BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 4 • N° 12 • AUGUST 2018

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

UNDERSTANDING THE BALANCING ACT BEHIND THE LEGITIMATE INTEREST OF THE CONTROLLER GROUND: A PRAGMATIC APPROACH

by Irene Kamara and Paul De Hert

Abstract

The General Data Protection Regulation provides new tools and concepts such as Data Protection Impact Assessments, accountability and certification, but to a large extent retains the rationale of the Data Protection Directive for a principles-driven legislation. One of the cornerstones of both the reformed and new EU data protection legislation is the grounds for lawful processing.

Much debate has taken place over consent and the conditions for a meaningful informed choice of the data subject, while other grounds have not been at the spotlight of academia and practitioners. The legitimate interest of the controller has been one of the least discussed legal grounds for lawful processing, with a few exceptions, mainly the opinion of the Article 29 Data Protection Working Party, despite its significance as equally binding ground for processing. This contribution analyses the concept of legitimate interest of the controller of art. 6 (f) GDPR in relation to art. 7 (f) of the Data Protection Directive 95/46/EC and the interpretations of the concept by the Court of Justice of the EU and the Article 29 Data Protection Working Party.

Keywords: Article 6 GDPR, balancing, Breyer, consent, Data processing, ground for processing, legitimate interest

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html
ISSN N° 2565-9979. This version is for academic use only.

This is a Working Paper (version: May 2017). Please refer to the final published version: Kamara, I., & De Hert, P. (2018). Understanding the Balancing Act behind the Legitimate Interest of the Controller Ground. In E. Selinger, J. Polonetsky, & O. Tene (eds.), **The Cambridge Handbook of Consumer Privacy** (pp. 321-352). Cambridge: Cambridge University Press. doi: 10.1017/9781316831960.019

Disclaimer

Reproduction and translation for non-commercial purposes are authorized, provided the source is acknowledged and the publisher is given prior notice and sent a copy.

1. Introduction

The new EU legislation regulating the protection of personal data is finally adopted after a lengthy legislative process, which lasted nearly four years. The General Data Protection Regulation (GDPR) is a legal instrument of 99 Articles and 173 Recitals, directly applicable to all EU Member States of the European Union.[2]

The GDPR, which replaced the Data Protection Directive, aims to modernise and render more effective data protection law, aiming among others to respond to technological challenges and the risks emerging technologies pose to the protection of personal data. Fundamental rights concerns partly explain the reform. Protection of personal data received the status of a fundamental right in the EU with the adoption of the Lisbon Treaty.[3]. Another important concern is the need for enabling free movement of personal data, or, as Recital (10) of the Regulation provides, to 'remove the obstacles to flows of personal'. One of the cornerstones of the protection of personal data in that respect is the lawfulness of processing. Lawfulness of processing is one of the fundamental principles relating to processing of personal data, established in art. 5(1) (a) GDPR, according to which: "Personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject". Article 6, provides six grounds for lawfulness of processing: consent of the data subject (6(1) (a)), legal obligation of the controller (6(1) (c)), performance of a contract (6(1) (b)), vital interests of the data subject (6(1) (d)), performance of a task carried out in the public interest or the exercise of official authority (6(1) (e)) and the legitimate interest of the controller (6(1) (f)). The GDPR requires that at least one of these six grounds applies in each data processing operation for the processing to be deemed lawful. The grounds are to a large extent same as the Data Protection Directive 95/46/EC. Despite the numerous opinions and essays on other grounds, mainly relating to the conditions for a valid consent, the legitimate interest of the controller has not been at the spotlight. Some comments on the topic deal critically with this ground as a basis for lawful processing, sometimes going as far as to characterise the ground as a 'loophole' for the protection of personal data, for the reason of being flexible enough in comparison with some stricter or at least more straightforward requirements for the other grounds for lawful processing of art. 6 GDPR (and relevant art. 7 of the Data Protection Directive). While authorities and academics are in general hesitant to discuss in depth the legitimate interest of the controller ground (except for the Article 29 Data Protection Working Party opinion in 2014), this does not seem to be the case for actual practice and data controllers, which quite often rely on that ground.[4]

1 Paul De Hert paul.de.hert@vub.be, Irene Kamara i.kamara@tilburguniversity.edu, Vrije Universiteit Brussel, Research Group on Law, Science, Technology and Society (LSTS) and Tilburg University, Tilburg Institute for Law, Technology and Society (TILT). The authors would like to thank Omer Tene for his comments on a previous version of this chapter.

2 The final version of the GDPR was published in May 2016 in the Official Journal of the EU, but applies in May 2018. The EU legislator offers to persons bound by GDPR a two-year transition period from the old regime of the Data Protection Directive 95/46/EC to the new GDPR. In parallel, data protection authorities, the independent supervisory authorities of the EU Member States responsible for supervising the application and compliance with the GDPR, will also make use of the two-year period to adjust to their new tasks and increased powers.

3 Art. 8 of the Charter of Fundamental Rights of the EU. This advancement of the status is often called 'constitutionalisation' of the right to protection of personal data. See De Hert, Paul, and Serge Gutwirth. "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power." Erik Claes, Antony Duff, Serge Gutwirth (eds.) Privacy and the criminal law, Interentia, 2006, pp. 61-104.

4 For instance a paper published by the think-tank CIPL, which, based on insights shared by the industry participants of CIPL, identifies a list of current practices, where legitimate interest is used as a ground for processing. The paper highlights that "organisations in all sectors currently use legitimate interest processing for a very large variety of processing personal data and this trend is likely to continue under the GDPR". Centre for Information Policy Leadership (CIPL) Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR" May 2017, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf (accessed 20 May 2017)

Taking into account the above, this contribution proposes a formalisation of the balancing act of art. 6(1) (f) GDPR. We propose three steps in this act: legitimacy of the interest of the controller, necessity of the pursued aim and the balancing of opposing interests of the controller and the data subject. We also discuss essential components of each step that help determine the outcome of the test. We argue that the legitimate interest of the controller ground is largely based on context and might significantly differ on a case-by-case level. The legitimate interest ground, is not a loophole in the new EU data protection law. It is an equally important ground for legitimate processing. If misinterpreted or applied in bad faith the ground can be seen as too lenient or a loophole. The newly introduced accountability principle, the other principles of art. 5 GDPR and of course art. 8 and 52(2) Charter however set the proper framework for the grounds of lawful processing, including the legitimate interest of the controller or a third-party ground of art. 6(1) (f) GDPR.

The contribution is structured as follows: First, we briefly refer to the fundamental right to protection of personal data, enshrined in the Charter of Fundamental Rights and the conditions for interference to the right, set in art. 52(2) Charter. Section three presents the grounds for lawful processing in the Data Protection Directive and the criticism exercised on the legitimate interest ground. This section helps better understand section four, the transition from the Directive to the GDPR. Section four includes the main discussions in the preparatory works of the GDPR and the proposed conceptualisation of the legitimate interest of the controller ground of art. 6(1) (f). Following that, the fifth section provides an overview and analysis of the most relevant case law of the Court of Justice of the EU in relation to the legitimate interest ground, with the aim to shed light to the analysis. Last, section six provides examples of legitimate interest grounds and examines the 'suitability' of the ground in each of these cases. The contribution ends with conclusions which provide a summary of the discussion and reflections for the application of the provision.

2. The fundamental right to protection of personal data

2.1 Charter of Fundamental Rights: not an absolute right and the limitations to the rights provided for in art. 52 (1) Charter

The right to protection of personal data is established as an autonomous self-standing right in the Charter of the Fundamental Rights of the European Union. The Charter was declared legally binding with the Lisbon Treaty in 2009. Art. 8 of the Charter 'constitutionalised' the right by protecting it separately than the right to respect of private life protected in art. 7 of the Charter. Paragraph 2 of art. 8 Charter already provides the legal basis for processing. Processing may be based on the consent of the individual concerned or other legitimate basis laid down by law. The right to protection of personal data is not an absolute right. Limitations to the right are provided in art.52 of the Charter, which should be read in combination with art. 8(2). Limitations need to be provided for by law, respect the essence of the right, and be necessary and proportionate. The primary law of the EU therefore, already provides the framework in which a limitation to the right of art. 8 can take place. Due to the hierarchy of the EU legislation (primary, secondary law) and the fact that the EU data protection legislation has its legal basis in the EU primary law, including art.16 Treaty on the Functioning of the European Union (TFEU) and the Charter, any limitation cannot deviate, or go further than the conditions of art. 8 and 52 Charter.

2.2 European Convention of Human Rights and the proportionality test

Beyond the Charter and the European Union, the European Convention of Human Rights has long protected the right for protection of personal data, as an aspect of the right to respect for private life (art. 8 ECHR). Art. 8 (2) ECHR provides that by means of exception, interference with the right to respect for private life, is allowed under conditions. The article establishes a proportionality test to assess whether an interference is allowed. The interference has to be in accordance with the law ('legality'), have a legitimate basis ('legitimacy') and be necessary in a democratic society ('proportionality stricto sensu').[5] The article provides exhaustively a list of broadly framed interests, which qualify to provide a legitimate basis for the interference to the right to respect for private life. These are national security, public safety, the economic wellbeing of a country, the prevention of disorder or crime, the protection of health, the protection of morals, the protection of the rights and freedoms of others. Even though the EU data protection legislation is not legally based on the ECHR, to which the EU is only one of the member- parties, we take notice of the significant influences of the Convention to the EU data protection law. The new GDPR explicitly acknowledges that restrictions to data protection principles and the rights of the individuals should be "in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms."[6]

Balancing of conflicting interests and rights has been a doctrinal tool with which the Courts, both the European Court of Human Rights and the Court of Justice of the European Union, are following the doctrine in cases that involve conflicts of rights.[7] Several scholars have developed theories and frameworks on the principle of proportionality,[8] how to balance conflicting interests, and ultimately whether 'balancing' is appropriate doctrine when conflicts between interests occur.[9] According to Alexy's theory, the Law of Balancing, balancing can be broken down into three stages:

> "The first stage is a matter of establishing the degree of non-satisfaction, of, or detriment to, the first principle. This is followed by a second stage, in which the importance of satisfying the competing principle is established. Finally, the third stage answers the question of whether or not the importance of satisfying the competing principle justifies the detriment to, or non-satisfaction of, the first."[10]

Alexy in his theory refers to competing instead of conflicting principles. In the balancing, this would have consequences as to what the expected outcome of the assessment is. In conflicting principles, the conflict must be resolved in an "all or nothing fashion", whereas in the case of two competing principles, one

5 Read further Korff Douwe "The Standard Approach Under Articles 8 – 11 ECHR and Article 2 ECHR", 2008, http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf, (accessed 16 October 2016)

6 Recital 73 GDPR

7 The balancing doctrine has been criticised by Habermas for depriving constitutional rights of their normative power, in the sense that rights are downgraded to the level of policies, goals and values. Habermas also criticises the balancing approach for an underlying "irrationality". He argues that "because there are no rational standards here, weighing takes place either arbitrarily or unreflectively, according to customary standards and hierarchies" (see comments in Alexy Robert "Constitutional Rights, Balancing, and Rationality", Ratio Juris, vol. 16 no. 2, 2003, p.134). Habermas Jurgen, Between facts and norms, Cambridge: Polity, 1992

8 De Vries, Sybe A. "Balancing fundamental rights with economic freedoms according to the European court of justice." Utrecht Law Review 9.1, 2013, pp. 169-192.

9 See Harbo Tor-Inge "The Function of the Proportionality Principle in the EU law" European Law Journal, vol. 16 no.2, 2010, pp.158-185, Möller, Kai. "Proportionality: Challenging the critics." International journal of constitutional law 10.3, 2002, pp. 709-731,

10 Alexy, Robert, A Theory of Constitutional Rights, Oxford University Press, 2002

of the principles must be outweighed, without this meaning that the outweighed principle is invalid.[11] The concept of competing principles from that perspective is an interesting theoretical tool to read the legitimate interest of the controller ground in the GDPR. An interesting discussion relates to whether rights should be perceived as principles or rules.[12] Harbo, when interpreting Alexy's conceptualisation, asserts that perceiving rights as principles rather than rules, implies that rights are not absolute, and can be thus weighted against other "principles, i.e. against other individual rights but also policies laid down in legislative measures".[13] On the other hand, Dworkin's theory supports the view that "rights are only law, i.e. trumps vis-à-vis arguments of policy, or collective rights expressed through legislative acts."[14] In terms of the right to protection of personal data as enshrined in the art. 8 of the Charter, this discussion as extends to whether rights are absolute or relative, has been solved with art. 52 Charter, as mentioned above, which provides that the right of art. 8 can be subject to limitations. Despite this, influence of such theories can be traced in the provisions of EU data protection law, and the balancing test of the legitimate interest ground, even though an one-to-one application of the one or the other theory is not visible.[15]

3. EU data protection legislation: the 1995 EU Data Protection Directive

Taking the analysis to the secondary law of the EU, the 1995 Data Protection Directive introduces the grounds for lawful processing ('criteria for legitimate data processing') in its art. 7. The criteria are listed exhaustively and severally ('or..or'). If at least one of the grounds is fulfilled, the data processing operation is allowed.[16]

3.1 Consent in art. 7(a) of the Directive

Art. 7(a) requires the unambiguous consent of the data subject. Much discussion has been revolving around the question of when the consent is unambiguous, whether it has to be active or passive action is also sufficient, how relevant is consent in the context of technological emergence and automated processing (e.g. big data).[17] By definition, consent includes several requirements. It has to be freely given, specific and informed indication of the data subject's wishes by which the data subject signifies his or her agreement for the processing of personal data relating to him or her. The Article 29 Data Protection Working Party (WP29) has provided practical guidance on the conditions of a valid consent.[18] Data controllers often rely on this ground, especially in the context of the Internet or mobile applications. An (even not legitimately acquired) agreement of the data subject itself often offers a false assurance to the controller of legality of the data processing. However, it is very important that all the conditions for the valid consent – including the possibility of withdrawal - are fulfilled. An agreement to data processing without proper information being provided in advance to the data subject is not valid, and a processing operation based

11 Harbo (2010) p. 166
12 The distinction between rights and principles is clarified in art. 51(1) of the Charter: "subjective rights shall be respected, whereas principles shall be observed".
13 Harbo (2010) p. 166
14 Ibid.
15 Further analysis however evades the scope of this contribution.
16 See for extensive analysis read sub-section 4.3 of this Working Paper.
17 Read further Boyd, Danah, and Kate Crawford. Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon, Information, communication & society 15, no. 5 (2012), pp.662-679. Cate, Fred H., and Viktor Mayer-Schönberger "Notice and consent in a world of Big Data" International Data Privacy Law 3, no. 2 (2013) pp. 67-73. Solove, Daniel J. "Privacy self-management and the consent dilemma." Harvard Law Review Vol.126: 1880, 2013.
18 Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, WP187, 13 July 2011

solely on such agreement ('consent') is not legitimate. This is an issue that the GDPR aims to tackle, as is discussed later in this Working Paper.

3.2 Other grounds of processing of art. 7 95/46 Directive

The grounds 7(b) to 7(e) of the Data Protection Directive all require a necessity test, performed by the data controller. The Directive allows for processing of personal data only if processing is necessary either for the performance of a contract, or the compliance of the controller with a legal obligation, or the protection of the vital interests of the data subject, of for public interest. The necessity test is inevitably performed initially from the data controller himself, prior to the processing of the personal data.[19] Nevertheless, the decision of the controller to process personal data on the basis of the outcome of the necessity test is subject to administrative control from the supervisory (data protection) authority and judicial control from the competent courts. If the outcome of the necessity test is negative – this is that processing is not necessary – then there is no legal interest of the authorities to check the decision. However, if the outcome of the necessity test is positive, and the controller will start processing personal data, the lawfulness of processing is subject to control, as well as the ground(s) of lawfulness, and the decision (including the rationale) of the controller that justify that the conditions of the ground are fulfilled. The Directive left it to the national legislation of each Member State, to determine the meaning of the concepts of 'public interest', 'essential interest for data subject's life'. For instance, with regard to the concept of 'important public interest' some countries required approval by an ethics committee (e.g. Sweden), while others did not (e.g. Germany, Finland).[20] Such flexibility which apparently aimed to embrace the diversity of legal standards in the legislature of the EU Member States, led to non-harmonised results. The non-harmonised approaches in turn led to compliance difficulties for data controllers operating in more than one EU Member States. This is a difficulty that is expected to be overcome with the directly applicable GDPR[21].

3.3 Legitimate Interest of the controller in art. 7(f) of the Directive

The last ground of art. 7 is the legitimate interest of the controller or third parties. Art. 7(f) provides[22]:

> (f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

19 Bygrave, Lee A., and Dag Wiese Schartum. "Consent, proportionality and collective power." In Gutwirth Serge, Yves Poullet, Paul de Hert, Cécile de Terwangne and Sjaak Nouwt (eds.) Reinventing Data Protection? pp. 157-173. Springer Netherlands, 2009.

20 Korff, Douwe, "EC Study on Implementation of Data Protection Directive 95/46/EC", 2002, https://ssrn.com/abstract=1287667 (accessed 10 September 2016)

21 Article 288 of the Treaty on the Functioning of the EU European Union, OJ C 326, 26.10.2012

22 Art. 7(f) Directive 95/46/EC. The elements of the provision are further elaborated in the section on the General Data Protection Regulation.

The provision was amended several times during the legislative process, but did not substantially differ from one another. The first proposal,[23] the amended proposal[24] and the final text of art. 7(f) all included the condition that the legitimate interest of the controller is a ground for lawful processing if the interests of the data subject did not prevail. Thus, all versions included what is often called as a 'balancing' test between the legitimate interests of the data controller and the interests of the data subjects.[25] The final text of art. 7(f) Directive specified further the two sides of the balancing test: on the one hand, there was the legitimate interest(s) pursued by either the controller or a third party and on the other hand the interests for fundamental rights and freedoms of the data subject under art. 1(1) of the Data Protection Directive. However, the provision does not provide pointers or criteria on how to perform the balancing.

3.4 Criticism

The Directive entrusted the EU Member States with the task of specifying conditions for the balancing test. As it was shown in the Report concerning the implementation of the Directive, published in 2003 in line with art. 33 of the Directive, the implementation of art. 7 into national legislation was unsatisfactory and showed divergences. [26] Ferretti highlights that a loose application of the legitimate interest ground provision could lead to uncertainty and potentially be a 'tool for circumvention' of the legal protection offered to individuals.[27]

Apart from the diversity in the implementation of the provision in the national legislatures of the Member States, the legitimate interest ground has often been characterised as a 'loophole' in the protection of personal data.[28] Balboni et al. pinpoint the subjectivity of the data controller judgement as a key issue in that respect. [29] Moreover, another issue is that one cannot verify if the balancing test actually took place only, unless this is challenged in court.[30]

Criticism targets also the lack of useful guidance in the Directive for the interpretation of the legitimate interest of the controller.[31] This point is regularly made for provisions of principles-based legislation that are not descriptive enough. In the case of the legitimate interest, indeed some pointers or criteria as to when data subjects' rights override the legitimate interests are missing in the Directive. As we see further in this contribution, the GDPR introduces new concepts such as the reasonable expectations of the data subject and provides examples of legitimate interests in the Recitals with the aim to address the criticism.

23 Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM (1990) 314-2, 1990/0287/COD

24 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 ('Amended Proposal'), Mark Powell, 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 (92/C 311/04) COM (92) 422 final — syn 287, Computer Law & Security Review, Volume 10, 1994, pp. 43-46, ISSN 0267-3649, http://dx.doi.org/10.1016/0267-3649(94)90138-4.

25 The balancing even though included as a term in the provision of art. 7(f) stems from the Recital 30 of Directive 95/46/EC provides ("in order to maintain a balance between the interests involved while guaranteeing effective competition").

26 Commission of the European Communities, Report from the Commission. First Report on the Implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 final, Further on the implementation of the Directive: Poullet, Yves "EU data protection policy. The Directive 95/46/EC: Ten years after" Computer Law & Security Review, Volume 22, Issue 3, 2006, pp. 206-217, ISSN 0267-3649, http://dx.doi.org/10.1016/j.clsr.2006.03.004 (accessed 15 September 2016)

27 Ferretti, Federico "Data Protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights?" Common Law Market Review 51, 2014, pp. 843-868

28 Bits of Freedom "A loophole in data processing. Why the 'legitimate interests' test fails to protect the interests of users and the Regulation needs to be amended" 11 December 2012, https://www.bof.nl/live/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf, (accessed 10 August 2016)

29 Balboni, Paolo, Daniel Cooper, Rosario Imperiali, and Milda Macenaite "Legitimate interest of the data controller. New data protection paradigm: legitimacy grounded on appropriate protection." International Data Privacy Law 2013: ipt019, p.247f

30 Bits of Freedom (2012), section 4

31 Balboni, Paolo et al. (2013) p.247

4. Legitimate controller's interest in the 2016 General Data Protection Regulation

4.1 Preparatory works: Commission, EP, Council versions of art.6 (1) (f)

The Commission proposal (2012)[32] introduced the legitimate interest of the controller ground with a substantial differentiation from the Directive and the final version of the provision. The EC proposal simply excluded the legitimate interests of third parties from the scope of art. 6(1) (f). In addition, as with many provisions in the 2012 proposal, the Commission would be empowered to adopt delegated acts for the purpose of further specifying the conditions of the legitimate interest ground for various sectors and data processing situations, including as regards the processing of personal data related to a child.[33] Despite such a guidance would be useful, the choice of the Commission as a competent body and the means of delegated acts, was criticised for several reasons.[34] One argument was that the vital decisions for the interpretation of the ground should not be left to an executive body, with limited competence for such task. Instead the role of the WP29 in interpreting and providing guidance on the Directive could be continued by the European Data Protection Board in the GDPR.[35]

The European Parliament (EP) First Reading[36] reinstated the legitimate interest of the third party in the provision of art. 6(1) (f). The EP added a condition to the legitimate interest of the controller ground. This is the reasonable expectation of the data subject based on the relationship with the controller.[37] The EP also proposed the deletion of the provision on delegated acts of the Commission. An interesting proposed amendment of the EP was made regarding the processing of pseudonymous data. The Parliament suggested that the processing of such data should be presumed to meet the reasonable expectations of the data subject.[38] However, the WP29 strongly recommended omitting this phrase from the GDPR, as it could 'give rise to misinterpretation and could be understood as an exemption to the obligation of the controller to carry out the balancing test'.[39]

A discussion that emerged during the preparatory works of the GDPR revolved around the inclusion (or not) of an exhaustive list of acceptable legitimate interests. The Report of the Committee on Civil Liberties, Justice and Home Affairs to the European Parliament in 2012 ('Albrecht report') included such a list

32 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM (2012) 11 final – 2012/0011 (COD), 25.01.2012

33 Art. 6(5) Proposal for a GPDR (2012)

34 Kuner doubted the feasibility of such prior guidance from the Commission due to the complexity of the issue and the dependence on the particular facts of each case. Kuner C. (2012)

35 Rauhofer, Judith "One Step Forward, Two Steps Back? Critical observations on the proposed reform of the EU data protection framework." Journal of Law and Economic Regulation 6, no. 1, 2013, pp. 57-84.

36 European Parliament (2014) Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (COM(2012)0011 – C70025/2012 – 2012/0011(COD))

37 The concept of 'reasonable expectations' is further discussed later in section 5.3 of this Working Paper.

38 Recital 38 European Parliament First Reading (2014)

39 Article 29 Data Protection Working Party, Working Party Comments to the vote of 21 October 2013 by the European Parliament's LIBE Committee, Annex to letter to Greek Presidency, 11 December 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131211_annex_letter_to_greek_presidency_wp29_comments_outcome_vote_libe_final_en_.pdf, (accessed 10 June 2016)

in art. 6 (1) (b).[40] The article provided a list of cases when a legitimate interest of a controller overrides the interests, fundamental rights and freedoms of the data subject as a rule. Proposed cases included in the list were processing of personal data taking place as part of the exercise of the right to freedom of expression, the media and the arts.[41] However, such a solution was not embraced by neither the regulators nor the industry as it would involve the risk of being 'misleading' and 'unnecessarily prescriptive'.[42] The industry advised against such a restrictive list arguing that it would not anticipate the trajectory of new technologies and business models.[43] The Council First Reading is very close to the final version, which we discuss in the following section.[44]

4.2 Lawful processing grounds under art. 6 GDPR

While a detailed analysis of the grounds of legitimate processing is beyond the scope of this Working Paper, it suffices to mention that the GDPR kept almost intact the list of criteria for lawful processing as we know if from the Directive. The new listing of grounds is contained in art. 6 of the Regulation: consent (art. 6(1)(a)), performance of a contract (art. 6(1)(b)), legal obligation of the controller (art. 6(1)(c), vital interests (art.6(1)(d)), performance of a task carried out in the public interest (art. 6(1)(e)) and the legitimate interest of the controller (6(1)(f)) synthesise the exhaustive list of grounds for lawful processing of personal data. A new addition is article 7 GDPR, the conditions for consent. As a general comment, despite the broad criticism on over-relying on consent as a legal ground, the EU regulator chose to emphasise the consent ground with a separate provision. This choice of further specification of the consent ground is on the one hand partly justified by the wide discussions on the conditions for a valid consent (see above). On the other hand, it instigates the risk of being misinterpreted as a prioritisation of consent over the other grounds of art. 6 GDPR.

4.3 Framing the balancing act of art. 6(1) (f) GDPR

The final version of the legitimate interest of the controller ground in the Regulation 679/2016 is mostly based on the Directive provision (art.7 (f)). Two novelties are introduced regarding children's personal data, which merit attention from the side of the controller, and the public authorities, which cannot ground their data processing operation on art. 6(1) (f). The provision art. 6(f) GDPR reads:

> "(f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." [45]

40 Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf (accessed 10 June 2016)

41 Other cases provided in the article were the processing of personal data necessary for the enforcement of the legal claims of the data controller (art. 6(1)(b)(b)), the personal data would be provided by the data subject and the personal data would be used for direct marketing for its own and similar products and services (art. 6(1)(b)(c)), the processing in the context of professional business-to-business relationships (art. 6(1)(b)(d)), and when processing would be necessary for registered non-profit associations, foundations, and charities for the purpose of collecting donations (art. 6(1)(b)(e)).

42 Article 29 Data Protection Working Party, WP217, p. 12

43 International Chambers of Commerce, "ICC Position on Legitimate Interests", ETD/STM, 28 October 2015, http://www.iccgermany.de/fileadmin/user_upload/Content/Digitale_Wirtschaft/373-537legitimateint11-2015.pdf (accessed 25 September 2016)

44 European Council (2015) Preparation of a general approach. 9565/15, 11.6.2015, adopted at JHA Council Meeting on 15.6.2015

45 Art. (1)(f) GDPR

In comparison to the provision of art. 7(f) of the Directive 95/46/EC, art. 6(1) (f) does not have many new elements to offer. The wording was improved in several instances.[46] One significant differentiation is the de-linking of the scope of the data subjects' interests, rights and freedoms that should not be overridden, from the material scope of the legal instrument. The legitimate interest of the controller provision (art. 7(f)) of the 95/46/EC Directive referred explicitly to art. 1(1) of the Directive,[47] thus linked the scope of the data subject interests, rights and freedoms to scope of the Directive. The GDPR provision of art. 6(1) (f) drops the reference to the subject matter and refers to 'interests or fundamental rights and freedoms of the data subject which require protection of personal data'. The change in the wording can be considered as broadening of the scope. Any interests, rights and freedoms that merit protection of personal data should be assessed by the controller when considering the legitimate interest ground for its processing activities.

4.3.1 Step one - legitimacy

One of the first questions arising from the legitimate interest ground, also relevant to the different theoretical approaches to the balancing doctrine,[48] is the choice of the legislator of balancing between disparate interests: interests of the controller or a third party on the one hand and rights and freedoms of the data subject on the other. In principle, the disparity leads to the general rule that data subject rights override in principle the legitimate interests of the controller.[49] However, the ground of art. 7(f) implies that a legitimate interest pursued by a controller or a third party can prevail over rights and freedoms of the data subject.

Regarding the interests of the data subject, the WP29 opines that the omission of the word 'legitimate' is intentionally broadening the scope of the data subjects' interests that need to be balanced, so as to include even illegitimate interests of the data subject. The WP29 provides the example of an individual who has committed theft in a supermarket and his interest to have his picture not disclosed in the Internet by the owner of the shop. However, this example does not directly respond to the argument made by the WP29, as the interest of the data subject in this case is still legitimate. The right to protection of personal data is not automatically abolished once the individual has committed an illegal act, theft in this case. Nevertheless, the argument on the illegitimate interests of the data subject is still valid.

The very choice of 'legitimate'[50] instead of legal interest of the controller is also interesting. A legal interest would be an interest stemming from a legal instrument, reflecting the 'aggregate of the legal relations of a person with respect to some specific physical object or the physical relations of specific objects'.[51] A legitimate interest on the other hand, might not be specifically foreseen in a legal instrument, but in any case has to be in accordance with the law, in the sense that it does not violate the law.[52] As such, the legitimate interest of the controller can be a fundamental right established in the Charter of Fundamental

46 'Legitimate interest' is now 'legitimate interests' in art. 6(1) (f) GDPR, 'overridden by the interests for fundamental rights and freedoms' of the Directive is now 'overridden by the interests or the fundamental rights and freedoms'. The last amendment was also highlighted by the WP29 in its Legitimate Interest opinion. The WP29 indicated that the wording of the Directive was a misspelling ('or' instead of 'for').

47 Article 1(1) Directive 95/46/EC read: 'In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.'

48 See discussion in section 2 of this Working Paper.

49 Case C-131/12 Google Spain and Google, EU:C:2014:317, paragraph 81

50 The choice of the word 'legitimate' interest instead of conflicting rights has been discussed by Ferretti, who interprets the 'legitimate interest' as meaning a legally protected interest. Ferretti Federico (2014)

51 Corbin, Arthur "Legal Analysis and Terminology" 29 Yale L.J. 163 1919-1920, p.173

52 By 'law' here is meant 'any law', not only the data protection law.

Rights, a legal right provided in a Union or national law, or it can be any other interest pursued by the controller (including commercial), as long as it is in line with the law. The nature of the source of the interest of the controller is not important to determine its legitimacy. It does however play a role in the balancing test against the interests, rights or freedoms of the data subject, as we discuss later. The Article 29 Data Protection Working Party (WP29) proposes two conditions for the legitimacy of the interest of the controller. It must represent a real and present interest, and it has to be sufficiently clearly articulated.[53] As it is often in civil law, legal claims have to be real and present. Especially when the interest overrides rights of another party. According to this interpretation of the WP29, a future interest, an interest depending on the fulfilment of a condition or an expectation for an interest is not sufficient under art. 6(1) (f). The broad scope of the concept of legitimate interest of the controller, invites a spectrum of different interests under the legitimate interest ground, as are further discussed in this Working Paper.[54]

4.3.2 Third parties

The provision of 6(1)(f) GDPR retains the same terminology as regards the legitimate interest pursued by the controller or by a third party. The Directive included the phrase 'by the third party or parties to whom the data are disclosed', but this phrase ('to whom the data are disclosed') is redundant due to the definition for 'third parties' in art. 4 (10). A third party in the GDPR is a natural or legal person, public authority, agency or body, other than "the data subject, controller, processor, and persons who under the direct authority of the controller or processor" is authorised to process personal data. The term is not far from the way it is used in civil law, that is a person which is not party to an agreement.[55] The GDPR explicitly provides that the third party has to be other than the data controller, processor, data subject, and the persons under the direct authority of the controller or processor. In the data protection context, the third party is not part of the relationship data controller – data subject, nor of the relationship data processor-data subject. In practice, it will be challenging to determine who is a third party. The third party would need to be processing data not on behalf of the controller (as it would then be a processor), nor have its own personal data be processed (as it would then be a data subject), but would however need to pursue a legitimate interest to process the personal data of the data subject. The legitimate interest of the third party is distinct from the legitimate interest of the controller (although they both can constitute a ground for lawful processing). Thus, the third party, needs to have its own separate legitimate interest to process the personal data. This is problematic, as once the 'third party' pursues its own interests to process the data, and is granted access to the data, it will then most likely qualify as a data controller on its own right (provided that the other conditions for the controllership are met). With the definition of the third party included in art. 4 GDPR, the list of potential third parties is shortened due to the broad list of actors that are exempted from the definition of 'third party'. Taking the example of cloud computing environment, searching for possible actors to qualify as third parties could be troublesome. Broader categories such as the Internet users would be perhaps qualify as third parties in that case, but crystallising a legitimate interest pursued by such a broadly defined third party could be problematic.[56] Another actor that could qualify as a third party could be a person that has legal claims against the data subject, and needs therefore to process personal data

53 Article 29 Data Protection Working Party "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" WP217, April 2014
54 See section 8 of this Working Paper.
55 Article 29 Data Protection Working Party "Opinion 1/2010 on the concepts of 'controller' and 'processor'" WP169, 2010, p.33f
56 The WP29 assesses the interests of a wider community in the balancing test by including them under the legitimate interest of the controller together with any business or other interest of the controller itself. WP217, p. 35

of the data subject in order to proceed with its legal claims.[57] It is recommended therefore to interpret the provision regarding the third party strictly, as in principle, any third party receiving personal data would be considered a data controller or processor.[58]

4.3.3 Step two – necessity

Necessity is part of all the grounds of art. 6(1) GDPR, apart from consent.[59] As in the Directive,[60] the legitimacy of the interest pursued by the controller does not suffice for the ground of art. 6(10(f) GDPR to be fulfilled. The processing also needs to be necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Necessary in this case means that processing of personal data is the least restrictive measure to the rights of the data subjects. If there is another way of meeting the legitimate interest pursued by the controller or the third party, that interferes less with the right to protection of personal data of the individuals, then the processing is not necessary.[61] The European Data Protection Supervisor, in a recent background policy paper providing a 'toolkit' for assessing the necessity of a (legislative) measure, characterised the concept of necessity in data protection law as a 'facts-based' concept.[62] Indeed, whether a processing operation is necessary highly depends on the facts of the specific case under examination. But external boundaries to what is necessary in each case are to be set by the principles relating to processing of personal data, provided in art. 5 GDPR, such as lawfulness, fairness, data minimisation, integrity.

4.3.4 Step three - Balancing test

Art. 6(1)(f) involves the obligation to weigh the legitimate interests of the controller on the one hand and the interests, rights and freedoms of the data subject on the other in order to determine in each specific case whether the data subject rights override the legitimate interest of the controller or the third party ('balancing test'). Many elements should be considered in this balancing test. That is elements that can affect the outcome to the one or the other side. The nature of the data is one such element (sensitive, open, public, etc.). Another element relates to the power and status of the two parties (controller or third party and data subject).[63] An employer intending to process the personal data of an employee is in a relatively stronger position than the employee. The source of the legitimate interest of the controller or the third party is also significant. An interest stemming from a fundamental right established in the Charter of Fundamental Rights such as the freedom of expression has different weight than a commercial interest to attract customers through targeted advertising.[64] Other issues include the purpose of processing and the impact of the processing.

57 Case Rigas Satiksme case: suing the data subject for property damages is a legitimate interest, p. 18
58 Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor', WP169, 2010, p.33f
59 Art. 6(1)(a) GDPR
60 See section 3 in this Working Paper
61 ICO "Big Data and Data Protection" version 1.0, 2014, paragraph 64 p. 20, https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf (accessed 10 September 2016)
62 European Data Protection Supervisor "Developing a 'toolkit' for assessing the necessity of measures that interfere with fundamental rights, Background paper", June 2016, p. 8
63 Article 29 Data Protection Working Party (2014)
64 See for instance the Opinion of the Advocate General in CJEU Google Spain and Google case, section 7.2 of this Working Paper.

5. Further clarifications on the balancing test

5.1 Impact assessment

A crucial element of the balancing is the assessment of the impact of the processing operation at stake to the interests, rights and freedoms of the data subject. The impact should be understood as including both benefits and risks to the individual stemming from the processing operation. Risk assessment is not unusual to data and information security. Several methodologies exist for identification, classification, determination of severity of risks and recommendation of mitigation measures. OWASP,[65] a non-for profit organisation working on open source software projects, has proposed a methodology of five main steps, starting from risk identification, estimation of likelihood and impact,[66] determination of the severity of risk and prioritisation of risks for mitigation. Standardisation bodies have also developed standards and guidelines on risk management. For instance, NIST, the US Institute for Standards and Technology has proposed a privacy risk management framework, which includes a Privacy Risk Assessment Methodology.[67] ISO has published the ISO 31000 on risk management, but also the ISO/IEC 27005 which is specific to information security risk management.[68] While existing risk assessment methodologies could be useful for the balancing of the legitimate interest ground, assessing 'benefits' and positive impact is challenging. First, due to subjectivity involved in such a benefit analysis and second due to the nature of impact on rights and freedoms of individuals.

Bennett and Bayley argue that the legitimate interest ground is structured by a context in which there is 'pro-active assessment of risk' and demonstration of accountability.[69] Although as we said, the assessment goes further than just a risk assessment, the argument on demonstration of accountability is important. Indeed, in the framework of accountability principle of art. 5(2) GDPR, the concept of legitimate interest is seen as a continuous exercise for the controller to demonstrate the prevailing of his interest over the interests, rights and freedoms of the data subject. This is different from the Data Protection Directive, where accountability of the controller was implied. With the introduction of the accountability principle and the element of demonstration, the controller needs to document the decision (and its justification) to rely on the legitimate interest ground not only at the moment of the decision, but as long as he grounds the processing on the legitimate interest.

5.2 What should be the weight of mitigation measures in the balancing test?

There can be two approaches to the balancing test under art. 6(1) (f). A stricto sensu balancing test responds to the literal interpretation of the provision. Such a test would omit including in the balancing test as self-standing criteria, any mitigation measures and safeguards, such as organisational or technical

65 Website of OWASP, https://www.owasp.org/index.php/About_OWASP (accessed 18 September 2016)
66 According to OWASP methodology, this stage includes both technical impact factors such as loss of confidentiality, availability, integrity, availability and accountability, and business impact factors, such as financial damage, loss of reputation and others.
67 NIST, 'Privacy Risk Management for Federal Information Systems', NISTIR 8062 draft, http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf, (accessed 18 September 2016)
68 ISO 31000:2009 Risk Management-Principles and guidelines, ISO/IEC 27005:2011, Information technology -Security techniques - Information security risk management
69 Bennett Colin J. and Robin M. Bayley "Privacy Protection in the era of 'big data': regulatory challenges and social assessments" in Bart van der Sloot, Dennis Broeders & Erik Schrijvers (eds.) Exploring the Boundaries of Big Data, Amsterdam University Press 2016

measures, taken by the controller for the protection of the data subject rights. The rationale for this approach is simple. The ground of art. 6(1)(f) asks for a balancing test between two values, the legitimate interests of the controller (or a third party) and the interests, rights and freedoms of the data subject, and the mitigation measures are not inherent to any of those values. As discussed above, an interest lies with a controller when he has a present and real need to process personal data. By definition, a legitimate interest does not include mitigation measures and safeguards to reduce its adverse impacts. An argument in favour of adopting this approach is that making 'safeguards' part of the test would unfairly influence the assessment in favour of the legitimate interest of the controller. Any scheduled safeguards and mitigation measures would most likely weigh in favour of the controller and 'at the expense' of the data subject interests, rights and freedoms, by softening the impact and consequences of the interference. In case the legitimate interest of the controller prevails, the controller still needs to take safeguards to protect the data subjects' rights, on the basis of mainly art. 5, 13 and 21 GDPR. Prevailing should in no case be interpreted as abolishing.

Another approach is the one proposed by the WP29. The balancing would include mitigation measures to prevent undue impact, such as use of anonymization techniques and privacy enhancing technologies (PETs).[70]

From a teleological perspective, the WP29 approach fits better with the aim of the protection of the right, not to look at concepts bare from their context, but adopt a more pragmatic approach and investigate the protection and impact on the data subject rights. Thus, including mitigation measures in the assessment would lead to a representation of the actual expected impact of the processing to the data subjects' rights, and would still allow the legitimate interests to prevail. This approach does not 'punish' the controller that takes mitigation measures and safeguards, by not including them in the balancing test. On the contrary it encourages the controller to do so. On the other hand, one should keep in mind that the weight of future safeguards and mitigation measures is always relevant to their realisation and effectiveness. Such measures therefore should be considered, but not play a significant role in determining to which side the scale leans.

5.3 Reasonable expectations of the data subject

A new concept in the GDPR is the reasonable expectations of the data subjects based on the relationship with the controller.[71] The concept of reasonable expectations is known in other fields of law,[72] and in the case law of the European Court of Human Rights (ECtHR) on the art. 8 of the European Convention of Human Rights (ECHR).[73] The introduction of the concept was in general received positively from data protection advocates,[74] even though not without exceptions.[75]

70 Article 29 Data Protection Working Party (2014)

71 Recital 47 GDPR

72 The 'reasonable expectations' criterion in GDPR could be compared to the 'reasonable expectations' doctrine in other fields of law such as consumer protection law, contract law, insurance law and administration law. See Girot, Clarisse, User protection in IT contracts: A comparative study of the protection of the user against defective performance in information technology. Vol. 11. Kluwer Law International, 2001. Also, CJEU, Judgment of the Court of First Instance 8 May 2007, Citymo v Commission, Case T271/04, EU:T:2007:128

73 See for instance European Court of Human Rights, Judgement of 24 June 2004, von Hannover v Germany

74 Davies, S. "The Data Protection Regulation: A Triumph of Pragmatism over Principle?" European Data Protection Law Review, Volume 2, Issue 3, 2016, pp. 290 – 296.

75 See Cuijpers, Colette et al. who relate the 'reasonable expectations' criterion in the GDPR to the criticism attached to the reasonable expectations test in the US Informational Privacy literature and argue that "the legal protection is conditioned by people's expectations of privacy, but these expectations are significantly formed by the legal protection" Cuijpers, C.M.K.C., Nadeszda Purtova, N.N. and Eleni Kosta "Data protection reform and the internet: the draft Data Protection Regulation" in A Savin & J Trzaskowski (eds.), Research Handbook on EU Internet Law, Edward Elgar 2014, pp. 543-568,

Even though included only in a recital of the final text of the GDPR, the reasonable expectations criterion will be a significant element of the balancing test. According to this criterion, the controller would need to assess whether the data subject reasonably expects the collection of the personal data at the time and the context of the collection for the specific purpose.[76] The example of a client-provider relationship stands out in that respect. When an individual orders online a product, he would expect that the service provider would process his personal data. The controller pursues the interest to conduct business[77] and carry out the product order.[78] A reasonable expectation relates strongly to the circumstances before the processing takes place, including the provision of clear and timely information to the data subject. A reasonable expectation of processing therefore relates to the foreseeability and acceptance from the side of the data subject of the processing operation. While the foreseeability needs to be articulated objectively (clear, timely, and transparent information notice, justified for the purposes it serves, etc.) by the data controller, the acceptance of the data subject can also be implied (otherwise, we would refer to 'consent'). Scholars raise a flag of overlying on reasonable expectations; what is reasonable might be influenced by previous (not necessarily fair) practices of dominant players in a field.[79]

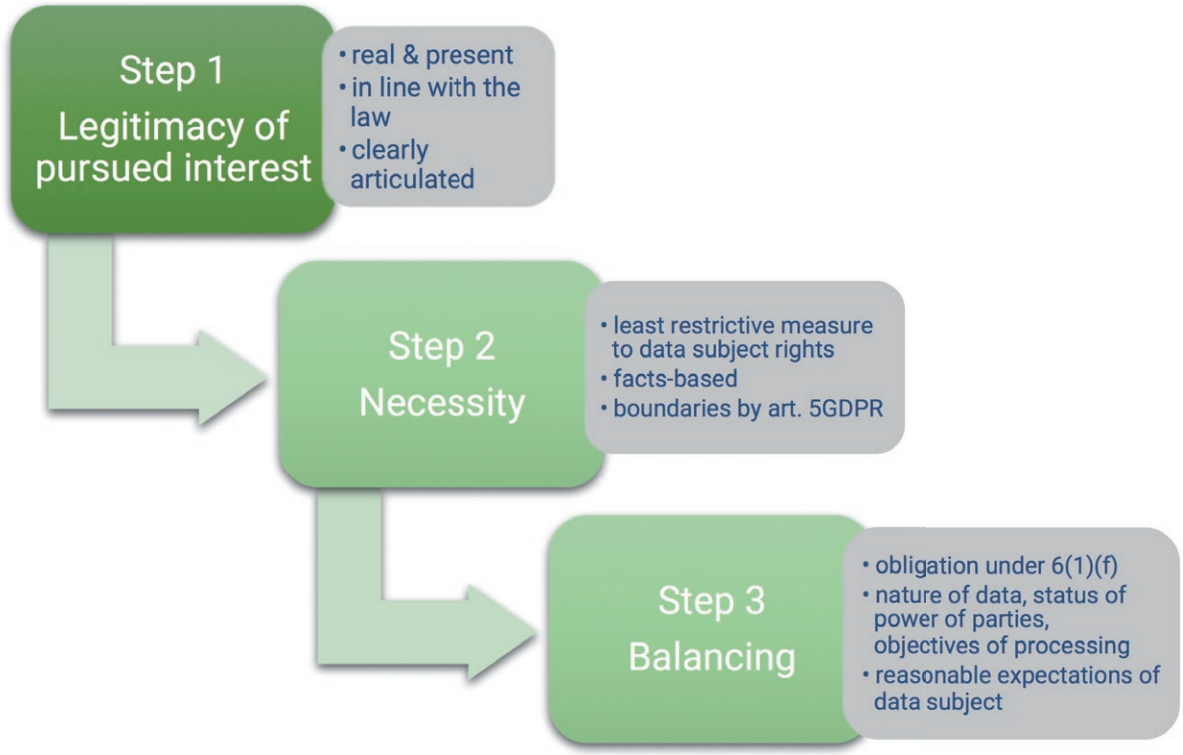

Figure 1: Conceptualisation of the balancing act framework of art. 6(1) (f) GDPR

76 Recital 47 GDPR

77 Article 16 of Charter of Fundamental Rights EU provides "The freedom to conduct a business in accordance with Union law and national laws and practices is recognised."

78 In Google Spain and Google case, the Advocate General recognised the fundamental right to conduct business, established in art. 16 Charter of Fundamental Rights, as within the meaning of legitimate interests of Article 7(f) of the Directive. The AG opined that "an internet search engine service provider lawfully exercises both his freedom to conduct business and freedom of expression when he makes available internet information location tools relying on a search engine."

79 Zingales argues that "consumers tend to recognize the rules and policies adopted by the dominant players as part of the general cultural and societal expectation". Arguably, this could lead, according to Zingales, to contractual practices being used as a shield against certain contractual obligations used in the market. Zingales N. "Unreasonable v. Unfair Data Processing: Contrasting Two Rising Modes of Protection Against Over-reaching Terms of Service", unpublished paper presented in Amsterdam Privacy Conference 2015.

6. Understanding the legitimate interest ground in the wider context of the GDPR

6.1 The right to access and the right to object

If processing takes place based on the legitimate interest of the controller or a third party, the GDPR provides the data subject with safeguards, aiming to counteract the interference with the data subject's interests, rights, and freedoms. Article 13 GDPR which concerns the information to be provided where personal data are collected from the data subject and art. 14 concerning the information to be provided where personal data have not been obtained from the data subject, establish the obligation of the controller to inform the data subject that the processing is based on the ground of art. 6(1) (f), the legitimate interests pursued by the controller or a by a third party.[80] This is an additional obligation to the disclosure of the legal basis of processing.[81] The controller needs to inform the data subject on which are the legitimate interests that the controller or the third party pursues and prevail over the rights of the data subject. De Hert and Papakonstantinou draw attention to the exception to the information obligation of the controller in the cases that 'the data subject already has the information',[82] as such broad exemptions could render in practice the right to information irrelevant.[83] The provision of this information is a prerequisite for the exercise of the right to object.

The right to object to processing based on the legitimate interest of the controller (or a third party) is established in art. 21 GDPR. This is not a new provision in the EU data protection law.[84] What is new is the reversal of burden of proof. In art. 14 of the Data Protection Directive, the data subject could object on compelling legitimate grounds and the controller would stop processing those personal data if the objection would be justified. Art. 21(1) GDPR provides:

> "The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims"[85]

Once the data subject objects, the controller is obliged to stop processing the personal data, unless the controller demonstrates compelling grounds for processing. The data subject's right to have his personal data not processed based on the legitimate interest of the controller is granted ab initio.[86] The compelling grounds provided by the controller need to override the interests, rights and freedoms of the data subject or to be important for legal claims. A new element in the legislation is the use of personal data for legal claims.[87] If interpreted broadly, the 'legal claims' term could include a broad range of cases, and could leave room for misuse, or even abuse by data controllers in bad faith. It should be accepted, that such legal claims should stem from the relationship of the controller with the data subject. There should also

80 Art. 13(1) (d) and art. 14(2) (b) GDPR.
81 Art. 13(1) (c) and art. 14(1)(c)
82 Art. 13(4) and 14(5) GDPR
83 De Hert Paul, Vagelis Papakonstantinou "The new General Data Protection Regulation: Still a sound system for the protection of individuals?", Computer Law & Security Review, vol. 32, 2016, pp. 179-194
84 Art. 21 GDPR corresponds to art. 14 Directive 95/46/EC.
85 Art. 21(1) GDPR
86 Rauhofer (2013)
87 It is not new in the case law however. See I. v Finland, despite the parties had reverse roles: the data subject wanted access to her personal data to support her legal claims against the controller. European Court of Human Rights, Case of I v. Finland (Application no. 20511/03), Strasbourg, 17 July 2008, Final 17-10-2008

be a strong causal link of the claim with the personal data at stake. This means that the legal claim cannot be otherwise established, exercised or defended unless the objected processing of personal data takes place ('compelling'). Both rights to information and to object are granted along the other data subject rights (access, restriction of processing, erasure, etc.). Data protection principles of art. 5 GDPR and the accountability principle constitute a framework of safeguards for the data subject.

6.2 Processing of sensitive data and further processing on the ground of legitimate interest

The provision on processing of special categories of data is enriched in the GDPR with the introduction of genetic and biometric data, as distinct categories from the data concerning health. Although the legitimate interest of the controller is not as such a ground constituting an exception to the general prohibition of processing of sensitive personal data in art. 9(1), elements of the legitimate interest ground can be identified in two of the grounds of art. 9(2) GDPR. First, there is the 'legitimate activities' by a non-for-profit body ground.[88] The legitimate activities is closely linked to the legitimate interest of art.6 (1) (f) ground, but it has more limited scope ('activities' instead of 'interests') and is conditioned on appropriate safeguards, the type of the controller (non-for-profit body), the aim of activity of the controller ('political, philosophical, religious or trade union') and the relationship of the data subjects with the controller (members, former members or persons with regular contact with the controller). The other ground of art.9 is the ground of establishment, exercise or defence of legal claims.[89] The legal claims usually fall within the legitimate interest of a controller (as is also obvious in the right to object provision), although it also includes not only claims of the controller, but also of the data subject.[90] The careful and limited introduction of elements of the legitimate interest of the controller ground in the processing of sensitive data confirms the aim of the GDPR to impose a stricter regime to the processing of such data and offers a good example for comparison with the broader and more flexible conditions of art. 6(1) (f)[91]

Regarding further processing, the GDPR makes use of the criterion of reasonable expectations of the data subject also in the case of further processing.[92] If the data subject, does not reasonably expect the further processing given the circumstances of each case, then further processing is not allowed with the original legal ground for processing. A critical issue is what can be considered as 'compatible' with the original purposes. Apart from the criterion of 'reasonable expectations' other criteria can also help the controller determine the compatibility of original with further processing purposes. Any links between the purposes, the context in which the personal data have been collected, the nature of the personal data, the consequences to the data subjects and the existence of safeguards in both original and further (intended) processing.[93] The controller needs therefore to conduct comprehensive compatibility and impact assessment before engaging in any further processing. The GDPR regards the indication and transmission of criminal acts or threats to public security in individual cases or in several cases relating to the same criminal act or threats to public security to as being in the legitimate interest pursued by the controller. It recognises however that often such disclosure of personal data could be incompatible with 'legal, professional or other binding obligation of secrecy' and thus includes an exception to the compatibility rule, when such obligations are involved and conflict with the processing.

88 Art. 9(2) (d) GDPR.
89 Art. 9(2) (f) GDPR.
90 See section 6 of this Working Paper
91 Even though the extension of the 'exceptions' list in comparison to art. 8 of the Directive 95/46/EC can be considered as achieving the opposite result.
92 Recitals 47 and 50 GDPR.
93 Article 6(4) GDPR and recital 50 GDPR.

6.3 Children and public authorities

Children are vulnerable to risks such as unwanted dissemination of their personal data on online social networks, targeted advertising,[94] but also to online and offline abuse, cyberbullying, and others. In line with the increased attention, the GDPR draws to the protection of children,[95] the provision of art. 6(1) (f) puts emphasis on the balancing when the data subject is a child ('in particular when the data subject is a child'). When the data subject is a child, this is an element that should weigh in the balancing test in favour of the interests, rights and freedoms of the data subject. The GDPR includes the condition on children only in the legitimate interest ground of art.6 and consent (art. 8). This heightened protection for children comes to outweigh the vulnerability of children as data subjects - in the form of information asymmetry, exercise of data subjects' rights to access, object etc. - as opposed to data controllers, that may be organisations and corporations such as online social networks and search engines. A practical difficulty for the controller in applying the special attention to the rights of the children, is that the age of the data subject, which is personal data, requires that the controller already engages into a processing operation, i.e. collection of the information, for which the controller already needs a legal ground.

Another novelty is the non-applicability of the legitimate interest of the controller ground to public authorities. The final text of the GDPR does not allow public authorities to use the legitimate interest ground for data processing activities in the performance of their tasks[96] Public authorities may however use the one of the other grounds for lawful processing of art. 6 GDPR.

7. Court of Justice of the EU: landmark cases, but few 'concrete' answers for legitimate interest ground

The role of the Court of Justice in interpreting EU data protection law has been of fundamental significance. Landmark cases such as the Digital Rights Ireland,[97] the Google Spain case[98] and the Schrems case[99] have elevated the role of the CJEU as gatekeeper of EU data protection law. Skouris, the former president of the Court, stated[100]:

> 'European justice is a fundamental guarantee for the application of the rule of law and democracy. But it is also a major factor of adjusting the legislative choices to ongoing societal changes. The institutional setup is such that calls for the European judge to make sure that legislative solutions adopted under given circumstances maintain their value even in view of novel phenomena.'

94 European Data Protection Supervisor "Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - "European Strategy for a Better Internet for Children", July 2012, https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-07-17_Better_Iternet_Children_EN.pdf, (accessed 25 September 2016)

95 Recital 38 and art. 8 GDPR. Results from Cookie Sweep of EU Data Protection Authorities and report on children online (in french): CNIL "Vie privée des enfants: une protection insuffisante sur les sites Internet", 2 September 2015, https://www.cnil.fr/fr/vie-privee-des-enfants-une-protection-insuffisante-sur-les-sites-internet-0, last accessed 25 September 2016. Read further about this issue and on the age for consent of children in Jasmontaite, Lina, and Paul De Hert "The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet" International Data Privacy Law 5, no. 1, 2015, pp. 20-33.

96 Art. 69(1) and Recital 47 GDPR. The Data Protection Directive 95/46/EC did not preclude public authorities from using the ground of legitimate interest of art. 7(f). In the case Manni, the Court of Justice EU found that the processing of personal data by an authority legally responsible to keep a register satisfies inter alia the ground of legitimate interest of the controller of Art. 7(f) Directive 95/46/EC, Case C-398/15, EU:C:2017:197

97 Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others, EU:C:2014:238

98 Case C-131/12 Google Spain and Google, EU:C:2014:317

99 Case C-362/14 Schrems, EU:C:2015:650

100 Vasilios Skouris, 'After 12 Years', Maastricht Journal of European and Comparative Law, 23 MJ 2, 2016

Despite the significance of the judgements in the data protection field, the CJEU did not have many occasions to interpret the ground of art. 7 (f) of the Data Protection Directive, and in the few occasions there was such an opportunity, it was not fully exploited. The CJEU missed for instance the opportunity to interpret the necessity condition of the ground in the ASNEF case. It provided some answers however in the recent Breyer case. The following cases are the most relevant jurisprudence with focus on the ground of legitimate interest. They are presented here aiming at exploring the stance of the CJEU on the matter under discussion.

7.1 ASNEF case: legitimate interest ground is **not strictly for personal data appearing in public sources**[101]

The CJEU was asked to issue a preliminary ruling referred by the Supreme Tribunal Court of Spain. The parties in the two joined cases were the Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and the Federación de Comercio Electrónico y Marketing Directo (FECEMD) against the Spanish state Administration. The references for preliminary ruling concerned the interpretation of Article 7(f) of Data Protection Directive.

7.1.1 Facts and preliminary questions

ASNEF and FECEMD brought administrative proceedings before the national courts of Spain complaining that the national legislation transposing the Data Protection Directive to the national law violated Art. 7(f) of the Directive. The argument of the plaintiffs was that the Spanish Royal Decree added conditions to the ground of Art. 7(f), in breach of the Data Protection Directive. The breach lied according to the plaintiffs on the condition that for the interest of the controller to be legitimate, the controller should process personal data which appear in public sources (files of the Spanish Organic law 15/1999).

The Supreme Court of Spain took the view that such restriction in the Spanish Decree is a barrier to the free movement of personal data, which is incompatible with the Data Protection Directive. Since the outcome of the cases depended to the interpretation of the Directive, the court referred two questions to the CJEU. The first question related to the interpretation of art. 7(f) as allowing the processing of personal data necessary to pursue a legitimate interest of the controller or of third parties when fundamental rights and freedoms are not being prejudiced, and the data to be processed appear in public sources. The second question referred to whether art. 7(f) of Data Protection Directive had direct effect.[102]

7.1.2 Ruling

The Court confirmed that the list of grounds for lawful processing of art. 7 Data Protection Directive is exhaustive and restrictive.[103] Member States therefore cannot include additional grounds or provide for additional requirements amending the scope of a principle of art.7. Guidance and national measures which provide a clarification of the ground are in line with the Directive. Regarding the content of the legitimate interest ground, the Court found two conditions that must cumulatively be fulfilled. The first is the necessity condition. The processing needs to be necessary for the legitimate interests of the controller or third

101 Joined Cases C-468/10 and C-469/10, ASNEF

102 The direct effect of EU law is a fundamental principle of EU law, which enables individuals to immediately invoke European law before courts, independent of whether national law exists http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l14547&from=EN (accessed 10 September 2016)

103 Joined Cases C-468/10 and C-469/10, para. 30

parties or parties to whom the data are disclosed. The second condition is that such legitimate interests must not be overridden by the fundamental rights and freedoms of the data subject.[104] The Court did not provide further interpretation of the 'necessity' condition. However, it provided further explanation of the second condition.

The Court noted the need for balancing between opposing rights and freedoms included in the second condition of art. 7(f). The ruling went further on to specify that the balancing depends in principle on the individual circumstances of each case. In the context of those individual circumstances, the person or the institution carrying out the balancing test should take account of the data subject's rights of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.[105] Here the Court included both the right for respect for private and family life and the right to protection of personal data in the scope of the balancing. The reason for the inclusion of both fundamental rights, as provided in the ruling, is the close connection of the right to respect for private life with the right of art. 8(1).[106] The fundamental rights of art. 7 and 8 of the Charter are not absolute rights. Interferences therefore with non-absolute rights can be allowed when the conditions of ar. 52 of the Charter are fulfilled. In the case under discussion, when referring to the limitations to the fundamental right to protection of personal data, the Court recalled art. 8(2) and art. 52(1). The Court therefore interpreted the balancing condition of art. 7(f) as depending on a case by case basis. The Court kept a reservation ('in principle') for this rule, without however further specifying exceptions. In relation to the elements of the balancing test, the Court said that it is possible to take into consideration the fact that the seriousness of the infringement can vary depending on whether the data in question already appear in public sources.
The Court replied to the first question that Article 7(f) of Directive 95/46 must be interpreted as precluding national rules to require not only that the fundamental rights and freedoms of the data subject be respected, but also that those data should appear in public sources, thereby excluding, in a categorical and generalised way, any processing of data not appearing in such sources.[107] In addition, the reply to the second preliminary question regarding the direct effect of the art. 7(f) of the Directive, the Court found that the art.7(f) has direct effect.

7.2 AEPD v. Google case: **the balancing tests depends in principle on individual circumstances**[108]

The Audiencia Nacional (Spanish national high court) requested a preliminary ruling concerning the application of the Directive 95/46/EC to Internet search engines and the right to be de-listed from the search results. The case was about a decision of AEPD, the Spanish Data Protection Authority, upholding a complaint of a Spanish citizen against Google Spain and Google Inc. and ordering Google Inc. to 'adopt the measures necessary to withdraw personal data relating to Mr Costeja González from its index and to

104 Joined Cases C-468/10 and C-469/10, para. 38
105 Article 7 Charter protects the right to respect for private and family life. Art. 8 establishes the right to protection of personal data.
106 In fact, the Court referred to 'the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter', citing the two distinct rights of art. 7 and art. 8 Charter as one. This is not new in the case law of the CJEU. Gonzalez Fuster discusses inconsistencies in the case law of the CJEU in separation and disentanglement of the rights of art. 7 and Art. 8 of the Charter. Fuster, Gloria Gonzàlez. "Fighting for Your Right to What Exactly-The Convoluted Case Law of the EU Court of Justice on Privacy and/Or Personal Data Protection." Birkbeck Law Review 2, 2014, p.263.
107 Joined Cases C-468/10 and C-469/10, para. 49
108 An extensive analysis of the judgement is not in the scope of this contribution. Read further Kuner Christopher, "The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges", in: Burkhard Hess and Cristina M. Mariottini (eds.), Protecting Privacy in Private International and Procedural Law and by Data Protection, Farnham, Surrey, UK England : Ashgate, 2015 pp. 19-55. De Hert, Paul, and Vagelis Papakonstantinou. "Google Spain: Addressing critiques and misunderstandings one year later." Maastricht Journal of European and Comparative Law 22, no. 4, 2015, pp. 624-638.

prevent access to the data in the future'. In short, the preliminary questions related to the interpretation of the territorial application of the Data Protection Directive, the activity of search engines as providers of content in relation to the Directive and the scope of the right to erasure.[109] The Advocate General (AG) in his Opinion recognised that the provision of Internet search engine services falls within the legitimate interests of the controller ground for lawful processing (art. 7(f) Directive). Further on the AG provided that this activity breaks down to three purposes:

> '(i) making information more easily accessible for internet users; (ii) rendering dissemination of the information uploaded on the internet more effective; and (iii) enabling various information society services supplied by the internet search engine service provider that are ancillary to the search engine, such as the provision of keyword advertising.'[110]

The AG related those purposes to freedom of the Internet users to receive information (art. 11 Charter), freedom of expression (art. 11 Charter) and freedom of the search engine service provider to conduct business (art. 16 Charter).

The judgement did not explicitly uphold the AG arguments on the legitimate interest of the Internet search engine providers. It limited the references to the legitimate interest ground of art. 7(f) to what was strictly necessary for the judgement. The Court referred to the two cumulative conditions of the legitimate interest ground and confirmed the requirement for a balancing test in the second condition ("except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject"). As in the ASNEF case, the Court provided that the balancing test depends, in principle, on the individual circumstances of each case, stressing at the same time the need to consider the data subject's rights of art. 7 and 8 Charter.[111]

7.3 RYNES case: protection of property, health, and life of family and the individual as legitimate interests [112]

The case concerned the interpretation of art. 3(2) of the Directive 95/46/EC, which is the so called 'household exemption'.[113] Rynes had installed a surveillance system at his home which recorded the entrance to his home, the public footpath and the entrance to the house opposite. In examining on whether the activity of Rynes fell under the exemption of art. 3(2), the Court of Justice EU also referred to the legitimate interest of the controller ground. The Court provided that the protection of the property, health and life of family and the individual (claimant himself) may constitute legitimate interests pursued by the controller.[114] The Court ruled that art. 3(2) of the Directive 95/46/EC must be interpreted as meaning that the activity of Rynes did not fall under the household exemption.[115] This case is interesting because despite it

109 C131/12, EU:C:2014:317
110 AG Opinion C131/12, EU:C: 2013:424 paragraph 95
111 C131/12 paragraph 40
112 C-212/13, EU:C:2014:2428
113 Art. 3(2) Directive 95/46/EC provides:
"*This Directive shall not apply to the processing of personal data:*
– by a natural person in the course of a purely personal or household activity".
114 Paragraph 34 C-212/13
115 The Court provided "the second indent of Article 3(2) of 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 must be interpreted as meaning that the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or household activity, for the purposes of that provision."

does not elaborate on the balancing test, it uses the legitimate interest ground to show that even when the Directive 95/46/EC applies (thus not under the household exemption), the interests of the controller are co-considered in the provisions of the law. The Court gave a broader role to the legitimate interest ground, the one of bringing the balance among conflicting interests and rights, and reminded us the relativity of the right to protection of personal data.

7.4 BREYER case: ensuring operability of online media services may constitute a legitimate interest

The German Federal Court of Justice requested a preliminary ruling on a case concerning a German citizen (Breyer) seeking a prohibitory injunction against the Federal Republic of Germany for storing IP addresses.[116] Breyer required the Federal Republic to refrain from storing, or arranging for third parties to store, the IP address of the host system from which he sought access, except when necessary to restore the availability of the telemedium in a case of a fault. The Advocate General in his Opinion delivered in May 2016 proposed:

> "Article 7(f) of Directive 95/46 must be interpreted as meaning that the objective of ensuring the functioning of a telemedium can, in principle, be regarded as a legitimate interest, the purposes of which justify the processing of personal data, subject to an assessment that that interest prevails over the interests or fundamental rights of the person concerned. A national provision which did not allow that legitimate interest to be taken into account would be incompatible with that article"

The Advocate General classified the functioning of a telemedium among the legitimate interests of art. 7(f) Data Protection Directive. Breyer rejected the argument that the storage of dynamic IP addresses is necessary to protect the proper functioning of Internet services against possible attacks. The AG responded that he did not think that 'a categorical answer can be given in relation to that problem, whose solution, on the contrary, must be preceded, in each particular case, by a balancing of the interests of the website owner and the rights and interests of users.'[117] The AG asserted that art. 7(f) Directive asks for a case-by-case balancing test.

On 19th October 2016, the Court of Justice published its judgement on the case. The Court decided that a dynamic IP address registered by an online media services provider constitutes personal data, where the provider "has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person."[118] The Court then went on to reply the second question posed by the German Court on whether the storage of those IP addresses at the end of the (website) consultation period is authorised by art. 7(f) of the Data Protection Directive. The Court first said that the national German law[119] had a more restrictive scope than the Directive. In explaining art.7 (f), the Court interpreted the legitimate interest ground provision as precluding "Member States from excluding, categorically and in general, the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in a particular case". The Court provided (65§2):

116 Case C-582/14, Breyer
117 Case C-582/14, Opinion Of Advocate General Campos Sánchez-Bordona delivered on 12 May 2016, footnote 40
118 Case C582/14, Judgment of the Court 19 October 2016, ECLI:EU:C:2016:779
119 Telemediengesetz (Law on telemedia) of 26 February 2007

> "Article 7(f) of Directive 95/46 must be interpreted as precluding the legislation of a Member State, pursuant to which an online media services provider may collect and use personal data relating to a user of those services, without his consent, only in so far as that the collection and use of that data are necessary to facilitate and charge for the specific use of those services by that user, even though the objective aiming to ensure the general operability of those services may justify the use of those data after a consultation period of those websites."

The Court therefore confirmed with its ruling, first, the opinion of the AG as to the case-by-case element of the legitimate interest ground ("in a particular case"). Second it confirmed the ASNEF case approach about the (lack) of powers of the Member States to restrict the scope of the legitimate interest ground. Third, it confirmed the approach of the Court in the RYNES case, namely that the legitimate interest ground guarantees that the (legitimate) interests of the data controller are not disregarded, but considered and balanced against the interests, rights and freedoms of the data subject. In addition, the case offers a new example of a legitimate interest of art.7 (f), not examined by the CJEU in this context before. That is the interest of an online media service provider to collect and use data relating to the use of online media services that are necessary to facilitate and charge for the specific use of the services by the user, with the aim to ensure operability of those services.[120]

7.5 RIGAS SATIKSME case: **suing the data subject for property damages is a legitimate interest**

The case (Rīgas satiksme)[121] concerned a request of a Latvian Court for a preliminary ruling on whether the phrase of art. 7 (f) Directive 95/46/EC 'is necessary for the purposes of the legitimate interests pursued by the third party or parties to whom the data are disclosed' should be interpreted as to allow National Police to disclose personal data to the public transportation company of Riga (Rīgas satiksme) in the civil proceedings.

7.5.1 Facts

A car accident occured in Latvia, after the passenger of a taxi opened the door of the vehicle while a trolleybus of the company Rīgas satiksme was passing next to the taxi. Initially the company sought damages against the taxi driver. The latter however claimed that the passenger was liable for the damages caused to the trolleybus. When Rīgas satiksme requested the personal data of the passenger from the national police, the latter provided the first and last name of the taxi passenger, but declined to provide the identity document number and the address of the passenger. The trolleybus company brought an administrative law action against the competent Administrative Court of Latvia, which at first instance, upheld the action of the trolley company and ordered the national police to provide the requested information. The national police appealed against the ruling, and requested the opinion of the national Data Protection Agency. The latter opined that the national Data Protection Act cannot be used as a legal basis to provide personal data, as the law does not oblige the controller to process the data, but "simply permits it'[122].The referring court however takes the view that in order to bring a civil action the applicant would need to know the residence of the taxi passenger. Following that, the referring court had doubts over the interpretation of the 'necessity' concept of art. 7 (f) of the Data Protection Directive 95/46/EC.

120 For detailed commentary on the significance of the Breyer case, read De Hert, Paul (2017)
121 Case C-13/16, Request for a preliminary ruling from the Augstākā tiesa (Latvia) lodged on 8 January 2016 — Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA (Rīgas satiksme)
122 EU:C:2017:336, para 18

7.5.2 Court Ruling

The CJEU ruled that art. 7(f) of the Directive 95/46/EC expresses the possibility of processing data such as "the communication to a third party of data necessary for the purposes of the legitimate interests pursued by that third party".[123] Thus, there is no obligation to process the personal data on the basis of art. 7(f). This does not mean however that art. 7(f) precludes such processing if the conditions set in the article are met.

The Court went on to examine the three cumulative conditions of the legitimate interest ground. The first condition is the pursuit of a legitimate interest by the data controller of by the third party or parties to whom the data are disclosed. The Court confirmed AG's opinion by ruling that "there is no doubt that the interest of a third party in obtaining the personal information of a person who damaged their property in order to sue that person for damages can be qualified as a legitimate interest"[124] Regarding the necessity condition, the Court reinstated that limitations to the protection of personal data must take place only in so far as is strictly necessary. In the case of the provision of the first and last name of the taxi passenger however, the Court found that merely those data do not make it possible to identify the passenger with 'sufficient precision' in order to bring action against him. In that sense, the Court identified a 'functional element' in the necessity condition of art. 7(f). As for the third condition of the legitimate interest ground, the Court followed the Breyer case argumentation, and ruled that the balancing of the opposing rights and interests depends "in principle on the specific circumstances of the particular case".[125] The Court, however, provided an additional criterion for consideration in the balancing act, and in particular, the seriousness of the infringement to right to protection of personal data; namely, the possibility of accessing the data public sources. The Court referred to the ASNEF case, which also provided that the "seriousness of the infringement of the data subject's fundamental rights resulting from that processing can vary depending on whether or not the data in question already appear in public sources"[126].

7.6 Remarks

The above cases are not providing elaborate interpretation of the legitimate interest ground, but a fragmented compilation of elements that are part of the legitimate interest ground and its components, namely the legitimacy of the interest of the controller or the third party, the necessity and balancing act. The recent Breyer case seems to show a new stance from the CJEU not to miss opportunities to provide interpretation of the legitimate interest ground, as in ASNEF case. In replying the second question for preliminary ruling, the Court could have just assessed whether the national German law restricts the scope of the legitimate interest ground of the Directive. However, the Court went further to clarify that under conditions, the data used by online media service providers to ensure operability of such services could serve a legitimate aim. The Rigas Satiksme case is a prominent example where the CJEU interpreted the three conditions of the balancing test of art. 7(f) of the Directive. Such interpretations are more than valuable. Despite that all the above case law refers to the Directive, the small changes of the provision in the GDPR text, render the case law findings a good first basis for interpretation also of the GDPR legitimate interest ground.

123 EU:C:2017:336, para 26
124 EU:C:2017:336, para 29
125 EU:C:2017:336, para 31
126 EU:C:2011:777, para 44

8. Selected case studies for the new legitimate interest ground

As seen in the previous section, a broad variety of interests can be brought under the legitimate interest ground. The ultimate reality check of the legitimate interest ground in the GDPR is done by the judicial authorities. The national courts and the Court of Justice of the EU will be the gatekeepers of the correct implementation of the GDPR, but also of what Skouris says "to adjust the legislative choices to societal challenges". Prior to that, supervisory authorities, the controllers, the data subjects, are called each one from a different perspective, to check whether the provision is applied in a harmonised way, whether the data subject rights are protected and whether processing based on the legitimate interest ground can allow business models to develop, while respecting the right to protection of personal data of the individuals.

The aim of this sub-section is to illustrate some of the questions, prepositions and practical issues regarding the application of the legitimate interest ground in several cases. As a starting point we take the examples provided in the Recitals of the GDPR and further elaborate on them. In the recitals of the GDPR,[127] we see a first distinction of legitimate interests of the controller, that is those that constitute prima facie 'legitimate interest' overriding the data subjects' interests, rights and freedoms, and the ones that may override the interests of the data subject. It should be noted that the first category is in principle considered as a legitimate interest, even though the GDPR relates it to a series of conditions (strictly necessary, proportionate) and it should be contextualised. In the first category,[128] the GDPR includes processing of personal data for preventing fraud (Rec. 47) and network and information security (Rec.49). In the second category, direct marketing purposes (Rec. 47) is brought as an example. [129]

8.1 Network & Information Security, and anti-fraud measures

An operator of a website may have a legitimate interest in storing certain personal data relating to visitors to that website in order to protect itself against cyberattacks. Network and information security purposes are in principle seen as a legitimate interest pursued by a controller.[130] The GDPR highlights that this is the case, when strictly necessary and proportionate. The above approach in the GDPR recital treating (under conditions) network and information security as legitimate interest pursued by the controller, is also compatible with the Directive on Information Systems (Cybercrime Directive).[131] The Cybercrime Directive provides that the identification and reporting of threats and risks posed by cyberattacks is a pertinent element of effective prevention (Rec.12).

Such a purpose would in principle be legitimate, if real and present, in line with the law and clearly articulated. Regarding the necessity element, it can be assumed that in specific cases (not as a general rule),

127 Recitals 47, 48 and 49 GDPR.
128 This categorisation is not formalised in the GDPR, but we follow it in this contribution in order to group the types of legitimate interests and facilitate the discussion.
129 Recital 48 GDPR also provides the example of processing, including transmission, for internal administrative purposes within a group of undertakings or institutions that may constitute a legitimate interest of the controller.
130 Recital 49 GDPR.
131 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, L 218/8, 14.8.2013

processing for the purpose of ensuring network and information security, could be regarded as necessary, when for instance there is an ongoing attack or an identified threat. The critical issue with network and information security purposes will be the balancing stage, which will determine whether and to what extent such purposes pursued by the controller or a third party can prevail over the interests of the data subject. Processing for information security purposes should not be abused as a generic clause that fits all cases.

In practice, it is rare that only the controller runs the information security activities. The processor should also provide sufficient guarantees to implement appropriate technical and organisational measures (art. 28 GDPR). In fact, often it is a processor, for instance in cloud computing, that provides the day-to-day information security measures. In addition, the obligation of art. 32 GDPR on secure processing applies to both controller and processor. It follows that the processor may also have a legitimate interest to process data in such cases, but this interest does not qualify to prevail over the interest, rights and freedoms of the individual based on art. 6(1) (f) GDPR. It should however be accepted that such processing activity aligns with the legitimate interest of the controller for information security, and subsequently, covered by this concept.

Another case is the prevention of fraud (Recital 47 GDPR). A processing operation which supports such purposes, is unlikely to be based on one of the other grounds of art. 6 GDPR. Consent of the data subject – who in the case of fraud investigation is the suspect criminal – will most probably not be provided by the data subject, by exercising its right to non-self-incrimination. Contract, vital interest, and public interest grounds are not relevant, with the exception of public interest when fraud is committed or attempted against the public sector. The only alternative to legitimate interest of the controller ground in the case of the prevention of fraud or crime in general, is the compliance with a legal obligation to which the controller is subject. Nevertheless, such obligation is often difficult to be established in the preliminary stages of a criminal investigation. The legitimate interest of the controller would qualify for the prevention of fraud, on the condition that the requirements are met and the principles of art. 5 GDPR are respected. A generic 'prevention of fraud' purpose is not a legitimate interest prevailing over the data subject's interests. Specific circumstances that justify the processing for the prevention of fraud in each case as the proportionate measure are necessary.

8.2 Big data and profiling

In a recent study, Moerel and Prins pinpoint deficiencies of legal norms of the data protection regulatory framework in Europe. One of the examples the authors put forward is the new age of systems based on algorithms, that are able to combine and analyse vast amounts of data gathered from numerous sources. This activity brings, according to the authors, the legitimate interest of the controller to the forefront. The authors propose a test based on the legitimate interest ground for data collection and processing purposes. Other scholars suggest that "personal data processing for behavioural targeting that involves tracking people over various Internet services cannot be based on Article 7(f) of the Data Protection Directive, necessity for the legitimate interests of the controller".[132]

The above discussion reflects two things: first that the processing personal data in the case of profiling, for instance for direct marketing purposes, may be a legitimate interest pursued by the controller. Recital

132 Borgesius, F. J. Z. "Personal data processing for behavioural targeting: which legal basis?" **International Data Privacy Law**, 2015, ipv011.

47 of the GDPR provides that "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest." Second, is that the opinions on whether the legitimate interest ground is an appropriate legal basis for processing are diverse. It is not far reaching to assume, a similar multi-vocal approach from the part of the supervisory authorities. For instance, the UK Information Commissioner (ICO) suggests that "an organisation may have a number of legitimate interests that could be relevant, including, for example: profiling customers in order to target its marketing; preventing fraud or the misuse of its services; physical or IT security". At the same time, other DPAs might take be more reluctant to point towards the direction of legitimate interest ground in the case of big data, profiling, but even marketing. In general, despite that in the case of big data, legal bases such as 'consent' might be difficult, we are not convinced that the legitimate interest ground is appropriate for each case of big data profiling. Instead, due to the problematic application of some of the personal data principles (such as purpose limitation and specification)[133] in the big data context, the risk for the (un)lawfulness of processing is increased.

9. Conclusions

The methodological tool of balancing is fundamental in the EU law to achieve a proportionate result between conflicting (or else 'competing') rights. The EU data protection law, both the Data Protection Directive and the new General Data Protection Regulation, introduce the proportionality principle in the grounds for lawful processing, in art. 6(1)(f), the legitimate interest of the controller ground. The rationale of the legitimate interest ground is that under certain conditions such interests might be strong and justified enough to prevail over the interests, rights, and freedoms of the data subject. When and how the prevailing can take place under the GDPR provisions is not a one-dimensional assessment.

The legitimate interest ground as provided in the previous regime of the Data Protection Directive, has been criticised as a 'loophole' in the EU data protection law, as being vague and flexible to allow for broad interpretations under what may constitute a legitimate interest of the controller or a third party. The Regulation does not substantially alter the wording of the relevant provision in relation to the Directive. In fact, the examples of legitimate interest provided in Recitals of the GDPR partially confirm the above critique referring to a broad range of interests that can 'slip through' under the provision of art. 6(1)(f) GDPR. Network and Information Security, anti-fraud measures to internal administrative purposes within a group of undertakings or direct marketing (Recitals 47-49) demonstrate this argument. However, we do not agree with that the legitimate interest ground is a loophole in the EU data protection law. First, the ground is not a self-standing provision, but one of the 'safeguards' established in the EU data protection secondary law, aiming to protect the fundamental right of art. 8 Charter. As such, the ground should be read through the lens of the data protection principles of art. 5 GDPR (i.e. lawfulness and fairness of processing). In that respect, the GDPR introduced a significant improvement in relation to the Directive; that is the principle of accountability: the positive obligation of the controller to respect, comply, document and demonstrate compliance with the Regulation. Along with the data protection principles, the legitimate interest ground 'boundaries' are framed by the art. 8 of the Charter. Thus, even if the interests of the controller prevail over the data subject's interests in one specific occasion, this only means that the controller has a base for lawful processing of the data subject's personal data. The ground and the weighing included in the provision should not be seen as having a broader effect than they have. The interests, rights and freedoms of the data subject are not abolished. On the contrary, once the controller is subject to the GDPR, he or she

133 Tene and Polonetsky characterise the relationship of data minimization with big data business models as antithetical. Tene and Polonetsky (2013)

needs to comply with his or her legal obligations derived from the Regulation, including the data subject rights, the organisational and technical measures and the whole set of obligations established in the GDPR.

This brings us to the second point. The legitimate interest ground is first necessarily determined by the controller himself or herself. It is of utmost importance that the supervisory authorities (DPAs), and subsequently the national courts, thoroughly check the continuous justification of the ground for as long as the processing takes place on the basis of this ground.

Ultimately, the CJEU will play a significant role in interpreting the provision in line with the Charter, but also the societal needs and technological emergence. To date, the Court has delivered marked decisions in the EU data protection law field, but has not fully taken the opportunity to interpret the legitimate interest ground. The recent Breyer and Rigas satiksme cases, showed the intention of the Court to provide answers.

In this contribution, we suggested a formalisation of the legitimate interest ground steps towards the decision of the controller on whether to base his or her processing on the legitimate interest ground. The proposed three steps and their components are informed primarily by the GDPR provision of art. 6(1) (f), the GDPR recitals, but also other sources, such as guidance provided by the WP29 and the European Data Protection Supervisor. Such a framework, with its essential components ('reasonable expectations of the data subject', impact assessment, and others), provides tools to protect against controllers in bad faith, who are over-broadening the concept of legitimate interest, and help controllers in good faith, make a proper decision on whether the ground of art. 6(1) (f) is an appropriate legal basis for their intended personal data processing activity.

Literature

Alexy Robert "Constitutional Rights, Balancing, and Rationality", ***Ratio Juris,*** vol. 16 no. 2, 2003

Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217, April 2014

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor', WP169, 2010

Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, WP187, 13 July 2011

Article 29 Data Protection Working Party, Working Party Comments to the vote of 21 October 2013 by the European Parliament's LIBE Committee, Annex to letter to Greek Presidency, 11 December 2013,

Bagger Tranberg Charlotte, "Proportionality and data protection in the case law of the European Court of Justice", ***International Data Privacy Law,*** 2011, Vol. 1, No. 4, pp.239-248

Balboni, Paolo, Daniel Cooper, Rosario Imperiali, and Milda Macenaite. "Legitimate interest of the data controller. New data protection paradigm: legitimacy grounded on appropriate protection." ***International Data Privacy Law***, ipt019, 2013

Bennett Colin J. and Robin M. Bayley "Privacy Protection in the era of 'big data': regulatory challenges and social assessments" in Bart van der Sloot, Dennis Broeders & Erik Schrijvers (eds.) ***Exploring the Boundaries of Big Data,*** Amsterdam University Press 2016

Bits of Freedom, "A loophole in data processing. Why the 'legitimate interests' test fails to protect the interests" 2012

Borgesius, Frederik J. Zuiderveen. "Personal data processing for behavioural targeting: which legal basis?" ***International Data Privacy Law***, 2015, ipv011

Boyd, Danah, and Kate Crawford "Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon" ***Information, communication & society*** 15, no. 5, 2012, pp.662-679.

Bygrave, Lee A., and Dag Wiese Schartum. "Consent, proportionality and collective power." In Serge Gutwirth, Yves Poullet, Paul de Hert, Cécile de Terwangne & Sjaak Nouwt (eds.) ***Reinventing Data Protection?*** pp. 157-173. Springer Netherlands, 2009.

Cate, Fred H., and Viktor Mayer-Schönberger "Notice and consent in a world of Big Data" ***International Data Privacy Law*** 3, no. 2, 2013 pp. 67-73.

Centre for Information Policy Leadership (CIPL) Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR" 2017

Commission of the European Communities, Report from the Commission. First Report on the Implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final

Corbin Arthur "Legal Analysis and Terminology" 29 ***Yale L.J.*** 163 1919-1920, p.173

Cuijpers, C.M.K.C., Purtova, N.N. & Kosta, E. "Data protection reform and the internet: the draft Data Protection Regulation", in A Savin & J Trzaskowski (eds.), ***Research Handbook on EU Internet Law***, Edward Elgar, 2014, pp. 543-568

Davies, S. "The Data Protection Regulation: A Triumph of Pragmatism over Principle?" ***European Data Protection Law Review***, Vol. 2, Issue 3, 2016, pp. 290 - 296

De Hert, Paul "Data Protection's Future without Democratic Bright Line Rules. Co-existing with Technologies in Europe after ***Breyer***", ***European Data Protection Law Journal*** vol. 1, 2017

De Hert Paul, Vagelis Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?', ***Computer Law & Security Review,*** vol. 32, 2016, pp. 179-194

De Hert, Paul, Serge Gutwirth. "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power." Erik Claes, Antony Duff, Serge Gutwirth (eds.) ***Privacy and the criminal law***, Interentia, 2006, pp. 61-104.

De Hert, Paul, Vagelis Papakonstantinou. "Google Spain: Addressing critiques and misunderstandings one year later." ***Maastricht Journal of European and Comparative Law*** 22, no. 4, 2015, 624-638.

European Data Protection Supervisor, Developing a 'toolkit' for assessing the necessity of measures that interfere with fundamental rights, Background paper, June 2016

European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - "European Strategy for a Better Internet for Children", July 2012

Ferretti Federico "Data Protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights?" ***Common Law Market Review*** 51: 843-868, 2014

Fuster, Gloria Gonzàlez "Fighting for Your Right to What Exactly-The Convoluted Case Law of the EU Court of Justice on Privacy and/Or Personal Data Protection" ***Birkbeck Law Review*** 2, 2014, 263.

Girot, Clarisse, ***User protection in IT contracts: A comparative study of the protection of the user against defective performance in information technology***. Vol. 11. Kluwer Law International, 2001.

Habermas Jurgen "***Between facts and norms***" Cambridge: Polity, 1992

ICO "Big Data and Data Protection" version 1.0, 2014

Harbo Tor-Inge "The Function of the Proportionality Principle in the EU law", ***European Law Journal,*** vol. 16 no.2, 2010, pp.158-185

International Chambers of Commerce, 'ICC Position on Legitimate Interests', ETD/STM – 28 October 2015

ISO 31000:2009 Risk management-Principles and guidelines, ISO/IEC 27005:2011, Information technology -Security techniques - Information security risk management

Jasmontaite, Lina, and Paul De Hert. "The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet." ***International Data Privacy Law*** 5, no. 1, 2015, pp. 20-33.

Korff Douwe "The Standard Approach Under Articles 8 – 11 ECHR and Article 2 ECHR", 2008

Kuner Christopher, "The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges", in: Burkhard Hess and Cristina M. Mariottini (eds.), ***Protecting Privacy in Private International and Procedural Law and by Data Protection,*** Farnham, Surrey, UK England : Ashgate, 2015 pp. 19-55.

Kuner Christopher, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", ***Privacy & Security Law Report***, 11 PVLR 06, 2012

Moerel, Lokke and Prins, Corien "Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things" 2016

Mark Powell, 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 (92/C 311/04) COM (92) 422 final — syn 287, ***Computer Law & Security Review***, Volume 10, 1994, pp. 43-46, ISSN 0267-3649

National Institute of Standards and Technology "Privacy Risk Management for Federal Information Systems', NISTIR 8062 draft, http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf, (accessed 18 September 2016)

Poullet, Yves "EU data protection policy. The Directive 95/46/EC: Ten years after" ***Computer Law & Security Review***, Volume 22, Issue 3, 2006, pp. 206-217, ISSN 0267-3649

Rauhofer, Judith. "One Step Forward, Two Steps Back? Critical observations on the proposed reform of the EU data protection framework." ***Journal of Law and Economic Regulation*** 6, no. 1 (2013): 57-84.

Skouris Vasilios, 'After 12 Years', ***Maastricht Journal of European and Comparative Law***, 23 MJ 2, 2016

Solove, Daniel J. "Privacy self-management and the consent dilemma." ***Harvard Law Review*** Vol.126: 1880 2013

Tene Omer and Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11

Nw.J.Tech. & Intell. Prop. 239, 2013
Zingales N. "Unreasonable v. Unfair Data Processing: Contrasting Two Rising Modes of Protection Against Over-reaching Terms of Service", unpublished paper presented in Amsterdam Privacy Conference, 2015
-
Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, L 218/8, 14.8.2013
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, L 281, 23.11.1995
European Parliament, Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (COM(2012)0011 – C70025/2012 – 2012/0011(COD))
European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM (2012) 11 final – 2012/0011 (COD), 25.01.2012
European Council, Preparation of a general approach. 9565/15, 11.6.2015, adopted at JHA Council Meeting on 15.6.2015
Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM (1990) 314-2, 1990/0287/COD
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)
Treaty on the Functioning of the EU European Union, OJ C 326, 26.10.2012
-
Court of Justice of the European Union, Judgment of the Court of First Instance 8 May 2007, ***Citymo v Commission***, Case T271/04, EU:T:2007:128
Court of Justice of the European Union, Judgement of 24 November 2011, ***ASNEF***, ***FECEMD***, Joined Cases C-468/10 and C-469/10, EU:C:2011:777
Court of Justice of the European Union, Judgement of 8 April 2014, ***Digital Rights Ireland, Seitlinger***, Joined Cases C-293/12 and C-594/12, EU:C:2014:238
Court of Justice of the European Union, Judgement of 11 December 2014, ***Ryneš***, C-212/13, EU:C:2014:2428
Court of Justice of the European Union, Judgement of 13 May 2014, Case C-131/12, ***Google Spain and Google***, EU:C:2014:317
Court of Justice of the European Union, Judgement of 6 October 2015, ***Schrems***, Case C-362/14, EU:C:2015:650
Court of Justice of the European Union, Opinion of Advocate General Campos Sánchez-Bordona of 12 May 2016, ***Breyer,*** C-582/14, EU:C:2016:339
Court of Justice of the European Union, Judgement of 19 October 2016, ***Breyer,*** Case C-582/14, EU:C:2016:779
Court of Justice of the European Union, Judgement of 9 March 2017, ***Manni,*** Case C-398/15 EU:C:2017:197
Court of Justice of the European Union, Judgement of 4 May 2017, ***Rīgas satiksme***, Case C-13/16, EU:C:2017:336
European Court of Human Rights, Judgement of 24 June 2004, ***von Hannover v Germany***, (Application no. 59320/00)
European Court of Human Rights, Judgement of 17 July 2008, ***I v. Finland*** (Application no. 20511/03)

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Editorial Board: Paul De Hert, Christopher Kuner and Gloria González Fuster

Contact: info@brusselsprivacyhub.org

N°1 "The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area" (November 2014) by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection" (November 2014) by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 "Towards efficient cooperation between supervisory authorities in the area of data privacy law" (October 2015) by Dariusz Kloza, Antonella Galetta (24 pages)

N°4 "The data protection regime in China" (November 2015) by Paul De Hert and Vagelis Papakonstantinou (30 pages)

N°5 "The right to privacy and personal data protection in Brazil: time for internet privacy rights?" (February 2016) by Vinícius Borges Fortes (23 pages)

N°6 "Permissions and Prohibitions in Data Protection Jurisdiction" (May 2016) by Mistale Taylor (25 pages)

N°7 "Structure and Enforcement of Data Privacy Law in South Korea" (October 2016) by Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung (20 pages)

N°8 "The "Right to be Forgotten" and Search Engine Liability" (December 2016) by Hiroshi Miyashita (15 pages)

N°9 "European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges" (March 2017) by Gianclaudio Malgieri & Paul De Hert (25 pages)

See following page for more recent Working Papers

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Editorial Board: Paul De Hert, Christopher Kuner and Gloria González Fuster

Contact: info@brusselsprivacyhub.org

N°1 - N°9 See list on previous page

N°10 "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw" (July 2017) by Meg Leta Jones, JD, PhD (31 pages)

N°11 "The Microsoft Ireland case and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies" (July 2018) by Paul De Hert and Johannes Thumfart (27 pages)

N°12 "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach" (August 2018) by Irene Kamara and Paul De Hert (35 pages)

VUB BRUSSELS PRIVACY HUB