# GDPR and the Concept of Risk:

Katerina Demetzou

# GDPR and the Concept of *Risk*:

## The Role of risk, the Scope of risk and the technology involved.

Katerina Demetzou

Business and Law Research Centre (OO&R), Radboud University, Nijmegen, Netherlands
K.Demetzou@cs.ru.nl

**Abstract.** The prominent position of *risk* in the GDPR has raised questions as to the meaning this concept should be given in the field of data protection. This article acknowledges the value of extracting information from the GDPR and using this information as means of interpretation of *risk.* The 'role' that *risk* holds in the GDPR as well as the 'scope' given to the concept, are both examined and provide the reader with valuable insight as to the legislator's intentions with regard to the concept of *risk*. The article also underlines the importance of taking into account new technologies used in personal data processing operations. Technologies such as IoT, AI, algorithms, present characteristics (eg. complexity, autonomy in behavior, processing and generation of vast amounts of personal data) that influence our understanding of *risk* in data protection in various ways.

**Keywords:** Risk, Concept, Data Protection, Accountability, Compliance, Role, Scope, Fundamental Rights, New Technologies.

## 1 Introduction

The GDPR[1] is the new EU legal framework for the fundamental right of personal data protection and for the free flow of personal data, which repeals the preceding Directive 95/46.[2] While the GDPR preserves the key concepts and the basic data protection principles, it introduces several novelties which aim to achieve an effective and high level

[1] Regulation (EU) 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 L 119, 4.5.2016, p. 1–88).

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281, 23.11.1995, p. 31–50.

protection of personal data. One such novelty is the prominent position[3] of the concept of *risk*, both in terms of forming and in terms of triggering legal obligations. *Risk* forms legal obligations in the sense that it has become one of the criteria that the data controller should take into account when deciding on the most appropriate technical and organizational measures;[4] *risk* triggers a legal obligation in the sense that if there is no risk then the obligation need not be fulfilled.[5] According to the WP29, "A risk is a scenario describing an event and its consequences, estimated in terms of severity and likelihood".[6] The fact that consideration should be given to both 'likelihood' and 'severity' is also mentioned in Recitals 75 and 76 of the GDPR.[7] The use of the concept of *risk* is part of the approach adopted by the European legislator in the GDPR, towards a more proactive, scalable and effective data protection.

Despite its importance, *risk* lacks a legal qualification under the EU general legal framework on personal data protection (GDPR). The legislator provides us with examples of *risks* (eg. in Recital 75, 91 GDPR) but does not give the tools for assessing other (new) types of risks, their severity and their likelihood, in an objective and consistent way. The legal qualification of *risk* in relation to data protection and the provision of objective legal criteria against which 'likelihood' and 'severity' will be measured, will allow data controllers to examine each processing activity and reach reliable and contestable conclusions as to the (high) risk(s) presented.

The GDPR, the legal framework in which the concept of *risk* is introduced, should constitute a major source of extraction of legal criteria that will be used as means of interpretation of the concept of *risk* in data protection. Understanding the meaning of *risk* in relation to the particular characteristics of the GDPR presents two important benefits; firstly, it adds objectivity to the assessment of *risk(s)*, in that it allows for the use of language and means, that those involved in the field of data protection share and understand. The legislator requires such an objective assessment of *risk* in Recital 76 GDPR.[8] Secondly, it provides for an interpretation which "guarantee[s] that there is no

---

[3] This prominent position of the concept of *risk* has led legal scholars to talk about a 'riskification' of the EU data protection legislation. See, SPINA, A. (2017). A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics. *European Journal of Risk Regulation*, 8(1), 88-94. doi:10.1017/err.2016.15. Also, MACENAITE, M. (2017). The "Riskification" of European Data Protection Law through a two-fold Shift. *European Journal of Risk Regulation*, 8(3), 506-540. doi:10.1017/err.2017.40.

[4] See the general legal obligation in Article 24(1) GDPR.

[5] See for example the legal obligation in Article 35(1) GDPR to perform DPIAs where there is 'high risk'.

[6] Article 29 Data Protection Working Party 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' WP 248 rev 0.1 (4 April 2017), as last revised and adopted on 4 October, 6, Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques', 7 : "severity and likelihood of this risk should be assessed".

[7] Recital 75 GDPR "The risk to the rights and freedoms of natural persons, of varying *likelihood and severity* […]",

Recital 76 GDPR "The *likelihood and severity* of the risk to the rights and freedoms of the data subject […]".

[8] Recital 76 GDPR "Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk".

conflict between it and the general scheme of which it is part".[9] This approach has also been encouraged by the WP29 in its Opinion[10] on the concepts of 'controller' and 'processor'. The WP29 thereby highlighted the need to deal with the concept of 'data controller' as an autonomous concept, meaning that it has "its own independent meaning in Community law, not varying because of -possibly divergent- provisions of national law"[11] and that "although external legal sources can help identifying who is a controller, it should be interpreted mainly according to data protection law".[12] This "uniform and therefore autonomous interpretation of such a key concept" contributes to an effective application of data protection rules and to a high level of protection.[13]

The purpose of this article is to identify the elements in the GDPR that should be taken into account and explain the way they inform the interpretation of the concept of *risk* in data protection. The research question of this article is, thus, formed as follows:

"How do the role and the scope of *risk* in the GDPR as well as the technology involved in data processing operations inform the meaning of *risk* in the field of data protection?"

To answer this research question, I will first look into the role that the European legislator has attributed to *risk*, by relating it to the principle of accountability and the approach that this principle brings in the GDPR [Section 2]. The discussion on the role of the concept of *risk* leads to the conclusion that *risk* in the GDPR should not be understood as a '(non) compliance risk'. *Risk* should, on the contrary, be understood as referring to 'the rights and freedoms of natural persons' as explicitly suggested by the legislator's wording. In Section 3, I will examine the (broad) scope of the concept of *risk*. In Section 4, I will discuss the technology involved in data processing operations. My purpose is to show that the concept of *risk* in data protection is highly influenced by the technology used. New technologies and the particularities they present should be taken into consideration when interpreting the concept of *risk* in data protection. In the Conclusion [Section 5] I answer the Research Question and summarize the findings of this article.

## *2* The role of *risk* in the GDPR: Accountability & Risk-based approach

As mentioned in the Introduction, the concept of *risk* has been given a prominent position in the GDPR. Having acknowledged this legislative choice, the following question

[9] Koen Lenaerts and José A Gutiérrez-Fons, 'To Say What the Law of the EU Is : Methods of Interpretation and the European Court of Justice' (2013) EUI Working Papers AEL 2013/9 Working Paper <http://cadmus.eui.eu//handle/1814/28339> accessed 16 June 2018, 14.

[10] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor", 8.

[11] ibid.

[12] ibid, 9

[13] ibid.

is raised: What is the role of *risk* in the GDPR? What should always be kept in mind when interpreting and applying data protection rules, is that the ultimate purpose of these rules is "to protect fundamental rights and freedoms of natural persons and in particular their right to privacy, with regard to the processing of personal data".[14] On top of that, what should also be kept in mind is the exact function / role of a concept in the given legal framework.

The importance of clarifying the role of a concept in order to interpret it in a way aligned with its role, could become apparent via the example of 'personal data'.[15]

**The example of 'personal data'.**

'Personal data' is a concept that relates to the material scope of the data protection legal framework. The material scope determines the conditions under which a case falls under the legal framework and natural persons benefit from the legal protection it offers. In the *Google Spain* case, the CJEU said that 'the provisions of Directive 95/46 […] must necessarily be interpreted in the light of fundamental rights'.[16] In its *Ryneš case*, the CJEU said that "derogations and limitations in relation to the protection of personal data must apply in so far as is strictly necessary"[17] which, *a contrario*, confirms the intention of giving a broad meaning to concepts that relate to the material scope of the GDPR.

Based on the role that this concept holds, being actually the 'gateway' for a natural person to get the protection offered by the data protection legislation, the European legislator has provided for a definition of 'personal data' that is 'extensive',[18] flexible enough so that it adapts to the new technological context[19] and has a general wording

---

[14] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' 29, 4.

[15] Article 4(1) GDPR: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"

[16] Case C-131/12 *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 68 (Also see, Case C-274/99 P *Connolly v Commission* [2001] ECLI:EU:C:2001:127, para 37, and Case C-465/00 *Österreichischer Rundfunk and Others* [2003] ECLI:EU:C:2003:294, para 68).

[17] Case C-212/13 *Ryneš* [2014] ECLI:EU:C:2014:2428, para 28 (Also see, Case C-473/12, *IPI* [2013] EU:C:2013:715, para 39, and Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C: 2014:238, para 52).

[18] Commission of the European Communities, 'Amended Proposal for a COUNCIL DIRECTIVE on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data', 10.

[19] Nadezhda Purtova (2018) 'The law of everything. Broad concept of personal data and future of EU data protection law', Law, Innovation and Technology, 10:1, 40-81, DOI: 10.1080/17579961.2018.1452176.

"so as to include all information concerning an identifiable individual".[20] When interpreting the concept of 'personal data', the approach is objective[21], meaning that the data controller's intention (or knowledge of whether the data that are processed qualify as personal data)[22] does not matter; as long as the data can likely result in the identification of a natural person, data protection law applies.[23] Also, the approach is factual, in the sense that in order that data qualify as personal data, the specifics and the context of each case is what should be examined ("the extent to which certain identifiers are sufficient to achieve identification is something dependent on the context of the particular situation").[24] An example is provided by the CJEU in the case of *Nikolaou v. Commission,* whereby even if the applicant was not named, the information published in the press release was personal data given that the applicant was easily identifiable "under the circumstances".[25] What we acknowledge from this example is that the particular role that the concept of 'personal data' plays in the system of protection of the fundamental right to data protection, is of tantamount importance to the way that this concept is interpreted.

**The role of risk.**

Coming back to the concept of *risk*, I will discuss its role in data protection by referring the concept to the principle of accountability. The principle of accountability is found in Article 5(2) which reads: "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability"). The controller shall be responsible for *ensuring compliance* and shall be able to *demonstrate compliance* with data protection principles in practice. The 'data controller'[26] is the actor that bears the responsibility to process personal data in accordance with the principles established in EU data protection law. It is a concept that plays a crucial role in data protection, since it "determines who shall be responsible for compliance with the data protection rules, and how data subjects can exercise their rights in practice".[27] In other words it helps in allocating responsibility. The legislator's intention is to "stimulate controllers to put into place proactive measures in order to be able to comply with all the elements of data protection law". [28]

---

[20] Commission of the European Communities, (n 18), 9.

[21] Which, as mentioned by Purtova (n.19), was also followed in the recent Case C-582/14 *Breyer* [2016] ECLI:EU:C:2016:779.

[22] Check Case C-131/12 *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* [2013] ECLI:EU:C:2013:424, Opinion of AG JÄÄSKINEN, para 72 ("The fact that their character as personal data would remain "unknown" to internet search engine provider, whose search engine works without any human interaction with the data gathered, indexed and displayed for search purposes, does not change this finding")

[23] Article 29 WP (n 6), 10.

[24] Article 29 WP (n 14), 13.

[25] Case T-259/03 *Nikolaou v Commission* [2007] ECLI:EU:T:2007:254, para 222.

[26] Article 4(7) GDPR

[27] Article 29 WP (n 10), 2.

[28] Opinion of the EDPS on the Communication from the Commission to the European Parliament, the Council , the Economic and Social Committee and the Committee of Regions – "A comprehensive approach

While accountability is not a novel concept in data protection[29], the shift[30] that we acknowledge in the GDPR is about the way that the legislator has chosen to set up a modified compliance scheme by, *inter alia*, materializing the accountability principle via a general obligation in Article 24[31] and via more specific obligations (e.g. DPOs, DPIAs, Privacy by design) all of which have a common characteristic: they all suggest specific measures and mechanisms which establish a proactive approach,[32] facilitate the implementation of accountability and therefore enable compliance and its demonstration thereof. They do not add any new principles; instead, they serve as mechanisms for the effective implementation of the already existing data protection principles.[33] Accountability and the compliance scheme as shaped by the legislator could be considered as a legal strategy "for defending what has been formally recognized".[34] And that is the data protection principles in Article 5. It has been argued that these principles constitute the "essence" of the fundamental right to data protection, in the meaning of Article 52(1) of the Charter of Fundamental Rights.[35] If this is the case, then the principle of accountability, whose main goal is a more effective data protection in practice, along with all the mechanisms and measures that enable it, relates to the scope of the fundamental right to data protection in that it requires that all data protection principles should be respected. In that way it actually enhances the rights-based approach and the fundamental rights character of the data protection legal framework.

Article 24, which constitutes the general obligation that materializes the principle of accountability, stipulates that the technical and organizational measures taken by the

---

on personal data protection in the European Union", < https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf > , 22.

[29] It first appeared as a basic data protection principle in the OECD Guidelines. OECD Guidelines on the Protection of privacy and transborder flows of personal data, 1980. < http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm >

[30] Alessandro Spina has also talked about a transformation in the GDPR, which is about an "enforced self-regulation model for managing technological innovation in uncertain scenarios", in Spina (n 3).

[31] As has been pointed out by the EDPS 'Opinion 5/2018, Preliminary Opinion on Privacy by Design'. "Article 24 refers to the implementation of all data protection principles and the compliance with the whole of the GDPR", para 25.

[32] Alhadeff J., Van Alsenoy B., Dumortier J. (2012) 'The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions'. In: Guagnin D., Hempel L., Ilten C., Kroener I., Neyland D., Postigo H. (eds) *Managing Privacy through Accountability*. Palgrave Macmillan, London <https://doi.org/10.1057/9781137032225_4>.

[33] Article 29 Data Protection Working Party WP 168 The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data, pp. 2,6; Alhadeff, Van Alsenoy and Dumortier (n 32), 27.

[34] Rodotà S. (2009) 'Data Protection as a Fundamental Right'. In: Serge Gutwirth and others (eds), *Reinventing Data Protection?*. Springer Netherlands doi: 10.1007/978-1-4020-9498-9 <//www.springer.com/gp/book/9781402094972> , 3.

[35] Joined cases *Digital Rights Ireland and Seitlinger and Others* (n 17), para 40. See also Orla Lynskey, *The Foundations of EU Data Protection Law* Oxford University Press 2015, ISBN: 9780198718239; EDPS (n 31), para 30.

controller should be dependent on the "nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons".[36] The legislator introduces *risk* as a criterion for "the determination of the concrete measures to be applied".[37] This is a choice that adds scalability when it comes to compliance, in the sense that the scope of the legal duties of data controllers depends on the risk posed by their processing operations,[38] and more specifically the *likelihood and severity* of that risk. Scalability is inextricably linked to the principle of accountability,[39] [40] in that the latter is "implemented through scalable obligations".[41] Putting *risk* in the spearhead of the compliance scheme as a way to implement the principle of accountability, does not and should not in any way alter the scope of the fundamental right. What it alters is the scope of the legal duties of data controllers, since these become dependent on the risks presented by the specific processing operations. Therefore, *risk* is a concept used in order to enable accountability, in that, by adding scalability to legal obligations, it allows for a more effective protection of personal data. It should be thus understood as a major criterion that belongs to the accountability principle and the proactive approach it establishes. Accountability has been characterised as a "fundamental principle of compliance".[42] That leads us to the conclusion that risk is a concept inextricably linked to the principle of accountability, and thus to compliance. *Risk* and compliance are in this way deeply interconnected.[43]

**The 'risk-based' approach.**

Because of the prominence of *risk* in the GDPR as well as the acknowledgment of a shift of approach with *risk* being the point of reference, the so called "risk based approach"[44] has captured the attention of legal scholars.[45] The debate on the relationship

[36] Also Recital 74 GDRP, mentions that measures of controllers should take into account the risk to the rights and freedoms of natural persons.

[37] Article 29 Data Protection Working Party, 'Opinion 3/2010 on the Principle of Accountability', 2.

[38] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks'.

[39] Article 29 WP (n 37).

[40] This has also been upheld by the EDPS (n 28), para 104.

[41] Commission, Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018, COM (2018) 43 final, 3.

[42] Alhadeff, Van Alsenoy and Dumortier (n 32), 19.

[43] Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) Volume 34, Issue 2, Computer Law & Security Review, 279-288, < https://doi.org/10.1016/j.clsr.2017.12.003.>

[44] The WP29 itself has also published a Statement on the risk-based approach of the GDPR: Article 29 WP (n 38).

[45] C Quelle, 'The "Risk Revolution" in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too.', in, R Leenes, R van Brakel, S Gutwirth and P De Hert (eds), *Data Protection and Privacy: The Age of Intelligent Machines* vol 10 (1st edn, Hart Publishing 2017); Macenaite (n 3); R Gellert, 'Why the GDPR Risk-Based Approach Is about Compliance Risk, and Why It's Not a Bad Thing.' in E Schweighofer, F Kummer & C Sorge (eds) *Trends und Communities der Rechtsinformatik - Trends and Communities of*

between the rights-based and the risk-based approach, was resolved by the WP29 which stated that the risk-based approach is a "scalable and proportionate approach to compliance" instead of an "alternative to well-established data protection rights and principles".[46] This statement makes us think twice on whether a debate between the rights-based and the risk-based approach, actually exists. Based on the line of arguments in the previous Subsection,[47] not only should we not consider these two approaches as opposing, but, on the contrary, we should understand the risk-based approach as a strategy for the enhancement of the rights-based character of the legal framework. The risk-based approach is integrated into the rights-based nature of the GDPR. They are not strictly separated and thus we should not follow a linear scheme whereby, first, full legal compliance takes place (in line with the rights-based character of the framework) and on top of that risk calculations are done (in line with the risk-based approach).[48]

By understanding *risk* as a concept inextricably linked to the principle of accountability and thus to compliance, we come to some valuable conclusions. First of all, relating the risk-based approach to the principle of accountability provides for a firm legal justification of *risk* as a criterion for the scalable and proportional approach to compliance. Secondly, we explain the modified compliance scheme introduced in the GDPR and we understand it as a way of enhancing the fundamental rights nature of data protection. This leads us to the third point which is the clarification of the relationship between the risk-based approach and the rights-based approach. The risk-based approach is not stand-alone. On the contrary, it is an expression of the principle of accountability[49] and is integrated into the rights-based approach, which is supposed to enhance.

Following the previous line of argumentation and based on the conclusions made, we can come to a further conclusion; we can draft away from the position that *risk* in the GDPR should be understood as a compliance (with the GDPR) risk.[50] The legislator seems to be trying to mitigate such a 'non-compliance risk', by adopting a different approach (which I discussed in the Subsection on 'The role of *risk'*) that introduces *risk* as a major criterion for more effective compliance. If we understood, under this scheme, risk as non-compliance risk, we would then run into a circle. Furthermore, if compliance with the GDPR meant that risks to rights and freedoms are reduced to an acceptable level, then the question that is raised is why then having *risk* as a concept inextricably linked to compliance, in the first place?

---

*legal informatics : Tagungsband des 20. Internationalen Rechtsinformatik Symposions - IRIS 2017 - Proceedings of the 20th International Legal Informatics Symposium.* Austrian Computer Society, pp. 527-532.

[46] Article 29 WP (n 38).

[47] Subsection on The role of *risk.*

[48] Gellert (n 43).

[49] This is something acknowledged also by the WP29, which stated that the "risk based approach […] has been introduced recently as a core element of the accountability principle itself", (n 38), 2.

[50] Gellert (n 43 & n 45).

# 3 The scope of *risk* in the GDPR: Risks to the "rights and freedoms of natural persons"

In the previous Section, we saw that the role, the meaning and the scope of each concept in the GDPR are highly interlinked. This interpretation has relied primarily on the legislator's broad wording which has been upheld and further elaborated by the WP29 and the CJEU. However, in the case of *risk* we do not have such clear guidance yet. Therefore, we need to carefully examine the legislator's wording which in combination with the role that *risk* plays, and the overall purpose of the GDPR, will provide us with important information as to the scope of the concept. Article 1(2) stipulates that:

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

Article 24 should also be taken into consideration. This is because of the role of *risk* and its connection to the principle of accountability, as discussed in Section 2. According to Article 24, for the implementation of appropriate technical and organizational measures, the data controller should take into account "the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons". Likewise, Article 35(1) requires an assessment of "high risk to the rights and freedoms of natural persons".[51] According to the WP29, the DPIA "primarily concerns the rights to data protection and privacy but may also involve other fundamental rights […]".[52]

We observe that the EU legislator gives an additional (double) dimension to the risks that might occur when personal data are processed. These risks should not be identified and assessed solely in relation to the right to data protection but they transcend its boundaries and have to be examined also in relation to other rights and freedoms that might be interfered with because of the processing operations that take place. Additionally, the risks should not be identified and assessed solely in relation to the data subject (the actor the rights of whom are protected under the data protection legal framework) but they transcend its boundaries and have to be examined also in relation to natural persons.

**'Risk to the Rights and freedoms…'.**

With regard to the "risk to the rights and freedoms", the legislator provides us with examples of the most relevant rights and freedoms, mainly in the Recitals of the GDPR. Recital 4, talks about

> "all fundamental rights […] the freedoms and principles recognized in the Charter as enshrined in the Treaties, in particular the respect for private

[51] Article 33 GDPR, also talks about "risk to the rights and freedoms of natural persons" in the case of a data breach.

[52] Article 29 WP (n 6), 6. The same position was upheld by the Article 29 WP (n 38), 4.

> and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

The WP29 has enriched the list by referring also to the freedom of speech, freedom of movement, prohibition of discrimination, right to liberty.[53] In Recital 75 the legislator enumerates risks in a non-exhaustive way (*"in particular"*): risk to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonimisation or any other significant economic or social disadvantage, the deprival of rights and freedoms or the prevention from exercising control over their personal data.

To give an example, let us consider the case where a data controller applies anonymization techniques on a set of personal data. Let us say that the personal data have been properly anonymized. In that case, they are not qualified as "personal" anymore, and therefore do not fall under the scope of the GDPR. As pointed out by the WP29, anonymization is a type of processing activity performed on personal data. While this processing operation will not result in a risk to the data subject's right to data protection (since its purpose is the anonymization of this data), it might well result in a risk to the individual's right to privacy.[54] For example, a dataset, although anonymized, may be given / sold to a third party which will take decisions (eg. calculation of credit risk) that will produce effects for the natural persons in that dataset. This risk is raised by the specific processing operation which while it is done as a technical measure for the mitigation of data protection risks, the purpose and use of this anonymized data set could raise a privacy risk.

An important point to be made is that *risks* are to be identified and assessed exclusively from the perspective of natural persons.[55] Whereas this is a point made in relation to the legal obligation of DPIAs, it should be understood as a general rule in all cases where data controllers are required to take into account the risks to rights and freedoms.

**'…of natural persons'.**

Data controllers should not limit the risk assessment to data subjects but they have to assess whether and in what way the processing operations could negatively impact also non data subjects (ie. natural persons whose personal data are not being processed). This is also acknowledged by the WP29 which stated that what should be taken into account is "every potential as well as actual adverse effect, assessed on a very wide scale ranging from an impact on the person concerned by the processing in question to a general societal impact".[56] This broad approach confirms also the quest for processing operations that are "designed to serve mankind".[57] Additionally, this approach is in line

---

[53] Article 29 WP (n 6) and Article 29 WP (n 38), 4.

[54] Article 29 WP (n 6), 11.

[55] Article 29 WP (n 6), 17.

[56] Article 29 WP (n 38), 4.

[57] Recital 4 GDPR "The processing of personal data should be designed to serve mankind"

with the sophisticated technical context,[58] whereby the outcomes of processing operations more often than not "refer to other or more people than those involved in the input data".[59]

The recent "Facebook - Cambridge Analytica"[60] case illustrates the way in which processing operations can raise risks that transcend the boundaries of data subjects and expand to natural persons and society at large. What is worth noting in this case is that the processing operations on personal data of Facebook users that downloaded the app, as well as personal data of their "friends" (who had not downloaded the app), had a broader societal impact, that is the "undermining of democratic legitimacy" via an unlawful and opaque interference with the "opinion formation process" for the elections.[61] These processing operations did not only create risks to the fundamental rights and freedoms of the data subjects but had a serious impact on the core values of our society. The European legislator intends to capture this wide spectrum of impacts, through the wording of both Article 24 and Article 35 GDPR.

## 4 The technology involved: IoT, AI, algorithms

It has been claimed and analysed why data protection "was born out of a need to protect fundamental rights from the risks created by the computer".[62] Technological developments have increased the risks to privacy and data protection, which need to be counterbalanced by the legal framework.[63] Therefore, when interpreting the concept of *risk* in data protection, one cannot disregard the technologies involved in data processing operations. As already mentioned,[64] *risk* is a scenario describing an event and its consequences. The technology involved in data processing operations relates to the "event" in this definition.

When talking about the data protection legal framework, one should keep in mind that 'technological-neutrality' should not be compromised but upheld. The quest for a

[58] See also Section 4 "The technology involved: IoT, AI, algorithms".

[59] Anton Vedder and Laurens Naudts, 'Accountability for the Use of Algorithms in a Big Data Environment' (2017) International Review of Law, Computers & Technology - Justice in Algorithmic Robes vol 31,Issue 2, 206- 224, 207.

[60] Cadwalladr C., Graham-Harrison E., "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", *The Guardian*, 17 Mar 2018.

[61] Council of Europe, Internet and Electoral Campaigns – Study on the use of Internet in electoral campaigns, DGI(2017)11, < https://rm.coe.int/use-of-internet-in-electoral-campaigns-/16807c0e24 >

[62] Gellert Raphaël, 'Understanding Data Protection as Risk Regulation' (2015) Internet Journal of Law, vol.18, n.11, pp. 3-15. Also see, Ware report, pp 37-38; EDPS (European Data Protection Supervisor), 'Opinion 5/2018, Preliminary Opinion on Privacy by Design'. " […] the birth of this legal concept is linked to the development and popularization of the computers first, and, more recently, of the Internet", 2.

[63] Article 29 WP (n 33), para 43.

[64] In the Introduction, where I refer to the definition of *risk* given by the WP29: "A risk is a scenario describing an event and its consequences, estimated in terms of severity and likelihood".

technologically neutral protection appears in Recital 15 GDPR[65] and has also been encouraged by both the EDPS[66] and the WP29.[67] Case law from the CJEU has shown that the use of open and broad terms is a strategy that allows for personal data protection to be adaptable to new technologies. For example, in the *Google Spain* case,[68] the broad, functional and in light of the fundamental rights interpretation of the term 'data controller', allowed for the identification of the responsible actor (allocation of responsibility); an actor who is new[69] in terms of functionality (internet search engines) within a complicated digital environment. The European Commission recently highlighted that the "EU's sustainable approach to technologies creates a competitive edge, by embracing change on the basis of the Union's values".[70]

### 4.1 New technologies: characteristics and challenges

In the following paragraphs I will present some of the main characteristics that new technologies (IoT, AI, algorithms) share. In line with the need to sustain the technologically-neutral character of the GDPR, I will group these characteristics in a way so that it becomes apparent that the legal challenges they present are similar and such should be the response to them.[71] Having done that, I intend to examine if and how these challenges could influence the concept of *risk* and potentially its role.

The Internet of Things (IoT) is a technology sector whereby a network of physical devices, sensors, software etc. is created. This network relies on "large data collection from diverse sources and data exchange with various devices to provide seamless, linked-up and personalized services".[72] Massive collection and linkage of user data as well as the creation of new information and inferences, are definitive characteristics of

---

[65] Recital 15 GDPR: "In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. […]"

[66] EDPS (n 28), para 38.

[67] Article 29 WP (n 33), 12.

[68] Case *Google Spain SL*, (n 16).

[69] Case *Google Spain SL*, Opinion of AG JÄÄSKINEN (n 22), para 10: "the present preliminary reference is affected by the fact that when the Commission proposal for the Directive was made in 1990 the internet in the present sense of the www did not exist and nor where there any search engines. […] nobody could foresee how it would revolutionise the world"

[70] Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe COM(2018) 237 Final <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe> accessed 10 November 2018.

[71] See also, Sandra Wachter, Brent Mittelstadt and Luciano Floridi, (2017) 'Transparent, Explainable, and Accountable AI for Robotics' Science Robotics 2(6):eaan6080: "Designing imprecise regulation that treats decision-making algorithms, AI and robotics separately is dangerous. It misinterprets their legal and ethical challenges as unrelated. Concerns about fairness, transparency, interpretability and accountability are equivalent, have the same genesis, and must be addressed together, regardless of the mix of hardware, software, and data involved".

[72] Sandra Wachter (2018) 'The GDPR and the Internet of Things: a three-step transparency model', Law, Innovation and Technology, 10:2, 266-294, DOI: 10.1080/17579961.2018.1527479.

IoT, so that a more personalized experience is provided to the users.[73] Artificial intelligence (AI) "refers to systems that display intelligent behavior by analyzing their environment and taking actions –with some degree of autonomy- to achieve specific goals".[74] AI needs vast amounts of data to be developed, to learn about and to interact with the environment. Algorithms are encoded procedures through which input data are being transformed into a usable, and therefore desirable, output.[75] "By following a logical and mathematical sequence, they can structure and find additional meaning in a big data environment".[76] Many of these systems operate as "black boxes"; [77] they are opaque software tools working outside the scope of meaningful scrutiny and accountability.

The afore mentioned technologies present a high degree of complexity[78] due to the interdependency between the different components and layers[79]. Each system is part of a larger structure and forms part of a sequence of outputs.[80] Complexity also results from the multiple actors involved in these ecosystems.[81] For their optimal functionality, the systems require the processing of vast amounts of data. Additionally, they also generate a huge amount of data.[82] Last but not least, these systems present autonomy in their behavior[83] which derives from the self-learning process and leads to the interpretation of the environment and to the execution of actions without human intervention.[84]

The complexity of these systems together with their autonomous behavior lead to the issue of 'unpredictability' of both their behavior and their outputs. It is quite possible that methods and usage patterns developed by these systems were not considered, not even imagined by the entity that collects the data nor the data subject at the time of collection.[85] At the same time, the black-box phenomenon, along with the complexity

---

[73] Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' 11 Nw. J. Tech. & Intell. Prop. 239 (2013).

[74] Commission (n 70).

[75] Gillespie, Tarleton (2012) 'The Relevance of Algorithms', In Gillespie, Tarleton, Boczkowski, Pablo and Foot, Kirsten (eds) Media Technologies: Essays on Communication, Materiality and Society, Cambridge, MA: MIT Press. doi: 10.7551/mitpress/9780262525374.003.0009.

[76] Vedder and Naudts (n 59).

[77] Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, 2015 ISBN 9780674368279.

[78] Complexity is both on a technical and a contextual level. For a more extensive analysis of "technical and contextual complexity of algorithms" check Vedder and Naudts (n 59).

[79] Commission Staff Working Document: Liability for Emerging Digital Technologies SWD(2018) 137 Final'<https://ec.europa.eu/digital-single-market/en/news/european-commission-staff-working-document-liability-emerging-digital-technologies> , 9 "[…] (i) the tangible parts/devices (Sensors, actuators, hardware), ii) the different software components and applications, to iii) the data itself, iv) the data services (ie. collection, processing, curating, analysing), and v) the connectivity features."

[80] Vedder and Naudts (n 59).

[81] Commission (n 79).

[82] Commission (n 79).

[83] Commission (n 79). "AI software can reason, gather knowledge, plan intelligently, learn, communicate. Perceive and manipulate objects"

[84] These are characteristics identified and grouped by the Commission (n 79).

[85] Purtova (n 19).

of these systems' functionality, raise issues with regard to the 'explainability and interpretability' of both the systems per se and their outputs.

### 4.2 New technologies and the concept of risk

According to Rodotà, new technologies and their characteristics create "a reality that becomes estranged from the fundamental rights' framework" in the sense that "some of the principles underlying the system of personal data protection are being slowly eroded".[86] [87] For example, the principle of transparency highly relates to the issue of interpretability of these systems. The inherent opacity and complexity of algorithmic systems challenges the right to information. However, transparency of processing operations is a fundamental requirement of the GDPR[88] since it constitutes the basis for the data subject to exercise all their rights. As Kaminski notes, "information asymmetries render underlying rights effectively void".[89] If transparency is difficult (or even impossible) to achieve, then a major risk is the data subject being deprived of having control over their personal data. Against this reality, we must ensure that the regulatory frameworks for developing and using of AI technologies are in line with these values and fundamental rights.[90] In this line, when talking about *risk* in data protection, it should be understood as a major criterion for enhancing the fundamental rights character of the data protection framework.

As mentioned already, an important characteristic is the complexity presented by these technologies. It is a double-pronged complexity, in terms of systems' functionality and in terms of actors involved and the network created. The consequence is a distribution of control over multiple actors, which in turn has major implications for the allocation of responsibility among them. For example, "the developer of algorithmic tools may not know their precise future use and implementation [while] [t]he person(s) implementing the algorithmic tools for applications may, in turn, not fully understand how the algorithmic tools operate".[91] Each actor has knowledge limited to their role, and their ability to mitigate risks is again dependent on their role in this chain of actors. The allocation of accountability for algorithmic decision-making becomes therefore complicated.[92] As mentioned in an earlier section,[93] *risk* relates to accountability. Allocation of accountability and responsibility is a prerequisite for compliance and effective

---

[86] Rodotà (n 34).

[87] For a more extensive overview of how data protection principles are influenced by the advancement of new technologies, check Wachter (n 72). Also see C Kuner and others, 'The Challenge of "big Data" for Data Protection' (2012) 2 International Data Privacy Law 47. And Macenaite (n 3), 6.

[88] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251rev.01)' 29, 9.

[89] Margot E Kaminski, 'The right to explanation, explained' 26, DOI: 10.31228/osf.io/rgeusp, 21.

[90] Commission (n 70).

[91] Council of Europe, Algorithms and Human Rights Study on the Human Rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, DGI (2017)12, 39.

[92] idem, 39.

[93] Section 2 'The role of *risk* in the GDPR: Accountability & Risk-based approach'

data protection. If this is not done correctly, then risk assessment and management will be incomplete and incorrect. This is the reason why, both risk assessment and risk management should be a multi-actor exercise. That points towards the role of developers, who are considered to be the ones with the expert knowledge when it comes to the functionality of new technologies. The GDPR does not impose any legal obligations on developers. However, their involvement is highly recommended. Recital 78,[94] [95] the WP29[96] and the EDPS[97] encourage the more active involvement of developers in the identification, assessment and management of risks.

New technologies "may create new types of risks or accentuate existing risks".[98] An example of the creation of new types of risks can be found in profiling and invasive inferential analytics.[99] They both involve processing operations that raise new types of risks due to the functionality of the new technologies used (additional collection and sharing of personal data). A similar new type of risks, are cybersecurity risks. An example of the accentuation of existing risks can be found in the case of discrimination. Discrimination is an already existing risk which could, however, be accentuated because of the increased possibility of bias in algorithms. Additionally, new technologies may also bring out other dimensions of the rights and freedoms as we know them. This is, for example, the case of **"**interdependent privacy"[100] or "group privacy rights".[101] What we realize is that *risk* is not a static concept. In this technical context it is more dynamic than ever before and is subject to transformations/additions/changes. It is a

---

[94] Recital 78 GDPR: "[…] producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations."

[95] Recitals are not legally binding as are the substantial provisions of the legal framework. However, they are supposed to "cast light on the interpretation to be given to a legal rule", Case 215/88 *Casa Fleischhandels-GmbH v Bundesanstalt für landwirtschaftliche Marktordnung* [1989] ECLI:EU:C:1989:331, para 31.

[96] Article 29 WP (n 6), 8 : "A DPIA can also be useful for assessing the data protection impact of a technology product, for example a piece of hardware or software, where this is likely to be used by different data controllers to carry out different processing operations. Of course, the data controller deploying the product remains obliged to carry out its own DPIA with regard to the specific implementation, but this can be informed by a DPIA prepared by the product provider, if appropriate.".

[97] EDPS (n 31), para 37.

[98] Commission (n 79).

[99] Wachter (n 72).

[100] Gergely Biczók and Pern Hui Chia, 'Interdependent Privacy: Let Me Share Your Data' in Ahmad-Reza Sadeghi (ed), *Financial Cryptography and Data Security* (Springer Berlin Heidelberg 2013).

[101] Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) Philosophy & Technology 30:475 DOI: https://doi.org/10.1007/s13347-017-0253-7; Alessandro Mantelero, 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2017) <https://doi.org/10.1007/978-3-319-46608-8_8> ; Luciano Floridi, 'Group Privacy: A Defence and an Interpretation' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2017) <https://doi.org/10.1007/978-3-319-46608-8_5> .

concept highly dependent on the advancement of technology. We can therefore acknowledge the importance of having in place a broad scope of the concept of *risk* as already suggested by the legislator. It will also challenge the process of identifying *risks*, in the sense of being able to foresee them.[102] This points towards the need of having a flexible and dynamic concept of *risk*.

Until now, I have discussed the challenges that new technologies bring and what they tell us about the concept of *risk*. However, what needs to be acknowledged is that new technologies do not only raise risks but can and should be used to also address them (e.g. an AI system will be trained and then used to spot cyberattacks on the basis of data from the concerned network or system).[103] Technology is both a friend and a foe for fundamental rights and freedoms. This is also apparent from the fact that "data protection by design and by default" is introduced in Article 25.

## 5 Conclusion

In this article I answered the following research question: "How do the role and the scope of *risk* in the GDPR as well as the technology involved in data processing operations inform the meaning of *risk* in the field of data protection?"

To answer this research question, I firstly examined the 'role' that has been attributed to *risk* in the GDPR. I argued that *risk* is inextricably linked to the principle of accountability and thus to compliance. Its role is to contribute to the effective protection of the "essence" of the fundamental right to data protection and therefore enhance the rights-based approach of the GDPR. By furthermore explaining that the GDPR introduces a modified compliance scheme through an enhanced accountability principle, I argued that *risk* should not be understood as a '(non)compliance risk'. I then turned to the examination of the 'scope' of *risk*. By looking at the legislator's wording and by identifying the broad scope and meaning they assign to *risk* ("risk to the rights and freedoms of natural persons") I argued in favor of the legislator's intention to place *risk* in a central position in the broader system of protection of fundamental rights and freedoms.

This broad scope is in line with the current data processing reality, whereby data operations are largely and increasingly performed via the use of new technologies (e.g. IoT, AI) thereby raising risks to all fundamental rights and freedoms. Due to the complexity, the autonomy in behavior and the vast amounts of data they process but also generate, new technologies require that *risk* is given a flexible and dynamic meaning, so that it captures new risks that are raised but also novel dimensions of the fundamental rights as we currently know them. Apart from the broad scope in terms of subject matter, *risk* should have an equally broad scope in terms of the actors involved in its assessment and management. Allocation of responsibility in complex ecosystems is difficult given that control is distributed among the multiple actors involved. Adopting a functional approach towards *risk* by examining the factual influence of each actor, is highly suggested and renders the assessment and management of *risk*, a multi-actor

[102] Wachter (n 72) "the uncertain value of personal data generated and processed by IoT devices and services necessarily limits the scope of risks that can be foreseen, and thus the protection offered by DPIAs"

[103] Commission (n 70).

exercise, whereby technology developers and providers have an important role to play. Apart from the fact that this enhances the role that the risk is called to play, it is also in line with the principle of proportionality that should apply to the legal duties of data controllers. Aiming for a broad, open and flexible concept of risk additionally enhances the technologically-neutral character of the data protection legal framework.

In this article, I extracted information from the GDPR and explained the reason why they should be used as means of interpretation of the concept of *risk* in data protection. This is one important message of this article. The second message of the article is that we shall not disregard the new technologies involved in data processing operations and the way in which their characteristics can influence our understanding of *risk*. This is an element also extracted from the GDPR. The understanding of the role and the scope attributed to *risk* in the GDPR, and of the new technologies involved in data processing operations, all contribute to the development of a theoretical framework against which the concept of *risk* can be approached in an objective and consistent way in the field of data protection. The findings of this article should be understood as a firm starting point for further steps to be taken towards the legal qualification of *risk* as well as of its constitutive elements (likelihood and severity) in data protection.

**References**


1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281, 23.11.1995, p. 31–50.
2. Regulation (EU) 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 L 119, 4.5.2016, p. 1–88.
3. Case C-131/12 *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* [2014] ECLI:EU:C:2014:317.
4. Case C-131/12 *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* [2013] ECLI:EU:C:2013:424, Opinion of AG JÄÄSKINEN.
5. Case C-274/99 P *Connolly v Commission* [2001] ECLI:EU:C:2001:127.
6. Case C-465/00 *Österreichischer Rundfunk and Others* [2003] ECLI:EU:C:2003:294.
7. Case C-212/13 *Ryneš* [2014] ECLI:EU:C:2014:2428.
8. Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C: 2014:238.
9. Case C-582/14 *Breyer* [2016] ECLI:EU:C:2016:779.
10. Case T-259/03 *Nikolaou v Commission* [2007] ECLI:EU:T:2007:254.
11. Case C-473/12, *IPI* [2013] EU:C:2013:715.
12. Case 215/88 *Casa Fleischhandels-GmbH v Bundesanstalt für landwirtschaftliche Marktordnung* [1989] ECLI:EU:C:1989:331.
13. Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data'.
14. Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"'.
15. Article 29 Data Protection Working Party 'Opinion 3/2010 on the Principle of Accountability'.
16. Article 29 Data Protection Working Party 'Opinion 05/2014 on Anonymisation Techniques'.
17. Article 29 Data Protection Working Party 'Statement on the role of a risk-based approach in data protection legal frameworks.' Tech. Rep. WP 218 (30 May 2014).

18. Article 29 Data Protection Working Party 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' WP 248 rev 0.1 (4 April 2017), as last revised and adopted on 4 October.
19. Article 29 Data Protection Working Party 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251rev.01)'.
20. Article 29 Data Protection Working Party WP 168 The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data. 28
21. Commission of the European Communities, 'Amended Proposal for a COUNCIL DIRECTIVE on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data'.
22. Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe COM(2018) 237 Final <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe> .
23. Commission, Communication from the Commission to the European Parliament and the Council, Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018, COM(2018) 43 final < https://ec.europa.eu/commission/sites/beta-political/files/data-protection-communication-com.2018.43.3_en.pdf>.
24. Commission, Commission Staff Working Document: Liability for Emerging Digital Technologies *Accompanying the document* Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe SWD(2018) 137 Final, <https://ec.europa.eu/digital-single-market/en/news/european-commission-staff-working-document-liability-emerging-digital-technologies>.
25. Council of Europe, Internet and Electoral Campaigns – Study on the use of Internet in electoral campaigns, DGI(2017)11, <https://rm.coe.int/use-of-internet-in-electoral-campaigns-/16807c0e24 >.
26. Council of Europe, Algorithms and Human Rights Study on the Human Rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, DGI(2017)12 < https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html>.
27. EDPS (European Data Protection Supervisor), 'Opinion 5/2018, Preliminary Opinion on Privacy by Design', 31 May 2018.
    EDPS (European Data Protection Supervisor), Opinion of the EDPS on the Communication from the Commission to the European Parliament, the Council , the Economic and Social Committee and the Committee of Regions – "A comprehensive approach on personal data protection in the European Union", Brussels, 14 January 2011 < https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf >
28. OECD Guidelines on the Protection of privacy and transborder flows of personal data, 1980. <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm >.
29. Alhadeff J., Van Alsenoy B., Dumortier J. (2012) The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions. In: Guagnin D., Hempel L., Ilten C., Kroener I., Neyland D., Postigo H. (eds) Managing Privacy through Accountability. Palgrave Macmillan, London <https://doi.org/10.1057/9781137032225_4>.

30. Biczók G and Chia PH, ‘Interdependent Privacy: Let Me Share Your Data’ in Ahmad-Reza Sadeghi (ed), Financial Cryptography and Data Security (Springer Berlin Heidelberg 2013).
31. Cadwalladr C., Graham-Harrison E., “Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach”, *The Guardian*, 17 Mar 2018.
32. Floridi L, ‘Group Privacy: A Defence and an Interpretation’ in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), Group Privacy: New Challenges of Data Technologies (Springer International Publishing 2017) <https://doi.org/10.1007/978-3-319-46608-8_5> .
33. Gellert R, *‘Why the GDPR Risk-Based Approach Is about Compliance Risk, and Why It’s Not a Bad Thing.’ in E Schweighofer, F Kummer & C Sorge (eds) Trends und Communities der Rechtsinformatik - Trends and Communities of legal informatics : Tagungsband des 20. Internationalen Rechtsinformatik Symposions - IRIS 2017 - Proceedings of the 20th International Legal Informatics Symposium*. Austrian Computer Society, pp. 527-532.
34. Gellert R, ‘Understanding the Notion of Risk in the General Data Protection Regulation’ (2018) Volume 34, Issue 2, Computer Law & Security Review, 279-288, < https://doi.org/10.1016/j.clsr.2017.12.003.>.
35. Gellert R, ‘Understanding Data Protection as Risk Regulation’ (2015) Internet Journal of Law, vol.18, n.11, pp. 3-15.
36. Gillespie, T (2012) ‘The Relevance of Algorithms’, In Gillespie, Tarleton, Boczkowski, Pablo and Foot, Kirsten (eds) Media Technologies: Essays on Communication, Materiality and Society, Cambridge, MA: MIT Press. doi: 10.7551/mitpress/9780262525374.003.0009.
37. Rodotà S. (2009) ‘Data Protection as a Fundamental Right’. In: Serge Gutwirth and others (eds), *Reinventing Data Protection?*. Springer Netherlands doi: 10.1007/978-1-4020-9498-9 <//www.springer.com/gp/book/9781402094972> .
38. Kaminski, M. (2018, June 19). The Right to Explanation, Explained. https://doi.org/10.31228/osf.io/rgeus.
39. Kuner C and others, ‘The Challenge of “big Data” for Data Protection’ (2012) 2 International Data Privacy Law 47.
40. Lenaerts K and Gutiérrez-Fons JA, ‘To Say What the Law of the EU Is : Methods of Interpretation and the European Court of Justice’ (2013) EUI Working Papers AEL 2013/9 <http://cadmus.eui.eu//handle/1814/28339> accessed 16 June 2018.
41. Lynskey O, The Foundations of EU Data Protection Law, Oxford University Press 2015, ISBN: 9780198718239.
42. MACENAITE, M. (2017). The “Riskification” of European Data Protection Law through a two-fold Shift. *European Journal of Risk Regulation*, 8(3), 506-540. doi:10.1017/err.2017.40.
43. Mantelero A, ‘From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era’ in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), Group Privacy: New Challenges of Data Technologies (Springer International Publishing 2017) <https://doi.org/10.1007/978-3-319-46608-8_8> .
44. Mittelstadt B, ‘From Individual to Group Privacy in Big Data Analytics’ (2017) Philosophy & Technology 30:475 DOI: https://doi.org/10.1007/s13347-017-0253-7.
45. Purtova, N (2018) 'The law of everything. Broad concept of personal data and future of EU data protection law', Law, Innovation and Technology, 10:1, 40-81, DOI: 10.1080/17579961.2018.1452176.
46. Pasquale, F The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, 2015 ISBN 9780674368279.
47. Quelle C, ‘The “risk Revolution” in EU Data Protection Law: We Can’t Have Our Cake and Eat It, Too.’, In R Leenes, R van Brakel, S Gutwirth and P De Hert (eds), *Data Protection and Privacy: The Age of Intelligent Machines* vol 10 (1st edn, Hart Publishing 2017).

48. SPINA, A. (2017). A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics. *European Journal of Risk Regulation*, 8(1), 88-94. doi:10.1017/err.2016.15.
49. Tene O and Polonetsky J, 'Big Data for All: Privacy and User Control in the Age of Analytics' 11 Nw. J. Tech. & Intell. Prop. 239 (2013).
50. Vedder A and Naudts L, 'Accountability for the Use of Algorithms in a Big Data Environment' (2017) International Review of Law, Computers & Technology - Justice in Algorithmic Robes vol 31, Issue 2, 206- 224.
51. Wachter S, (2018) 'The GDPR and the Internet of Things: a three-step transparency model', Law, Innovation and Technology, 10:2, 266-294, DOI: 10.1080/17579961.2018.1527479.
52. Wachter S, Mittelstadt B and Floridi L, (2017) 'Transparent, Explainable, and Accountable AI for Robotics' Science Robotics 2(6):eaan6080.