisory authorities use their resources more efficiently. The self-reporting which occurs through the DPIA report might ease their workload, but it cannot be relied on to replace independent investigation. Similarly, the risk-based approach might be a justifiable way to allocate resources and lead to a focus on offenders, but the DPIA reports cannot be a comparable indicator of the risks posed by processing operations. The assessment of the riskiness of processing would still need to be done by supervisory authorities, too.

More fundamentally, even if data subjects are provided with the option to exercise their rights, their actual control over ubiquitous data processing is very limited. As discussed above, the ubiquity and complexity of big data processing makes it difficult for data subjects to use their rights whenever they disagree with a processing operation. It is not only uneconomical, if not impossible, to consider the costs and benefits of every exchange of data;[872] a number of cognitive limitations also limit our ability to assess them rationally.[873] Moreover, with regard to the notorious tech giants, the option to switch to a competitor is severely limited in practice. Data subjects cannot protect themselves against discrimination through their legal rights to forego consent or to object to the processing; nor can they ensure that sufficient security measures are taken to prevent data breaches. For this reason, any additional protection which the DPIA can offer to the "rights and freedoms" of data subjects, instead of only data subject rights, forms a welcome contribution to data protection regulation. The function of compliance should be supplemented by additional risk mitigation. While the travaux préparatoires do not highlight this potential function of the DPIA, the Impact Assessment does note that it can help improve the security of personal data and manage data protection risks.[874]

Risk mitigation is of particular importance for the risky processing operations which big data makes possible. Controllers can make decisions which affect the life opportunities and the autonomy of individuals, treating them differently on the basis of profiles which are constructed with the help of big data analysis. For example, people who might commit a terrorist act are placed on a no-fly list, while 'high-risk individuals' used to be permitted to fly unless there is sufficient evidence that they are actually committing a criminal act.[875] Online personalisation also differentiates between people on the basis of their profiles. The differentiation can occur on the basis of legally protected or sensitive characteristics, even if they were not used as a variable in the dataset. These characteristics may be inferred from other data and influence the preemptive and preferential decisions. For example, if the residents in certain area codes are predominantly from a certain ethnic background, this characteristic may creep into the model

[872] Solove (2013) 1884; B Van Alsenoy, E Kosta and J Dumortier, 'Privacy notices versus informational self-determination: Minding the gap' (2014)28 International Review of Law, Computers & Technology 185, 189.
[873] Solove (2013) 1891; Van Alsenoy, Kosta and Dumortier (2014) 190. See also D Kahneman, *Thinking Fast and Slow* (Farrar, Straus and Giroux 2011).
[874] SEC(2012)72,122.
[875] E Kerr and J Earle, 'Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy' (2013) 66 Stanford Law Review Online 65, 69.

and indirectly reinforce existing prejudices against minorities.[876] Richards and King fear that big data predictions and the companies that wield them will in effect limit our choices and possibilities by nudging, persuading, influencing or restricting our identities to how they were defined in the past, changing how we make decisions about who we are.[877] The way in which big data analysis is used can thus conflict with fundamental rights such as the right to non-discrimination, the right to privacy, and freedom of thought. It can pose risks to these rights and freedoms even if the data protection principles are adhered to. The principle of purpose limitation, for example, is not as protective as it was when the collection or use of data was driven by its purpose. In the data-driven society, controllers can come up with a project and describe a purpose to match.[878]

It is difficult to provide a framework which offers lasting protection to the rights and freedoms of individuals despite changes in technology and the way in which personal data is used and shared in society. Many of the data protection principles are of a general nature, so they need to be specified to be applied. The data protection impact assessment attempts to provide a bridge between the general rule and its application in practice, inducing controllers to achieve substantive compliance under the threat of a prohibition. This is particularly important in the context of big data, as several data protection principles are at odds with the practice of collecting and analyzing large amounts of data to find unanticipated discoveries and predictions. However, the data protection impact assessment is unlikely to induce the notorious tech giants to actually empower data subjects and minimise their data collection. Supervisory authorities would need substantial resources to enforce vague norms. Moreover, even if data subjects are provided with the option to exercise their rights on paper, they will not be able to prevent discriminatory use of (big) data or data breaches, let alone interferences with their autonomy. While the DPIA does not introduce a hard system for risk management, it is a step in the direction of a sound system for the regulation of responsible rights protection by both public and private entities.

[876] Moerel (2014)11; K Waterman and P Bruening, 'Big data analytics: risks and responsibilities' (2014) 4(2) International Data Privacy Law 89, 94.
[877] N Richards and J King, 'Three Paradoxes of Big Data' (2013) 66 Stanford Law Review Online 41, 44; N Richards and J King, 'Big Data Ethics' (2014) 49 Wake Forest Law Review 393, 424.
[878] cf L Moerel and C Prins, 'Further processing of data based on the legitimate interest ground: the end of purpose limitation' TILT website (2015) 2-3.

Sources

Van Alsenoy B, Kosta E and Dumortier J, 'Privacy notices versus informational self-determination: Minding the gap' (2014)28 International Review of Law, Computers & Technology 185

Article 29 Working Party, 'Statement of the WP29 on the impact of the development of Big Data on the protection of individuals with regard to the processing of their personal data in the EU' (WP221, 2014)

Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union' COM(2010) 609 final

——, 'Impact Assessment. Accompanying the Documents Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation); and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' SEC(2012)72 final

——, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final

Crawford K and Schulz J, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55(1) Boston College Law Review 93

European Parliament, 'Personal data protection in the European Union: European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union' P7_TA(2011)0323

Hermstrüwer Y and Dickert S, 'Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten' (2013)15 Preprints of the Max Planck Institute for Research on Collective Goods

Hildebrandt M, 'Who is Profiling Who? Invisible Visibility' in Gutwirth S, Poullet Y, De Hert P, De Terwangne C and Nouwt S (eds), *Reinventing Data Protection?* (Springer 2009)

Information Commissioner's Office, 'Big data and data protection' (2014) <http://ico.org.uk/for_organisations/data_protection/topic_guides/big_data> accessed 26 July 2015

——, 'Conducting privacy impact assessments: code of practice' (2014) < https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/> accessed 15 August 2015

Kahneman D, *Thinking Fast and Slow* (Farrar, Straus and Giroux 2011)

Kerr E and Earle J, 'Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy' (2013) 66 Stanford Law Review Online 65

Kuner C and others, 'The challenge of 'Big Data' for data protection' (2012) 2 International Data Privacy Law 47

Leonard P, 'Costumer data analytics: privacy settings for 'Big Data' business' (2014) 4(1) International Data Privacy Law 53

Le Métayer D and Le Clainche J, 'From the Protection of Data to the Protection of Individuals: Extending the Application of Non-discrimination Principles' in Gutwirth S, Leenes R, De Hert P and Poullet S (eds), *European Data Protection: In Good Health?* (Springer 2012)

Moerel L, 'Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof?' (inaugural lecture 2014)

Moerel L and Prins C, 'Further processing of data based on the legitimate interest ground: the end of purpose limitation' TILT website (2015)

Richards N and King J, 'Three Paradoxes of Big Data' (2013) 66 Stanford Law Review Online 41

——, 'Big Data Ethics' (2014) 49 Wake Forest Law Review 393

Solove D, 'Introduction Privacy self-management and the consent dilemma' (2013) 126 Harvard Law Review 1880

Waterman K and Bruening P, 'Big data analytics: risks and responsibilities' (2014) 4(2) International Data Privacy Law 89