Risk to the Right to the Protection of Personal Data:

An Analysis Through the Lenses of Hermagoras

*István Böröcz**

One of the novelties of the General Data Protection Regulation (GDPR) will be the application of the risk-based approach in European data protection law on a larger scale. Although the Regulation uses the term 'risk' in numerous provisions, it does not answer the question 'What is risk to a right and how should it be assessed?'. Although Article 35 (Data Protection Impact Assessment, DPIA) provides a tool to assess these risks, to keep the GDPR suitable for assessing new technologies, the conduct of a DPIA should be based on solid and clear understanding of the provisions. The applicability and suitability of a risk assessment process is yet to be discovered if the risk relates to a fundamental right. A unified perception of risk to a right is necessary as it is the core element of the risk-based approach, furthermore, a varying perception of risk to a right would undermine the endeavours of the GDPR relating to harmonisation. This contribution elaborates on the attributes of risk to a right and advises a unified understanding of risk to a right and risk to the right to the protection of personal data.

I. Introduction

The drafting of the General Data Protection Regulation (GDPR),[1] which is the prime element of the data protection reform package,[2] has been concluded in April 2016. The Regulation will replace the Data Protection Directive (Directive 95/46/EC)[3] and will evoke noticeable changes in the management of personal data processing operations. The revised principles and new tools will impose stricter obligations on data controllers. While doing so the GDPR aims to increase the level of compliance with the provisions, thus 'protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'.[4] The application of the risk-based approach in European data protection law will be one of the novelties on a larger scale. Reasons behind this innovative approach are the pace of tech-

* István Böröcz, researcher at the Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab), Research Group on Law, Science, Technology & Society (LSTS) at Vrije Universiteit Brussel (VUB). This contribution is partially based on the master's thesis of the author (title: 'The Notion of Risk in Data Protection Law - Can Data Protection Impact Assessment Ensure Compliance?'), written and defended in the academic year of 2015/2016 in the Law and Technology LLM Programme, at Tilburg University [Tilburg Institute for Law, Technology and Society (TILT)], under the supervision of Prof Paul De Hert. The research has been carried out in the context of a project funded by the European Union under the Horizon 2020 Programme: FORENsic evidence gathering autonomous sensor (FORENSOR), grant agreement no 653355. For correspondence: <istvan.mate.borocz@vub.ac.be>.

1 Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[2016] OJ L119/1.

2 The EU data protection reform package consist of the GDPR which will replace the 95/46/EC Data Protection Directive and the Criminal Justice Data Protection Directive, replacing the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60. Legislative initiatives are also related to the reform package, such as the Proposal for a Directive on the use of PNR data or the revision of the Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L8/1 in order to meet the standards imposed by the GDPR and the Directive.

3 Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

4 art 1 (2) GDPR.

nological changes, the increasing number and size of data processing operations of public and private actors and the natural development of different management techniques.[5]

The Regulation will, besides emphasising the notion of risk to the rights and freedoms of the data subject relating to data processing operations, provide a tool to assess them: data protection impact assessment (DPIA), as one of the earliest examples of risk assessment being applied in data protection law. According to Article 35(1) GDPR the data controller shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons.

The goal of the legislator with DPIA was to facilitate compliant processing of personal data.[6] Data protection impact assessment is intended to implement the general risk assessment logic into data protection law, thus systematise and clarify its existing risk assessment logic. DPIA can be conducted *inter alia* as a standalone process or as part of the organisational risk management of the data controllers.[7] It will, prior to the processing, help controllers identify the elements of the data processing operations which might cause adverse effects to the rights and freedoms of the data subject. The term 'risk' became an integral, explicit part of the Regulation: the number of occurrences of the term 'risk' in the Regulation is 75. Although it has a pivotal role during the application of the Regulation, it does not answer the question 'What is risk to a right and how should it be assessed?'

Since the Regulation aims to be future-proof, it should target the highest-level goals where law is still effective.[8] In order to keep the openness for new technologies, the conduct of a DPIA should be based on solid and clear understanding of the provisions. The applicability and suitability of a risk assessment process is yet to be discovered if the risk is a limitation of a fundamental right.[9] The perception of risk to a right raises numerous questions (eg, what are its main attributes and the determining factors of its perception), furthermore the general characteristics of DPIA in the Regulation are not entirely clear.

Article 35 GDPR is triggered when the processing operation is likely to constitute a high risk to the rights and freedoms of natural persons. As the GDPR protects particularly the right to the protection of personal data, this paper aims to provide a detailed description of the attributes of risk to a right, furthermore elaborate on the distinctive marks of risk to the right to the protection of personal data. As a conclusion, it provides a definition of risk to a right and risk to the right to the protection of personal data.

A unified perception of risk to a right is necessary as it is the core element of the risk-based approach. Guidelines, methods may establish different versions of DPIA (as there is no 'one size fits all' model for impact assessments), but a varying perception of risk to a right would undermine the endeavours of the GDPR relating to harmonisation. This article advises a unified understanding of risk to a right and risk to the right to the protection of personal data.

To understand the concept of risk, more specifically risk to a right, this paper divides the concept of risk into its 'seven circumstances'. The role of circumstances (*circumstantiae*) was pivotal in ancient Greek rhetoric. It helped define the specific attributes of a case. A Greek rhetorician from the second century BC, Hermagoras of Temnos, recognized both thesis and hypothesis as rhetorical controversies. He delimited the hypothesis by seven attributes: *quis (who), quid (what), quando (when), ubi (where), cur (why), quem ad modum (in what way), quibus adminiculis (by what means)*. It served to introduce an argument by circumscribing it.[10] The 'seven circumstances', as a preliminary definitional method, are also suitable for pointing out the necessity of a unified perception

5 Roger Clarke, 'Privacy Impact Assessment: Its Origins and Development' (2009) 25 Computer, Law and Security Review 123 <http://www.rogerclarke.com/DV/PIAHist-08.html> accessed 12 April 2016.

6 It should be underlined that some experts critically state that DPIA, in its current form, does not require controllers to carry out a proper impact assessment, as it facilitates a mere legal compliance check. Read more at: Roger Clarke, 'Approaches to Impact Assessment' Brussels, 22 January 2014 <http://www.rogerclarke.com/SOS/IA-1401.html#RA> accessed 3 May 2016.

7 Leon Hempel and Hans Lammerant, 'Impact Assessments as Negotiated Knowledge' in Serge Gutwirth et al (eds), *Reforming European Data Protection Law* (Springer 2015) 125.

8 Lyria Bennett Moses, 'Recurring dilemmas: the law's race to keep up with technological change' (2007) University of Illinois Journal of Law, Technology & Policy 239, 276.

9 Niels van Dijk, Raphaël Gellert and Kjetil Rommetveit, 'A risk to a right? Beyond data protection risk assessments' (2015) 32 Computer Law & Security Review: The International Journal of Technology Law and Practice 286, 292.

10 Read more about the theory of Hermagoras at: R Copeland, *Rhetoric Hermeneutics and Translation in the Middle Ages (Academic Traditions and Vernacular Texts)* (Cambridge University Press 1991) or M Heath, 'The substructure of stasis-theory from Hermagoras to Hermogenes' (1994) 44 Classical Quarterly 114-29.

of risk (thus risk to a right), especially in the case of data protection impact assessments. It also highlights the strengths and weaknesses of the subject. With specific questions, based on the seven circumstances, the paper will tackle the notion of risk to a right (What is risk?), by elaborating on the possible ways of its perception (Who perceives risk?), and the incentives and elements of its assessment (Why and when to deal with risk? In what way and by what means?). After describing the attributes of risk to a right, and where necessary the risk to the right to the protection of personal data (ie it has a significant difference), the findings will be summarized and the advised perception of risk to a right and risk to the right to the protection of personal data will be defined.

II. Risk to the Right to the Protection of Personal Data

This chapter provides a brief explanation of the nature and importance of the notion of risk, as the most centric and practical element of risk-based approach, in particular when it affects a fundamental right or freedom, such as the right to the protection of personal data. The chapter will describe its main attributes through its 'seven circumstances': what is risk, who perceives the risk, why and when is risk to a right perceived, in what way and by what means is risk perceived and assessed. The question 'where' will not be answered as in case of risk to a right it seems irrelevant. To make the understanding of this chapter easier for legal experts, common, data protection related examples will be used.

1. What Is Risk?

The term 'risk' is usually used in the context of an adverse consequence of an event, however it is not necessarily a negative term. Risk is 'the probability of an event multiplied by some measure of its consequence.'[11] Bernstein defines risk as a 'technique for creating knowledge and certainty about future events that are uncertain by definition.'[12] The French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés*, CNIL) provides a more detailed definition, whereas

> risk is a hypothetical scenario that describes how risk sources could exploit the vulnerabilities in personal data supporting assets in a context of threats and allow feared events to occur on personal data, thus generating impacts on the privacy of data subjects.[13]

The purpose of the definition is clear, however it implies that only unwanted events have impact on the privacy of the data subject. Exclusion of aspects in such a general term is not necessarily advantageous. Definitions may differ, but most of them imply that risk appears in every activity, therefore taking the risk into consideration is an essential element of human life[14] and its management is part of the human existence.[15]

Although often seen as an experience of an adverse impact,[16] this article considers risk as a neutral term, wherewith different areas of life, such as market, legal or insurance domains can be interpreted equivalently.[17] If the event has a positive outcome, it can be referred to as 'opportunity risk', in case of negative impact, 'hazard risk', or 'hazard'.[18] The objective of

11 Gary Yohe and Robin Leichenko, 'Chapter 2: Adopting a risk-based approach' (2010) New York City Panel on Climate Change 2010 Report, Annals of the New York Academy of Sciences 29, 31 <http://onlinelibrary.wiley.com/doi/10.1111/j.1749-6632.2009.05310.x/epdf> accessed 8 December 2016.

12 Peter L Bernstein, *Against the Gods: The Remarkable Story of Risk* (John Wiley & Sons Inc 1998)

13 CNIL, 'Privacy Impact Assessment (PIA) – Methodology (how to carry out a PIA)' (2015) 6 <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf> accessed 8 December 2016.

14 Jonathan B Wiener, 'Precaution in a Multirisk World' in Dennis J Paustenbach (ed), *Human and Ecological Risk Assessment: Theory and Practice* (John Wiley & Sons Inc 2002) 1511 <http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1923&context=faculty_scholarship> accessed 8 December 2016.

15 Centre for Information Policy Leadership (CIPL), 'The role of risk management in data protection – Paper 2 of the Project on Privacy Risk Framework and Risk-based Approach to Privacy' (2014) 4 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf> accessed 8 December 2016.

16 James F Short Jr, 'The Social Fabric of Risk: Towards the Social Transformation of Risk Analysis' (1984) 49 American Sociological Review 711, 711 <https://oied.ncsu.edu/selc/wp-content/uploads/2013/03/The-Social-Fabric-at-Risk-Toward-the-Social-Transformation-of-Risk-Analysis.pdf> accessed 8 December 2016.

17 Jack A Jones, 'An Introduction to Factor Analysis of Information Risk (FAIR)' (2005) 8 <http://www.slideshare.net/Kabogo/an-introductiontofactoranalysisofinformationriskfair680> accessed 8 December 2016.

18 The Association of Insurance and Risk Managers (airmic), 'A structures approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000' (2010) 6 <https://www.theirm.org/media/886062/ISO3100_doc.pdf> accessed 8 December 2016.

risk management[19] is to 'direct and control an organization with regard to risk'.[20] Regarding harm risk management aims to avoid or minimise the adverse effect.

The purpose of perceiving an event as risk is to assess it in a homogeneous system as equal occurrences.[21] The notion of risk implies that the event is perceived in a proper way (eg based on comprehensive knowledge). Inappropriate, false interpretation (such as an uncertain or ignored event)might result from different forms of perceptions, such as an uncertain or ignored event.[22] For example, processing of personal data, based on the consent of a data subject, could be interpreted as a risk. The data controller should notify the data subject about the details of this risk to give informed consent. Otherwise, the data subject might have a misconception of the consequences of the data processing operation. A third option is that the data subject simply ignores the fact that his personal data will be processed.

The right perception of a risk is based on an appropriate and comprehensive knowledge, but the prediction of the occurrence of risk is excluded. Optimally perceived risk can be either certain or uncertain. The general causes of uncertainty are unpredictability or unreliable, insufficient knowledge, however, the fear from a hitherto unknown event can also be considered as an uncertain risk.[23] An example for uncertainty can be the knowledge of the data subject relating to the processing operation. Consent can be given based either on comprehensive knowledge (eg when the privacy policy is read and understood) or insufficient knowledge (when the policy or the functioning of the data processing is not understood or the policy not even read).

2. Appearance of Risk in Data Protection Law

The notion of risk is not entirely new to data protection law, although the risk to privacy is not a central element in the Directive 95/46/EC. Under the auspices of consistent and high level protection of individuals, the notion of risk gained significantly more attention during the data protection reform and was integrated in the GDPR.[24] Although critics pointed out that a risk-based approach in data protection might sacrifice the will of the individual to the ethics and accountability of an organisation,[25] the Article 29 Working Party (A29 WP) reiterated that the risk-based approach is not an alternative to the rights and principles of data protection, but a scalable and proportionate approach to foster compliance.[26]

The Regulation follows the ideology of the Directive and aims to reinforce data protection rights, rather than to become an entirely new way of protection.[27] Therefore, to assess the effectiveness and *raison d'etre* of the notion of risk in the Regulation, its appearance in the Directive must be assessed beforehand. The Directive aims to protect fundamental rights, especially the right to privacy,[28] by laying

19 Risk management can be considered as a 'systematic process of identifying and assessing risks, avoiding or mitigating them where possible, and then accepting and managing the remaining risks'. Read more at: CIPL (n 15) 5.

20 Read: ISO 31000:2009 2.2 or ISO 73:2009 2.1 <https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en> accessed 13 March 2016. The ISO 31000:2009 and ISO 73:2009 are currently under revision. Read more at: Sandrine Tranchard, 'The revision of ISO 31000 on risk management has started' (2015) <http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1963> accessed 8 December 2016.

21 Jones (n 17).

22 Paul Slovic and Elke U Weber, 'Perception of Risk Posed by Extreme Events' (2002) 16 <https://www.ldeo.columbia.edu/chrr/documents/meetings/roundtable/white_papers/slovic_wp.pdf> accessed 8 December 2016.

23 Marcela Brugnach et al, 'Toward a relational concept of uncertainty: about knowing too little, knowing too differently, and accepting not to know' (2008) 13(2) Ecology and Society 30 <http://www.ecologyandsociety.org/vol13/iss2/art30/> accessed 8 December 2016.

24 Article 29 Data Protection Working Party (A29 WP), 'Statement on the role of a risk-based approach in data protection legal frameworks' (2014) WP218 2 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf> accessed 8 December 2016

25 Jedidiah Bracy, 'Demystifying the Risk-Based Approach' (30 April 2014) <https://iapp.org/news/a/demystifying-the-risk-based-approach/> accessed 8 December 2016

26 A29 WP, 'Statement on the role of a risk-based approach' (n 24) 2.

27 Introduction s 2 GDPR (trilogue) <http://statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf> accessed 8 December 2016

28 art 1(2) GDPR emphasises the right to the protection of personal data. It must be underlined that the right to privacy and the right to the protection of personal data are not the same. There are numerous discussions about the scope and nature of these rights, however one commonly used interpretation says privacy can be used as a tool of opacity, meanwhile the right to personal data serves as a tool of transparency. About privacy and the differences between privacy and the protection of personal data read more at: Paul De Hert and Serge 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) 61 <http://works.bepress.com/serge_gutwirth/5/download/> accessed 8 December 2016; Bert-Jaap Koops et al, 'A Typology of Privacy' (2016 forthcoming) University of Pennsylvania Journal of International Law 38 <http://ssrn.com/abstract=2754043> accessed 8 December 2016.

down requirements regarding the processing of personal data. It does not mention the right to the protection of personal data since it was drafted before the era of the Charter of Fundamental Rights of the EU(the Charter) . The Directive (along with eg Regulation 45/2001 or CoE 108.[29]) refers to Article 8(1) of the European Convention on Human Rights (ECHR), which establishes the right to private life. As the Lisbon Treaty came into force in 2009 and Article 6(1) of the Treaty on European Union incorporated the Charter, furthermore the right to the protection of personal data was reiterated in Article 16 of the Treaty on the Functioning of the European Union, the newly established right became binding primary law of the EU (through Article 8 Charter).[30] Article 52(3) Charter states that as it

> contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention.

Although the right to the protection of personal data is not apparent as a separate right in the Convention, connection can be drawn with parts of Article 8 ECHR.[31] The Court of Justice of the EU (CJEU) also interpreted EU data protection law in light of Article 8 ECHR prior to the proclamation of the Charter.[32] The right to private life can be considered as an umbrella right which protects *inter alia* the individuals against the processing of information relating to them.[33]

The aforementioned fundamental rights are not absolute rights, their limitation is possible,[34] however the limitation

> must be provided for by law, respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[35]

According to the Charter, certain activities constitute a limitation of a right or freedom, as they affect the individual. The processing of personal data affects the individual through her personal information by limiting her fundamental right. However, in certain cases it is possible that the benefits outweigh the costs of limitation (and the requirements of Article 52(1) Charter will be met), thus such limitation of a right will be legitimised.

As every event, limitation of a right also can be interpreted as a risk. The process of defining and assessing the limitation of a right through a risk-based approach is promoted by, *inter alia*, the A29 WP, which considers the aforementioned approach as a bouquet of 'strengthened obligations result from processing which is considered as a risk for the persons concerned'.[36]

3. Who Perceives Risk?

Risk is a knowledge intensive concept, as it is built upon infinite amount of information.[37] To assess risk in details one has to possess comprehensive knowledge. The perception of risk, which affects the risk-taker himself, seems more straightforward, as most of the influencing factors, details, along with complementary information are visible and known to the risk-taker (data subject). In case of the perception of risk of others the relevant information should be acquired, which requires additional effort.

29 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37> accessed 8 December 2016.

30 Albeit it was expressed by the Charter, the right (as part of art 8 ECHR) was articulated in the decisions of the ECtHR as well. See *Amann v Switzerland* App no 27789/95 (ECtHR, 2000) para 65 or *Rotaru v Romania* App no 28341/95 (ECtHR, 2000) para 43. Read more at: Juliane Kokott and Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) 3(4) International Data Privacy Law 222.

31 About the differences and overlaps between the right to privacy and right to the protection of personal data read: Raphaël Gellert and Serge Gutwirth, 'The legal construction of privacy and data protection' (2013) 29(5) Computer Law & Security Review 522.

32 Gloria González Fuster, 'Curtailing a right in flux: restrictions of the right to personal data' in Artemi Rallo Lombarte and Rosario García Mahamut (eds), *Towards a new European Data Protection Regime* (Tirant lo Blanch 2015) 513, 522.

33 See *Leander v Sweden* App no 9248/81 (ECtHR, 1987) para 48.

34 Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* (CJEU, 2010) I-11063 para 48. Also emphasized by Recital (5) GDPR.

35 art 52(1) Charter.

36 A29 WP, 'Statement on the role of a risk-based approach' (n 24) 2.

37 Richard V Ericson and Kevin D Haggerty, *Policing the Risk Society* (University of Toronto Press 1997) referred by Raphaël Gellert, 'Data Protection: a risk regulation? Between the risk management of everything and the precautionary alternative' (2015) 5 International Data Privacy Law 3, 15.

Risk is not limited to individuals: it can relate to groups or to an entire society as well.[38] Risk can have an impact on each cluster and it is usually managed by the affected cluster. The clusters are mainly independent of each other, meaning for example the perception of risk to a group as a group will not affect the individual in perceiving of a risk to himself (eg one user might refuse to use Google because of its privacy invasive nature but for the whole society it is acceptable and used as the main search engine). Although data protection is a relevant issue for each cluster, the GDPR provides protection directly to the individual (data subject) and indirectly to other clusters.

a. Own Risk of the Individual

The comprehension of risk by individuals can be described by two separate systems: risk as feeling and risk as analysis.[39] Intuition is a dominant factor for individuals to assess risk as they base their decisions on feelings, previous experience, current emotional state and other feelings. Assessment, based on instinct and intuition, results a prompt and mostly automatic decision making. Slovic explains it as the 'experiential' mode of thinking.[40] With this type of perception individuals usually compare the negative effects and the potential benefits of a risk (eg providing access to a mobile app to the personal data stored on the phone, in order to use the app).

The other method (analysis) is based on logic, objective reasons and various assessments. As individuals gained more control on their lives, analytic thinking became more popular and rationality got a pivotal role in experiential thinking (ie resulted in different forms of privacy-awareness).[41] Consequently the two forms of risk perception are not entirely separate, they are continually active.[42] From the perspective of the individual both are essential, for example feelings might overweight the consideration of negative consequences. With rational thinking the likelihood of that consequence might become estimable.[43]

The data subject, as an individual perceives his own risk when his personal data is going to be processed. Article 4(1) GDPR provides a definition of the data subject (identified or identifiable natural person). Although exceptions exist,[44] European data protection law protects the living being,[45] should he be identified or identifiable through any information relating to him. Neither the Directive, nor the Regulation provide clarification when a natural person should be considered identified,[46] however the role of identification is to describe a person in a way that he becomes 'distinguishable from all other persons and recognised as an individual'.[47]

b. Risk of Group

In cases where the risk-taker and decision-maker are a group, the importance of emotional thinking becomes secondary beside the objective analysis system. As for a group, primarily, its common interest is taken into consideration, thus the perception of risk is based on logical thinking, facts and assessments. If the group is an organisation, the perception of risk is a part of a detailed risk management framework, led by principles, goals and methodologies.[48] As the GDPR requires the controller (considered as a group) to carry out a DPIA, this paper will elaborate on the 'risk as analysis' as the primary way of risk perception.

---

38 Lennart Sjöberg, Bjørg-Elin Moen and Torbjørn Rundmo, 'Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research' (Rotunde publikasjoner 2004) 7 <http://www.svt.ntnu.no/psy/torbjorn.rundmo/psychometric_paradigm.pdf> accessed 8 December 2016.

39 Paul Slovic et al, 'Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk and Rationality' (2014) 24(2) Risk Analysis 311 <http://onlinelibrary.wiley.com/doi/10.1111/j.0272-4332.2004.00433.x/epdf> accessed 8 December 2016.

40 Paul Slovic and Ellen Peters, 'Risk Perception and Affect' (2006) 15(6) Current Directions in Psychological Science 322 <http://faculty.psy.ohio-state.edu/peters/lab/pubs/publications/2006_slovic_peters_current_directions_590.pdf> accessed 8 December 2016.

41 ibid.

42 For more information about the simultaneous perception read: AR Damasio, *Descartes' error: emotion, reason, and the human brain* (Avon 1994).

43 Slovic et al (n 39) 320.

44 See *Bernh Larsen Holding AS and Others v Norway* App no 24117/08 (ECtHR, 2013) or Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* (n 34).

45 A29 WP, 'Opinion 4/2007 on the concept of personal data' (2007) WP13622 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> accessed 8 December 2016.

46 See *Odièvre v France* App no 42326/98 (ECtHR, 2003).

47 European Union Agency for Fundamental Rights (FRA), *Handbook on European data protection law* (Publications Office of the European Union 2014) 39 <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf> accessed 8 December 2016.

48 CIPL (n 15) 4.

c. Risk of Society

Society has a constantly growing awareness regarding risks, encountered in everyday life.[49] Social awareness requires information regarding risks society can face. The social demand requires decision makers to provide sufficient, yet understandable information regarding the risk they create, thus putting a remarkable amount of burden on them. A detailed, sometimes mere technical explanation might be sufficient, but not understandable for the wide range of people (eg the description of the algorithm used by Google search engine would not be helpful for most of the users). Studies have also shown that beliefs of people change very slowly, moreover, they are persistent even if the opposite opinion is proven.[50] However, every piece and form of information have an influenceincluding *inter alia* the form in which the information is conveyed.

d. Risk of Others

The perception and assessment of risk is not limited to the own risk of the assessor. Assessing risk of other clusters (or other units within the same cluster) is a commonly used method: eg the government as a group intends to make the life of citizens more secure by following a stringent cybersecurity strategy; the employer intends to improve the working conditions for his employees by providing them adequate infrastructure; etc. Risk of others can affect the assessor (from a different cluster or unit) as well, therefore the assessment of risk to others can serve as a key element to treat (mitigate or avoid) one's own risk: the government will not be re-elected if their decisions are unpopular or have disadvantageous consequences; the company will generate less income if the working conditions are not entirely satisfactory; the data controller will be fined if the data processing operation is not compliant with data protection law; etc.

The assessment and treatment of risk to others often result a balanced, win-win situation, eg by treating the risk of an individual (data subject), risk of the group (data controller) will become treated as well. In certain cases, activity of the controller itself constitutes a risk to the data subject, thus the controller should have full control and liability over the consequences of its activity.

The risk to the right of a data subject affects both the controller and the data subject. By assessing and treating the risk to the right of the data subject, the data controller can mitigate or avoid the effects on him/herself as well. Before the controller focuses on the assessment of the risk to the data subject, he/she should define the consequences of the risk to both parties. Van Dijk, Gellert and Rommetveit categorise this perception as 'right as risk'.[51]

Due to the connection between the parties, risk assessment, conducted by the controller on the risk to right of the data subject, the reasons and implications of the risk assessment should be clear for both parties. The data subject needs to know the severity and likelihood of his/her risk, the legitimacy of that prediction, moreover the capabilities of the assessor on judging her risk. Without sufficient knowledge or adequate risk mitigation the data subject might become distrustful and – as a form assessing and treating his/her own risk – stop further interactions with the data controller – 'inappropriate risk comparisons can be dangerous to one's own credibility'[52].[53] The term risk in the GDPR refers to the data subject and constitutes an event when her data is processed by someone else, notably the data controller. Therefore, it is assessed both by the data subject and by the data controller.

4. Why and When to Deal With Risk?

The aim of assessing risk is the estimation of possibly negative impacts through consistent processes, thus the mitigation, avoidance or other acceptable forms of treatment will become achievable.[54] Assessing risk in a homogeneous system helps the decision-

49 Paul Slovic, Baruch Fischhoff and Sara Lichtenstein, 'Perceived risk: psychological factors and social implications' (1981) 376 Proceedings of the Royal Society of London A 17, 29 <http://rspa.royalsocietypublishing.org/content/376/1764/17> accessed 8 December 2016.

50 ibid.

51 Van Dijk, Gellert and Rommetveit (n 9).

52 Vincent T Covello, Peter M Sandman and Paul Slovic, 'Risk Communication, Risk Statistics and Risk Comparisons: A Manual for Plant Managers' (*Chemical Manufacturers Association*, 1988) <http://www.psandman.com/articles/cma-4.htm> accessed 8 December 2016.

53 Baruch Fischhoff, 'The psychology of risk characterization' in Berndt Brehmer and Nils-Eric Sahlin (eds), *Future Risks and Risk Management* (Springer Netherlands 1994) 130.

54 ibid 127.

maker to make informed choices, prioritise between different actions and find the best possible outcome.[55] The process of risk assessment is repeatable, but should have a starting and ending point in order to successfully tackle the risk (ie consent should be given prior to the processing of personal data; DPIA should be carried out prior to the processing operation).

As data processing constitutes a limitation on the rights and freedoms of the data subject, he/she should be granted the opportunity to know the reasons, extent and consequences of the processing operation, furthermore the extent of the protection, described in Article 1(1) GDPR.[56] This attitude was interpreted as the right to informational self-determination by the German Federal Constitutional Court[57] in 1983. In the census decision[58] the Court said that personality rights contain 'the authority of the individual to decide himself, on the basis of the notion of self-determination, when and within what limits information about his private life should be communicated to others'.[59]

As mentioned earlier, from the point of view of the controller, risk to a right has an additional layer, as it (either as a group or as an individual) perceives both the risk of the data subject and the risk of itself. Data controllers are responsible for complying with the rules of data protection law. The controller must consider the protection of fundamental rights and freedoms of the data subject. By achieving compliance through DPIA the controller can reach further benefits, such as establishing trust, transparency, cost-effectiveness or waiver of civil liability.[60] The other incentive, besides abiding the law, is to avoid possible sanctions, prescribed in Chapter VIII GDPR. As the CJEU pointed out in the *Von* Colson and *Kamann v Land Nordrhein-Westfalen* case,[61] sanctions must have a deterrent effect.

When risk is dealt with prior to its occurrence, the adverse effects can be mitigated or avoided, albeit, in certain cases risk can be assessed after its occurrence as well [eg DPIA shall be carried out before and during the processing operation (as a form of monitoring or review)]. Previously occurred risk cannot be affected, only its consequence through ex post remedies (ie sanctions), furthermore it can also provide essential information for future, refined risk assessments.[62] In case of data processing the data controller sets the level of data security, however it can be modified (increased or upgraded) later, if necessary – for example in the event of an unauthorised breach. Generally, compliance with the provisions must be reached during the entire processing period. This implies that risk assessment shall be carried out before and during the entire period of the processing operation.

The necessity of proactivity appears as a principle in DPIAs in order to be effective the assessment shall be carried out prior to the processing, at an early stage. While Recital (89) only implies, Recital (90) GDPR and Article 35(1) GDPR states explicitly that the assessment should be carried out prior to the processing. The most efficient moment to carry out an impact assessment is the final phase of the development (that is the stage of development when almost every detail of the processing operation is clear but modifications still can be applied).

5. In What Way and by What Means Should Risk Be Assessed?

As discussed earlier, the risk assessment of the data subject is less institutionalised and more intuitive, but the controller is still obliged to help the data subject in the process. In order to successfully assess risk,

55 ISO 31000:2009 3c.

56 'This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.'

57 *Bundesverfassungsgericht* (BVerfG).

58 The German Federal Constitutional Court declared that numerous provisions of the Census Act were unconstitutional. The census included the collection of personal information, data connected to employment, real estates, buildings, flats, furthermore registration of non-agricultural organisations. The Act also allowed data transfers for federal statistics offices and administration bodies. Read more at: Herbert Burkert, 'Privacy – Data Protection – A German/European Perspective' in Christoph Engel and Kenneth H Keller (eds), *Governance of Global Networks in the Light of Different Local Values* (Nomos Verlagsgesellschaft 2000) 43, 49 <http://www.coll.mpg.de/sites/www/files/text/burkert.pdf> accessed 8 December 2016.

59 Antoinette Rouvroy and Yves Poulet, 'The Right to Informational Self-Determination and the Value of Self-Deployment: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer 2010) 45.

60 Raphaël Gellert and Dariusz Kloza, 'Can privacy impact assessment mitigate civil liability? A precautionary approach' (*Österreichische Computer Gesellschaft*, 2012) Transformation juristischer Sprachen.

61 Case C-14/83 *Sabine von Colson and Elisabeth Kamann v Land Nordrhein-Westfalen* (CJEU, 1983) 1984-01891.

62 Paul Slovic, 'Perception of Risk' (1987) 236 Science 280, 283 <http://heatherlench.com/wp-content/uploads/2008/07/slovic.pdf> accessed 8 December 2016.

the data subject needs sufficient information. Data controller is obliged to provide the data subject certain information about the data processing in an easily understandable language,[63] prior to its beginning.[64] Data subject also has the right to obtain information regarding the processing of his personal data any time,[65] in order to verify the accuracy of the data and the lawfulness of processing.[66] As the CJEU clarified in the *Rijkeboer* case, the right to access is necessary to enable the data subject to exercise his rights under Article 12(b) Directive.[67]

From the point of view of the data controller, as the assessor, risk assessment, as part of risk management and as a prominent part of DPIA (described in Article 35(7)(c) GDPR), can be separated into three plus one parts: identification, analysis, evaluation and treatment of risk.[68] With an assessment the data controller is able to identify the future event, along with its possibility of occurrence, its consequences and handle them afterwards.[69] The range of techniques to conduct a proper assessment is relatively wide. The assessor can base the process on, *inter alia,* the outcomes of questionnaires, workshops, audits or SWOT analyses.[70] As the appropriateness of the tools may vary per risk, this part will focus on the mandatory parts of the assessment from a general, theoretical aspect.

a. Identifying Risks

When the envisaged data processing constitutes a (high) risk to the rights and freedoms of the data subject, a DPIA shall be conducted (by the controller) and provide a solution, how the risk should be mitigated or avoided by the means of data protection law. The necessity is justified by Article 1(2) GDPR.[71] The core part of risk assessment is the articulation of a clear and consistent risk statement. The statement is an expression of a relationship between a real, existing event, fact (eg processing of personal data) and a potential, unrealised second event or fact (eg its effect on the rights of the individual).[72] Clear statements help in the identification of possible adverse effects (eg personal data will be stored by a cloud service provider which does not meet the basic requirements of data security, therefore almost every type of attempted breach would be successful). The last element of this step is the identification of the possible outcome and the description of possible consequences.[73]

To help the identification, the controller should take into consideration all possible areas of impacts on the rights and freedoms of the individual and create a comprehensive list of risks, either by himself or through the involvement of stakeholders, especially external stakeholders, such as the affected individual/public.[74] Regarding stakeholder engagement, De Hert and Wright, based on the ISO 27005:2008 standard, identified several benefits to the controller, such as providing assurance of the outcome of the risk management; collecting risk information; increasing mutual understanding between decision-makers and stakeholders; communicating the results of the assessment; improving awareness; etc.[75] If the

63 A detailed, comprehensive information is not always understandable, therefore the Working Party tried to find a balance and introduced in its opinion the so-called layered notices. It allows the data subject to decide which level of detail he prefers. About the layered notices read more at: A29 WP, 'Opinion 10/2004 on More Harmonised Information Provisions' (2004) WP100 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf> accessed 8 December 2016.

64 Although it is not explicitly articulated, the provisions of the Directive imply it: eg '…the purposes of the processing for which the data are intended…' or '…no later than the time when the data are first disclosed…'

65 art 15 GDPR.

66 recital (63) GDPR.

67 Case C-553/07 *College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer* (CJEU, 2009) I-03889.

68 ISO, 'IEC 31010:2009 Risk management — Risk assessment techniques' (*Online Browsing Platform*, 2009) <https://www.iso.org/obp/ui/#iso:std:iec:31010:ed-1:v1:en> accessed 8 December 2016.

69 ibid.

70 For more examples see the chart at: Association of Insurance and Risk Managers (n 18) 13.

71 'This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.'

72 Microsoft Operations Framework (MOF) Risk Management Discipline, 'Identifying Risks in Operations' <https://technet.microsoft.com/en-us/library/cc535338.aspx> accessed 8 December 2016.

73 ibid.

74 About stakeholder engagement read: Dariusz Kloza, 'Public Voice in Privacy Governance: Lessons from Environmental Democracy' in Erich Schweighofer and János Böszörményi (eds), *Knowledge Rights – Legal, Societal and Related Technological Aspects. 25 years of Data Protection in Finland* (Österreichische Computer Gesellschaft 2013).

75 David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer 2012) 467.

impact assessment is conducted from a single viewpoint, risks might be overlooked. A consultation with stakeholders provides input to their perceptions of the severity of the envisaged processing operation; give a preliminary picture, how the service would work in practice; furthermore, it would increase transparency and trust. The positive effects can be reached only if the stakeholder engagement is conducted properly (eg both internal and external stakeholders are involved, the categories of affected individuals are representative they are provided with sufficient information regarding the data processing operation and the terms of involvement to the DPIA).[76] In any other case, it could cause an opposite, damaging effect.[77]

b. Analysis of Impacts

Risk analysis focuses on the understanding of the identified risk. According to Recital (90), a data protection impact assessment shall be carried out in order to assess the particular likelihood and severity of the (high) risk. Likelihood of a risk cannot be completely predicted, albeit certain and uncertain risks are treated differently. According to CNIL 'severity essentially depends on the level of consequences of the potential impacts'.[78] Sample diagrams help in the visualisation of severity and likelihood of the identified risks (Figure 1). This type of diagram is an effective visualisation tool for risk assessment, as it remains an abstract, empty, numerical device.

Although the quantification (or qualification) of severity and likelihood is scalable and commonly used in risk assessments, its suitability in DPIA should be revised. The processing of personal data constitutes risk to the rights and freedoms of the data subject, meaning the right or freedom will be limited. In most cases these rights are not absolute rights, their limitation is possible.[79] A limitation of a right is usually not easily quantifiable, additional attributes and governing principles are required.

In case of the risk to the right to the protection of personal data the GDPR describes circumstances under which the processing operation is compliant with the rules. Therefore, the severity of this risk should be visualised in a two-grade scale: the processing of personal data is either violating or non-violating legal provisions (Figure 2). With this analysis the controller can learn the nature or the severity of its operation and define whether the processing operation is in compliance with the Regulation. Although the analysis of risk is not regulated by the GDPR, the severity of the risk can be measured, based on the governing principles of data protection law and the opinions of the A29 WP and the national supervisory authorities.

The impact of the identified risk depends also on the possibility of its occurrence. The likelihood can never reach 100%, therefore the controller must ensure that the impacts of the risk will not violate the rules of data protection, even if the risk is uncertain. This assumption implies that data processing operations (based on ICT) are dangerous until they are proven to be safe.[80] This can be interpreted as a general precautionary attitude.[81] As Van Dijk, Gellert and Rommetveit point out, precaution is based on subjective knowledge,[82] and as Gellert explains 'risk relies upon an infinite number of factors, therefore it is simply impossible to fully prevent risk'.[83] Therefore, complete avoidance of risk cannot be a goal of impact assessment, only mitigation.[84] Wiener indicates that the achievable goal of the precautionary principle is not maximum, but optimal precaution.[85] To be effective, possible risks should be taken seriously, which demands different types of comprehensive knowledge. Gellert says 'taking risk seriously means complexifying things rather than simplifying them.'[86] To describe the level of optimal precaution is difficult, however, the interpretation of Recital (23)

76 Read more at: Privacy Impact Assessment Framework: Recommendations for a Privacy Impact Assessment Framework for the European Union (2012) 29 <http://www.piafproject.eu/ref/PIAF_D3_final.pdf> accessed 8 December 2016.

77 Wright and De Hert (n 75) 443, 469.

78 CNIL, 'Methodology for Privacy Risk Management' (2012) 8 <https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf> accessed 8 December 2016.

79 art 52(1) Charter.

80 Charles Raab, 'The future of privacy protection' (2004) Cyber Trust & Crime Prevention Project 15 <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.7940&rep=rep1&type=pdf> accessed 8 December 2016.

81 Van Dijk, Gellert and Rommetveit (n 9).

82 ibid.

83 Raphaël Gellert, 'Data Protection: a risk regulation? Between the risk management of everything and the precautionary alternative' (2015) 5 International Data Privacy Law 3, 15.

84 ibid 15-16.

85 Wiener (n 14) 1526.

86 Gellert (n 37) 18.

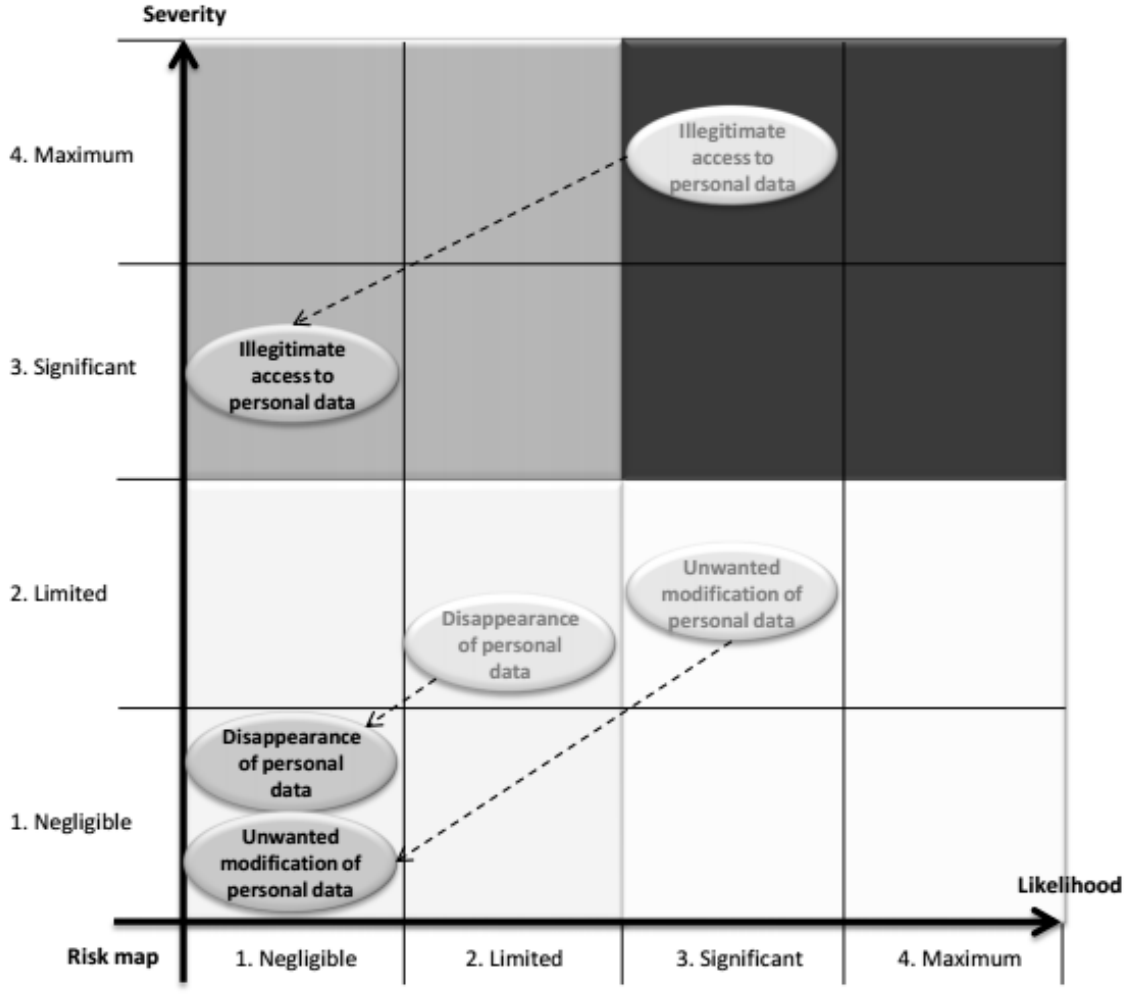

Figure 1.

GDPR as the proportionality test of optimal precaution might provide a (vague) answer: 'all means reasonably likely to be used... either by the controller or by another person' should be taken into consideration during the analysis of an uncertain risk.[87] The precautionary approach also contributes to the practical implementation of the principles of data protection by design and by default.[88]

87 recital (23) GDPR.

88 European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) 32 <http://www.europarl.europa.eu/document/activities/cont/201205/20120524ATT45776/20120524ATT45776EN.pdf> accessed 8 December 2016.

89 A29 WP, 'Statement on the role of a risk-based approach' (n 24) 2.

c. Risk Evaluation

The evaluation of risk to a right should be based on the determining factors, mentioned in Article 52(1) Charter, furthermore the corresponding official documents and judicial cases. Regarding the risk to the right to the protection of personal data, the provisions and principles of the Regulation can be interpreted as the basis of a risk-classification system. The evaluation must be strict, as the level of protection of the rights and freedoms of the data subject must be the same, regardless of the severity and likelihood of the risk.[89] The evaluation of uncertain risk shall be governed by the precautionary principle. This means that the treatment of these risks should be based on an evaluation which foreshadows the worst

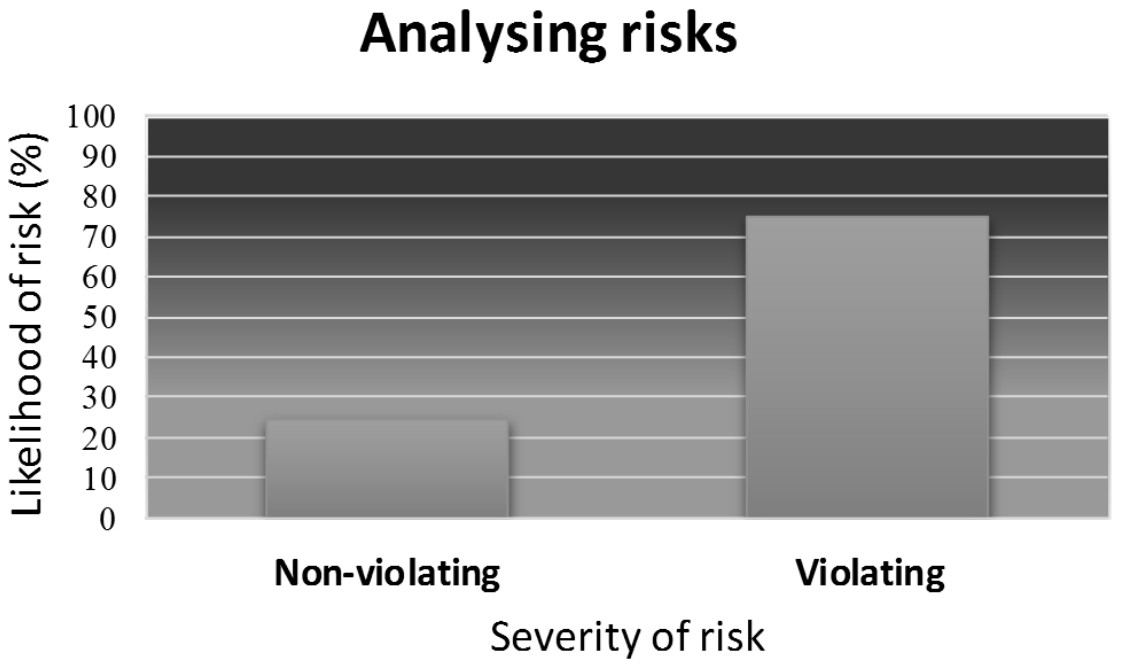

Figure 2.

possible outcome. As the A29 WP pointed out, an 'assessment is not a straightforward balancing test consisting merely of weighing two easily quantifiable and comparable weights against each other'.[90] The traditional balancing, referred by the Working Party, relates to the comparison of the conflicting fundamental rights or values, where the support of one right or value weakens the other one. The aim of balancing can be understood as the reconciliation of values by preserving and enforcing them in the most efficient way.[91] In DPIA, the risk evaluation should be conducted from a constitutional viewpoint, as the data processing operation affects the right or freedom of the individual.

If the risk-classification system is based on the provisions of data protection law, the assessment of risk to the right to the protection of personal data will become a mere legal compliance check. From the point of view of this particular risk to the right DPIA should be treated as a data protection risk assessment. The risk-based approach and the assessment of risk in the Regulation should not only provide a scalable and proportionate approach to foster compliance.[92] It should go beyond a compliance check and assess the impacts of the processing operation on the rights and freedoms of the individual, both one by one and together. It should also affect the goals of an organisation in their entirety – how the organisation implements, *inter alia,* the legal and technical requirements, opinions of internal and external stakeholders and the different measures to meet technical, constitutional, social, ethical, etc norms.

III. Definition of Risk to a Right and Risk to the Right to the Protection of Personal Data

The main function of the system of Hermagoras is to introduce a case or a problem by describing its

90 A29 WP, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (2014) WP217 3 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 8 December 2016.

91 Raphaël Gellert et al, 'Minimizing Technology Risks with PIAs, Precaution and Participation' (2011) 4(30) IEEE Technology and Society Magazine 7 <http://works.bepress.com/michael_friedewald/56/> accessed 8 December 2016.

92 A29 WP, 'Statement on the role of a risk-based approach' (n 24) 2.

main attributes. In case of risk to a right, and more specifically risk to the right to the protection of personal data, these attributes can be summarised as follows:

The perception of risk to a right (and in particularly the risk to the right to the protection of personal data) should be based on comprehensive knowledge in order to ensure the adequacy of its perception and assessment. To assess the risk, as a neutral interpretation of the processing of personal data, successfully, numerous elements must be clarified beforehand. The risk itself is the core element and subject of the risk assessment. A general definition says risk is 'the probability of an event multiplied by some measure of its consequence.'[93] In the terminology of the Charter this event is a limitation of a fundamental right, eg the right to the protection of personal data. The most common way of this limitation is data processing.

Data processing, as risk, can have an impact either on an individual, group or society, furthermore these clusters can assess not only their own risk but risk of other clusters as well. The risk to the right to the protection of personal data is usually perceived by the data subject and the data controller. The reason of its assessment is to find the best possible outcome by mitigating or avoiding adverse impacts of the processing operation prior to its occurrence.

The assessment of risk stands on three pillars: identification, analysis and evaluation of risk. In order to be assessed, the source of risk, the risk itself and its outcomes should be identified precisely. The analysis focuses on the understanding of the identified risk, by measuring the likelihood of occurrence and the severity of the possible consequences. The result of the analysis should be compared with a classification system in order to evaluate the risk. The severity of the processing operation depends on this classification system, used in its assessment. In other words, legal rules legitimise the severity of the processing operation. The evaluation identifies the elements which need some form of treatment in order to minimize or avoid the adverse consequences.

These 'circumstances' of risk to a right could form a starting point in a debate about its consolidated perception and application in DPIA. Based on the attributes and roles of risk, described in this contribution, a viable definition of risk to a right could be the following:

Risk to a right is a form of activity, in connection with the exercise of that right, which might constitute a limitation thereof.

In the level of data protection, where the affected right is – primarily, but not exclusively – the right to the protection of personal data, the definition could be modified:

Risk to the right to the protection of personal data is a form of personal data processing or any activity, in connection with the processing operation, which might constitute a lawful or unlawful limitation of the right.

This interpretation implies that the most apparent difference between risk to a right and risk to the right to the protection of personal data lies in their evaluation. While the former relies mostly on the constitutional and judicial (case by case) interpretation of the right, the latter relies mainly on the GDPR.

The definition of risk to the right to the protection of personal data implies that the impact on the individual is a consequence of a processing operation which is either compliant or non-compliant with data protection law. Instead of a case by case analysis, focusing on the specificities of the processing operation along with its potential impacts, general legal rules determine the evaluation of the risk. Legal rules (used as benchmark) draw the attention from the impacts of the risk to the compliance of the risk with the aforementioned rules. Thus, Article 35 GDPR rather serves as a 'compliance-check' instead of an impact assessment. Therefore, 'high risk' in the GDPR has no substantive functionality during the evaluation and qualification process. However, it could be interpreted as an umbrella term of certain data processing operations which have clear, negative impacts on the rights and freedoms of the data subject (eg the examples mentioned in Article 35(3) GDPR).

The 'compliance-check' nature of DPIA is the strongest in case of that particular right which it aims to protect the most. To preserve its *raison d'etre*, the assessment of the impacts on the rights and freedoms of the data subject should not be based solely on the provisions of the GDPR (ie ethical and privacy measures cannot be effectively evaluated through data protection law). On another matter, to ensure that the processing operation is 'good', the impacts of the processing operation on every right, freedom, technical, ethical, etc aspect should be assessed. Not as part of

93 Yohe and Leichenko (n 11).

a DPIA, but as part of a comprehensive fundamental right impact assessment. Due to the nature of data processing, the number of affected rights and freedoms are limited, which can be identified in a threshold analysis, as the first step of an impact assessment.

IV. Conclusion

From the perspective of risk to the right to the protection of personal data, DPIA is an important tool to ensure compliance due to its proactive nature, but nothing more. Remedies and sanctions are retroactive and their contribution to compliant data processing is their deterrent effect.[94] To exploit the benefits of DPIA, the national authorities and the European Data Protection Board shall establish lists[95] and methodologies, based on unified definitions, principles and interpretations. A definition of risk to the right to the protection of personal data, presented in this paper, could be a significant step towards an effective and clear DPIA. However, it must be kept in mind that risk to the right to the protection of personal data is one specific description of an event through a certain point of view and considering only one major aspect. From another perspective [eg other rights and freedoms (as required in Article 35(1) GDPR)), technical, ethical, security, social acceptance, etc] the same processing operation might raise entirely different risks with different impacts.

Generally, the notion of risk to a right can evoke a conceptual change in the application of data protection law. Instead of focusing on the past, the assessment of risks to the rights and freedoms of the data subject will draw the attention to the possible future.[96] Furthermore, the narrow, data protection oriented scope could be changed to a more comprehensive, wider scope which considers every possible impact on every possible right and freedom. The conduct of DPIA should go beyond a compliance check, as the process incites controllers to involve external stakeholders and recommends controller to consider uncertain risks as well. The goal of an impact assessment is not only to foster compliance but also to identify and resolve potential adverse impacts and find the best solution from the point of view of eg privacy, ethics, technology, etc.[97] This article aimed to contribute to that goal by elaborating on the nature and attributes of the notion of risk to a right and risk to the right to the protection of personal data, furthermore providing a viable definition thereof. Although the 'seven circumstances' serve only as an introduction of a problem, these attributes of risk to a right might evoke further discussions about a unified concept of risk to a right in the European legislation.

94 Case C-14/83 *Von Colson* (n 61).

95 Required by art 35 (4)-(6) GDPR.

96 Van Dijk, Gellert and Rommetveit (n 9) 3.

97 David Wright et al (eds), Privacy Impact Assessment Framework for data protection and privacy rights: Deliverable D1 – Revision of existing PIAs (2011) 189 <http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf> accessed 8 December 2016.