Data Protection by Design and by Default:

Framing Guiding Principles into Legal Obligations in the GDPR

*Lina Jasmontaite, Irene Kamara, Gabriela Zanfir-Fortuna and Stefano Leucci**

In this contribution we examine the principles of Data Protection by Design and Data Protection by Default (DPbD and DPbDf) as introduced in the General Data Protection Regulation 2016/679 (GDPR). In particular, we seek answering these questions: 'what are the elements of DPbD and DPbDf obligations under the Article 25 of the GDPR and how could they be interpreted and applied in practice'? By reflecting on elements embedded in these two concepts we aim at contributing to the ongoing debate on the implementation of these principles and conquering the opinion that DPbD and DPbDf contain ambiguous wording and confusing legalese that cannot be digested. Considering high stakes of being GDPR (in)compliant, we focus on the translation of the two legal provisions into high-level non-functional design requirements. We build on the existing knowledge about each element and also take into account a wider context in which such obligations were negotiated and introduced. We argue that while at first glance DPbDf is mainly linked to the data minimisation and purpose limitation principles, it is also equally relevant for the principles of data retention, confidentiality and accessibility. We suggest that the entire weight of the GDPR rests on the 'shoulders' of Article 25 and that, theoretically at least, complying with the DPbD and DPbDf principles is the key for the GDPR compliance.

I. Introduction

Data Protection by Design and Data Protection by Default (DPbD and DPbDf) left the realm of 'buzzwords' and entered the one of legal obligations, once the European General Data Protection Regulation[1] (GDPR) was adopted in 2016. The importance of these principles has grown in proportion to the deadline for the GDPR implementation and the fears over looming fines.

The underlying objective of DPbD and DPbDf obligations is to integrate privacy throughout the lifecycle of various technologies and applications that process personal data. At the same time, the practical implementation of DPbD and DPbDf is tremendously complex because of the uncertainty shielding the meaning of these principles. Challenges for engineers include the need for contextualisation, ambiguous legal principles embedding values and social perceptions that accompany the fundamental rights at stake – the right to respect for private life and the right to protection of personal data. In parallel, big data applications, such as predictive analytics in consumer marketing, and more recently machine learning applications, intensify the interference with the right to the protection of personal data and create the need for 'by design' and 'by default' protection.

* Lina Jasmontaite, Researcher, Vrije Universiteit Brussel, Research Group on Law, Science, Technology and Society (LSTS), Belgium <lina.jasmontaite@vub.be>. Irene Kamara, Researcher, Tilburg University, Tilburg Institute for Law, Technology, and Society (TILT), the Netherlands, Affiliated Researcher, Vrije Universiteit Brussel, Research Group on Law, Science, Technology and Society (LSTS), Belgium <i.kamara@uvt.nl>. Gabriela Zanfir-Fortuna, PhD, Fellow of the Future of Privacy Forum, USA, Affiliated Researcher, Vrije Universiteit Brussel, Research Group on Law, Science, Technology and Society (LSTS), Belgium <gzanfir-fortuna@fpf.org>. Stefano Leucci, Legal and technical researcher and fellow, Nexa Center for Internet and Society – Politecnico di Torino, Italy <stefanoleucci@gmail.com>.
The research for this article was made possible partially thanks to the funding from the EU Horizon 2020 Framework Programme for research and innovation under the CANVAS (Constructing an Alliance for Value-driven Cybersecurity) project, grant agreement no 700540 and the Research Coordination Network project of the Future of Privacy Forum, through a grant awarded by the US National Science Foundation. We would like to express sincere thanks to Prof Gloria Gonzalez Fuster, Dr Jaap-Henk Hoepman and the two EDPL reviewers for their feedback on an earlier version of this paper. We also would like to thank the participants of TILTing perspectives conference for their feedback and the

This article contributes to the efforts aiming at bridging the gap between legal requirements and practical steps towards compliance, by answering these questions: 'what are the elements of DPbD and DPbDf obligations under the new Article 25 GDPR and how could they be applied in practice'?

We preface our contribution with an overview of arguments that were used in support of, as well as against the introduction of Article 25 into the GDPR throughout the legislative process.[2] The second part of the article sets out the elements of DPbD as set forth in Article 25.1 of the GDPR. After identifying different elements and concepts included in the DPbD formula, the section explores them in greater detail. This section also suggests how data controllers could demonstrate compliance with the DPbD obligations. Our interpretation explains the relation of DPbD with other concepts essential to the EU Data Protection Framework and Privacy Enhancing Technologies (PETs) and by extending their meaning beyond the notion of information security.

In the following part, we analyse the concept of Data Protection by Default. To this end, we differentiate between the concepts of Data Protection by Design and Data Protection by Default. While the concepts are interrelated, Data Protection by Design refers to the existence of embedded safeguards and mechanisms throughout the lifecycle of the application, service or product that protect the right to data protection, whereas Data Protection by Default refers to the activation and application of such safeguards as default setting.

II. EU Data Protection Law Reform: GDPR Introduces DPbD and DPbDf

The GDPR, adopted in April 2016, repealed the Data Protection Directive 95/46/EC[3] (Data Protection Directive or Directive) and while doing so it has modernised the European Union (EU) data protection legal framework. The GDPR extrapolated rules set out in the Data Protection Directive by updating the existing requirements and principles as well as by introducing new concepts (eg, pseudonymisation) and obligations. Among these obligations is the requirement to implement Data Protection by Design and Data Protection by Default. While many consider the privacy by design principle as coined by Cavoukian had a huge impact for the development of these new obligations, some suggest and we are inclined to believe that the origins of these new requirements can be traced back to the requirements set forth by the Data Protection Directive.[4]

The Directive[5] addressed security of processing and required controllers to implement appropriate technical and organisational measures. Taken together these measures should have ensured protection of personal data 'against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access'.[6] Article 17 of the Directive did not explicitly refer to DPbD but its corresponding Recital 46 included wording and legal thinking that was carried over to the GDPR. According to the Recital, appropriate technical and organisational measures should have been implemented 'both at the time of the design of the processing system and of the processing itself'.[7] This wording has been transferred to Article 25, which requires controllers to implement appropriate technical and organisational measures 'at the time of the determination of the means for processing and at the time of the processing itself'.[8] Following up on this observation, it is apparent that the GDPR wording is not entirely new for EU data protection law. Article 25 GDPR rather frames the principle of the Directive into a mandatory legal requirement and it also broadens its scope.

IPEN (Internet Privacy Engineering Network of the European Data Protection Supervisor) which provoked our discussions and provided us with a platform for this collaboration.

1 European Parliament and the Council, 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).

2 Due to length limitations of this article the relevant scholarship on privacy by design is referred to where appropriate.

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

4 See Ann Cavoukian, 'Privacy by Design. The 7 Foundational Principles' (2011) <https://www.ipc.on.ca/?redirect=https%3A%2F%2Fwww.ipc.on.ca%2Fimages%2FResources%2F7foundationalprinciples.pdf> accessed 20 April 2017; Ann Cavoukian, 'Privacy by Design in Law' (2011) Policy and Practice; Peter Hustinx, 'Privacy by design: delivering the promises' (2010) 3 IDIS 253; Lee A Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4(2) Oslo Law Review.

5 Directive 95/46/EC, art 17.

6 ibid.

7 Directive 95/46/EC, recital 46.

8 GDPR, art 25.1.

In the following section we explain how the principles of Data Protection by Design and Data Protection by Default morphed into legally binding obligations.

1. A Call for Legislative Action on Data Protection by Design

Replying to the public consultation of the European Commission (EC or Commission) initiated on 9 July 2009 to gather input for the data protection reform, the Article 29 Working Party (WP29), composed of representatives of independent European Data Protection Authorities (DPAs), drew attention to the fact that even if the above mentioned provisions of the Data Protection Directive (Article 17 and Recital 46) were 'helpful towards the promotion of privacy by design, in practice, they have not been sufficient in ensuring that privacy is embedded in ICT'.[9] Considering that average users of ICT services have limited skills and knowledge about relevant security measures protecting their and others personal data, 'services and technologies should be designed with privacy by default settings' in mind.[10] To this end, WP29 called for the Commission to include in the future legal framework 'a provision translating the currently punctual requirements into a broader and consistent principle of privacy by design'.[11] WP29 reasoned that the principles of privacy and data protection by design and by default should be introduced in the revised EU data protection framework in order to outweigh risks arising from innovative technologies.[12] The WP29 was quite specific about what an enhanced Privacy by Design principle should mean in practice: respecting data minimization, transparency, data confidentiality and requiring user friendly systems, use limitation and controllability.[13] Moreover, the WP29 pleaded that the privacy by design principle should 'not only be binding for data controllers, but also for technology designers and producers'.[14]

To a large extent, the Commission took on board this idea. In the Communication that accompanied the proposal for a General Data Protection Regulation in 2012, it noted that 'introducing the Privacy by Design principle to make sure that data protection safeguards are taken into account at the planning stage of procedures and systems'[15] is a key point of the data protection reform, aiming to enhance the accountability of those that are processing data. A considerable weight to 'Data Protection by Design' principle was also placed by the Impact Assessment that stood at the basis of the data protection reform.[16] The Impact Assessment explained that the 'Data Protection by Design' principle required the controller 'to design the organisational structure, technology and procedures in a way that it meets the requirements of data protection'.[17]

The initial proposal for an article on 'Data Protection by Design and by Default' required controllers to implement appropriate technical and organisational measures and procedures, 'both at the time of the determination of the means for processing and at the time of the processing itself'.[18] This should be done in such a way that the processing would satisfy GDPR requirements and protect the rights of the data subject.[19] The proposed text required controllers to implement Data Protection by Design measures taking into account 'the state of the art and the cost of implementation'. While many of these elements remain in the final text of the GDPR, Article 25 represents a political compromise. The proposal for the Regulation, including the provision promoting Data Protection by Design and by Default, went through numerous modifications during the four year long legislative procedure, among the European Commission, European Parliament (EP) and the Council.[20]

9 Article 29 Data Protection Working Party, 'The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data' (2009) 02356/09/EN, WP168, para 45 (Article 29 Working Party, 'The Future of Privacy').

10 ibid.

11 ibid para 46.

12 ibid.

13 ibid, para 53.

14 ibid, 3.

15 European Commission Communication, 'Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st century' (2012) COM(2012) 9 final, 7.

16 Commission Staff Working Paper, 'Impact Assessment' (2012) SEC(2012) 72 final, Annex 2. Evaluation of the Implementation of the Data Protection Directive.

17 ibid 72.

18 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), 2012/0011 (COD), art 23.

19 ibid.

20 For an explanation on how the ordinary legislative procedure works at EU level, see European Parliament, 'Codecision and Conciliation. A guide to how the European Parliament co-legislates under the ordinary legislative procedure' (December 2014) <http://www.europarl.europa.eu/code/information/guide_en.pdf> accessed 16 April 2018.

In the following section we summarise discussions regarding the principles of DPbD and DPbDf during the legislative deliberations process of the GDPR. In particular, we focus on amendments suggested by the legislative bodies. We deem that understanding these positions facilitates interpretation of Article 25.

2. Legislative Deliberations: Framing the Principles of DPbD and DPbDf

In comparison to the Commission's proposal, the EP proposed[21] to expand the scope of Data Protection by Design obligations and make it applicable to processors.[22] With processors playing an increasingly important role within data processing operations, the EP argued that DPbD requirements should address the entire lifecycle management of personal data (ie, collection, processing and deletion). The EP also wanted to insert a special requirement that Data Protection by Design should be a prerequisite for public procurement tenders at EU level. These proposals probably fell short of support at the Council and therefore they are not reflected in the final text of the GDPR.[23]

For its version of the text, the Council[24] voted to add multiple criteria to be taken into account by controllers (and only controllers) when implementing technical and organisational measures, besides the state of the art and the cost of implementation: 'the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for rights and freedoms of individuals posed by the processing'. By doing so the Council brought this provision closer to the wording of a risk-based approach and also added to its complexity. Following recommendations of national experts, the Council also introduced a specific reference to pseudonymisation as an appropriate technical measure to be applied within the context of Article 23 of the Proposal (now Article 25 GDPR). In addition, it seems that the Council intended to abolish the 'by design' element of Data Protection by Design, as its final version of Article 23 deleted the requirement that technical and organisational measures must be taken 'at the time of the determination of the means for processing and at the time of processing itself'. The Council also inserted a new paragraph in Article 23, stipulating that an approved certification mechanism may be used as an element to demonstrate compliance with the requirements of Data Protection by Design and by Default.[25]

While the added criteria (ie, the reference to pseudonymisation and to the certification mechanism) appear in the final text of the GDPR as introduced by the Council, the suggestion to delete the 'by design' element did not receive support during the trilogue. Likewise, the proposal of the Parliament to extend DPbD obligations to processors is also not reflected in the final text of the GDPR.

However, the debate of who should be responsible for implementing DPbD and DPbDf measures is still ongoing in the EU. Discussions concerning the ePrivacy framework are illustrative of this unresolved issue.[26] Observing the absence of 'by design'

21 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)' (2014) [COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)].

22 However, this was not the case with the Data Protection by Default provision (art 23.2), as the Parliament 1st Reading maintained the scope of the provision limited to controllers. This is presumably due to the lack of power of the processor to determine default options whereas this is a decision to be made by the controller and implemented by both the controller and any processor processing data on the controller's behalf.

23 European Parliament and the Council, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)' [2016] OJ L119/1.

24 Council, 'General approach of the Council, 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)' (2015) Interinstitutional file 2012/0011 (COD), 9565/15.

25 The discussion of certification based on art 25.3 GDPR is beyond the scope of this article, which rather focuses on the analysis of the concepts and their prerogatives, than operationalisation mechanisms of DPbD and DPbDf, such as technical standards and certification. Read further on GDPR certification, including the scope of certification and existing Privacy by Design certifications in: ENISA, 'Recommendations on European Data Protection Certification' (2017) <https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification> accessed 10 February 2018 ('ENISA Recommendations').

26 European Parliament and the Council, 'Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector' [2002] OJ L 201 is currently undergoing a reform process with the aim of having a Regulation replacing it and becoming applicable on the same day with the GDPR.

and 'by default' legal requirements from the ePrivacy draft regulation as tabled by the Commission in January 2017[27], which lies on the *lex specialis* relationship of the two legal instruments,[28] the European Data Protection Supervisor (EDPS) advised the legislature to 'impose an obligation on hardware and software providers to implement default settings that protect end users' devices against any unauthorised access to or storage of information on their devices'.[29] This call to extend DPbD and DPbDf obligations to hardware and software providers, regardless of whether they are controllers or processors, perpetuates the view expressed by the Article 29 Working Party in 2009, as mentioned above.

III. The Elements of DPbD According to Article 25

This section carves out all of the elements embedded in Article 25.1 in order to clarify its legal construct. DPbD was rightfully described as 'a new type of legal concept, whereby law aligns itself with the earlier ethical and policy-oriented concept of Privacy by Design'.[30] At the same time, we challenge voices that consider the principle of DPbD (often referred to as Privacy by Design by engineers) to be a compilation of 'vague principles'.[31]

Essentially, Article 25.1 entails a positive obligation to act for the data controller. It has to implement both organisational and technical measures in order to ensure that the requirements of the GDPR are embedded in the processing activity, in an effective manner, at the time of initiating it as well as at its later stages. The data controller has to do so by taking into account the nature, scope and context of processing and other criteria detailed in the provision.

Understanding that the content of the DPbD principle requires implementing GDPR-specific requirements, with a focus on data protection principles and the rights of the data subject, in the design of processing operations highlights why DPbD is different than the concept of Privacy by Design, even though their underlying objective is the same: embedding safeguards to protect the rights of individuals from the conception of a system using personal data. Privacy by Design is a policy goal, promoted initially by the Privacy Commissioner of Ontario in 2009 with the proposal of seven foundational principles[32], then by the International Conference of Privacy Commissioners in 2010[33], and also by the Federal Trade Commission of the US (FTC) in a guidance document issued in 2012[34]. The FTC defined the baseline principle of Privacy by Design as meaning that '[c]ompanies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services'.[35] The FCT interpretation of Privacy by Design embraces principles that are close to the EU counterparts, such as 'data security, reasonable collection limits, sound retention and disposal practices, and data accuracy'.[36] However, these principles are worded broadly and are applicable to a limited number of sectors who are subject to substantive law provisions.

By contrast, DPbD is a legal obligation, the noncompliance with which is sanctioned with fines.[37] DPbD protects the right to protection of personal da-

27 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on privacy and electronic communications)' [2017] COM(2017) 10 final, 2017/0003 (COD).

28 The proposal for the ePrivacy Regulation (2017) explicitly refers to the lex specialis relationship of the ePrivacy Regulation to the GDPR (art 3.3 of the Proposal) and clearly provides that 'All matters concerning the processing of personal data not specifically addressed by the proposal are covered by the GDPR' (Explanatory Memorandum, 2).

29 European Data Protection Supervisor, 'Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)' (2017) 19.

30 Mireille Hildebrandt and Laura Tielemans, 'Data Protection by Design and technology neutral law' (2013) 29 Computer law & Security Review 509-521.

31 For example, Bygrave (n 5); Michael Veale, Reuben Binns and Jef Ausloos, 'When data protection by design and data subject rights clash' (2018) International Data Privacy Law, ipy002 <https://doi.org/10.1093/idpl/ipy002>.

32 Ann Cavoukian, 'Privacy by Design: The seven foundational principles' (The Information Commissioner of Ontario, 2009) This was revised in 2011.

33 'Resolution on Privacy by Design' (32nd International Conference of Data Protection and Privacy Commissioners Jerusalem, Israel 27-29 October 2010).

34 FTC, 'Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Businesses and Policymakers' (2012).

35 ibid 22.

36 ibid.

37 Such fines can reach up to €20 million or 4% of the global annual turnover of the controller (GDPR, art 83).

ta[38] and the rights of all individuals whose personal data are processed, not only consumer data. DPbD is moulded on the structure of the GDPR, with a focus on data protection principles under Article 5 and the rights of individuals (ie, the data subjects) under Chapter III.

Additionally, Article 25 GDPR entails most of the elements present in other articles that embody the risk-based approach, such as Article 24 on responsibility of the controller and Article 35 on data protection impact assessments (DPIAs). We suggest dividing the text of Article 25.1 into five elements. In the following sections we analyse these elements using literal interpretation and synthesising relevant scholarly contributions and opinions of regulators (in particular WP29). The five elements of the DPbD obligations under the GDPR include the following:

1. A positive obligation of the controller to act - he controller... shall implement appropriate technical and organisational measures;
2. Designed to implement data protection principles... and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects;
3. In an effective manner;
4. A risk-based approach - taking into account:
   - The state of the art ... of the means for processing;
   - The cost of implementation;
   - The nature, scope, context of processing;
   - Purposes of processing;
   - Risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing; and
5. At the time of the determination of the means for processing and at the time of the processing itself.

1. A Positive Obligation of the Controller to Act ('The controller… shall implement appropriate technical and organisational measures')

The obligation to implement DPbD measures pertains only to the controller of the processing activity, despite calls during the legislative process to extend the obligation to processors. Given that processors are always the ones closest to the data and the processing activity, it would have made sense to extend this obligation to them as well. Even though not addressed by the provision, precisely because processors are the ones closest to the data being processed, they will have to implement DPbD-related measures in order to support controllers' compliance with Article 25. This is a logical consequence of GDPR, which requires controllers to only use processors 'providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'.[39] Additionally, Article 83.2 of the GDPR establishing the administrative fines for non-compliance with the Regulation, provides at point d) that when deciding the amount of the fine, DPAs must take into account 'the degree of responsibility of *the controller or processor* taking into account technical and organisational measures implemented by them pursuant to *Articles 25* and 32' (*our emphasis*).

The obligation under Article 25.1 is a positive obligation to act. The core DPbD obligation of the controller is 'to implement appropriate technical and organisational measures'. This means that it is also an obligation of result. To be compliant the necessary measures must implemented and achieve Data Protection by Design.[40]

It is essential to understand the link between 'risks to rights and freedoms' and 'appropriate technical and organisational measures'. As per Hildebrandt and Tielemans, the use of the word 'appropriate' implies the contextual and dynamic nature of Article 25 and the principle of Data Protection by Design.[41] In practice, this means that what is appropriate changes and depends on the identified risk. Controllers are responsible for identifying risks associat-

38 For a differentiation between the right to privacy and the right to the protection of personal data see, for instance, Christopher Docksey, 'Four fundamental rights: finding the balance' (2016) 6(3) International Data Privacy Law 195-209; Paul De Hert and Serge Gutwirth, 'Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action' in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer Science 2009).

39 GDPR, art 28.1.

40 For a differentiation between obligations of result and obligations of best efforts, see Gabriella Zanfir, 'Tracing the Right to be forgotten in the short history of data protection law: The 'New Clothes' of an Old Right' in Serge Gutwirth et al (eds), *Reforming European Data Protection Law*(Springer 2013) 227-249.

41 Hildebrandt and Tielemans (n 31).

ed with the processing. They also have the discretion to choose the appropriate technical and organisational measures. What appropriate technical and organisational measures could include is also discussed in the context of security obligations (Article 32 GDPR), yet the exact meaning of this phrase in the context of DPbD principle is not wholly clear.[42] In principle, controllers are allowed to choose the measures they consider appropriate for the purposes of Article 25. The Regulation helps with providing an example of such an appropriate measure under Article 25.1 — pseudonymisation.[43] Additionally, Recital 78 enumerates other measures that can be taken for the purposes of both DPbD and DPbDf '*inter alia*' (*our emphasis*): 'minimising the processing of personal data', 'transparency with regard to the functions and processing of personal data', 'enabling the data subject to monitor the data processing', 'enabling the controller to create and improve security features'. But the controller is not under an obligation to use these specific measures, as they are only indicated as examples. The GDPR prescribes an obligation for technical measures for processing operations. It is not important which technical measures are implemented, as long as they are appropriate to achieve the intended result[44] — respond to the risks arising from the processing activities.

a. Technical and Organisational Measures

Some useful guidance in terms of what could constitute appropriate technical and organisational measures for the purposes of DPbD was published by the European Union Agency for Network and Information Security (ENISA) in January 2015[45]. For instance, ENISA recommends eight privacy design strategies, accompanied by operational design patterns, building on the work of Hoepman[46]. The ENISA study also includes examples of certain technical and organisational measures that could be specific for DPbD obligations, without any effect whatsoever on data security or data breaches.[47]

While it can be argued that the 'appropriate technical and organisational measures for security' under Article 32 GDPR and the 'appropriate technical and organisational measures for DPbD' under Article 25.1 cannot be differentiated, the fact is that the legislator did not give any indication that this should be the case. On the contrary, the measures referred to under Article 32 GDPR are given as example specifically to achieve the purpose of ensuring security of processing. For instance, they refer to tools reducing probability of cyber threats, restoring the availability of systems in case of a physical incident or to ensuring the 'resilience' of systems [Article 32.1 (b) and (c)] — measures from data security handbooks[48]. Even with providing such detailed examples, the legislator leaves it open to the controller (and to the evolution of IT and of privacy engineering) to use other measures, by specifying that the examples provided are relevant 'inter alia'. The same goes for Article 25.1, where the legislator only refers to one example — pseudonymisation, leaving the measures to the choice of the controller, but only as long as they are 'appropriate' to achieve the result of Data Protection by Design and provided they actually achieve it (*obligation of result*). A measure can be both technical and organisational. For example, considering the way the GDPR defines 'pseudonymisation', it implies that pseudonymisation has not only to be technically implemented in data protection systems, but also to result in organisational measures, such as management of access rights for the personnel that has access to the key of the pseudonymised data.[49]

42 The GDPR in art 24 (the responsibility of the controller) requires that appropriate technical and organisational measures are 'reviewed and updated where necessary'.

43 Recital 28 of the GDPR notes that 'the application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations'.

44 See s III.2 of this article.

45 ENISA, 'Privacy and Data Protection by Design - from privacy to engineering' (Report, 2014) ('ENISA Report').

46 Jaap-Henk Hoepman, 'Privacy design strategies' (Proceedings, ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, 446–459).

47 In fact, it is in the interest of controllers to implement appropriate technical and organisational measures (and be able to demonstrate that) as this may reduce their obligations in certain situations. For example, if a controller can prove that it has taken appropriate technical and organisational measures to the risk of the data processing, then it is no longer obliged to contact individuals' whose personal data was subjected to a data breach (even though this breach may have resulted in a high risk to the rights and freedoms of natural persons).

48 See, for instance, NIST, 'Framework for Improving Critical Infrastructure Cybersecurity' (2014) Version 1.0, 9, 21, and subcategory ID.BE-5 of the Framework.

49 GDPR, art 4(5): 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.

2. 'Designed to implement data protection principles... and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects'

If the positive obligation of the controller to implement appropriate technical and organisational measures lies at the heart of DPbD, then the requirement for these measures to be 'designed' in such a way that they 'implement data protection principles' and they 'integrate the necessary safeguards into the processing' activity can be considered to provide quality requirements, sometimes referred to as non-functional requirements. This obligation should be executed with the purpose to 'meet the requirements of this Regulation' (GDPR) and to 'protect the rights of the data subject'. This is a longer, complicated way to convey a message than saying that *the appropriate measures must be designed to ensure compliance with the GDPR*.

Looking at this DPbD obligation in its bare state, beyond the plethora of words, reveals that the weight of the entire Regulation was put on the shoulders of Article 25.1[50]. Specifically, the appropriate measures must address: (i) the data protection principles as listed in Article 5 of the GDPR; (ii) the rights of the data subject and (iii) the requirements of the GDPR, in general.

The data protection principles recognised in the GDPR and referred to in Article 25.1 are lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability[51]. While the wording of Article 25.1 only specifically gives the example of data minimisation ('such as data minimisation'), it is clear from the general formulation 'implement data protection principles' that the appropriate measures must refer to all the data protection principles recognised in the GDPR.

The principle of data minimisation seeks to ensure that personal data processing is limited only to the amount of data that is strictly necessary to attain the purpose(s) of the processing. Indeed, this principle can easily be achieved by embedding technical measures in the processing activity. Guidance issued by the German DPAs further specified data minimisation has to be proactively applied:

> [s]tarting with the design of information technology by the manufacturer and its configuration and adaptation to the operating conditions, to its use in the core and auxiliary processes of the operation, for instance in the maintenance of the systems used; from the collection of personal data, through its processing and use, to its erasure or complete anonymisation; throughout the entire lifecycle of the data.[52]

This means that when the DPAs recommend implementing the data minimisation principle through the entire lifecycle of the data, they refer to the configuration of systems and their 'adaptation' to the specific operating conditions of a certain processing activity, indicating that this must be an ongoing process.

The appropriate measures adopted by controllers under Article 25.1 must also 'integrate necessary safeguards' to protect the rights of the data subject. Both technical and organisational measures must be taken in order to integrate necessary safeguards for protecting the right to information (notice), the right of access, the right of erasure (to be forgotten), the right to restriction of data, the right to data portability, the right to object and the right not to be subject to profiling and automated decision making. In practice, at the moment of setting up a processing activity (see Section III.5), the controller must already acknowledge all the different types of rights individuals will have with regard to that activity. At the same time, the controller must already envision mechanisms to provide transparency towards the data subject and to provide control to the data subject over their own data, within the limits of the Regulation.

Finally, Article 25.1 also refers to integrating necessary safeguards 'to meet the requirements of this

50 Recital 78 solidifies this conclusion by using a general statement: 'The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken *to ensure that the requirements of this Regulation are met*', followed by the recognition that 'in order to be able to *demonstrate compliance with this Regulation*, the controller *should adopt internal policies and implement measures* which meet in particular the *principles of Data Protection by Design and data protection by default*' (*our emphasis*).

51 GDPR, art 5.

52 Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016, 'The Standard Data Protection Model. A concept for inspection and consultation on the basis of unified protection goals' (2016) 10.

Regulation'. This general formulation is meant to cover all the other GDPR requirements than the ones that result from Article 5 and Chapter III. It would be futile to enumerate them all here. What is important is to acknowledge that when an organisation has the intention to use personal data in any way it is obliged to visualise the processing activity in detail, to consider all GDPR requirements and, most importantly for the purposes of Article 25.1, to put in place both technical and organisational measures that integrate safeguards into the envisaged activity in order to ensure compliance with the GDPR.

3. 'In an effective manner'

Effectiveness, whose literal meaning is 'producing a decided, decisive, or desired effect'[53], is at the core of the GDPR and it relates to the proportionality principle. The ultimate goal of 'effectiveness' in the context of data protection is to ensure 'effective protection of personal data throughout the Union'.[54] The Court of Justice of the EU (CJEU) has given a significant weight to the principle of effectiveness in data protection, when it was called to interpret EU data protection law. For instance, provided that the underlying goal of Directive 95/46/EC was to ensure effective and complete protection of personal data, the CJEU interpreted the notion of 'data controller' to also include an internet search engine, in Case C-131/13 *Google v AEPD*.[55]

Many principles are designed to be adapted to the specific organisation processes and structures having in mind specific features of data processing systems and digital assets used for supporting them. It can be argued that Article 25 borrows the term 'effectiveness' from the risk management school. Even if this term is highly contested, it can be expected that it will allow challenging controllers' claims over appropriate technical and organisational measures. Automated, semi-automated or manual controls have to be installed directly inside processes and systems that involve personal data. In this context, the effectiveness principle becomes a parameter for understanding, measuring and demonstrating[56] if controls are properly designed for adapting general data protection principles in specific systems or processes.

Reflecting on additional information provided in Recital 78, when measuring effectiveness, the following questions could be asked: how are personal data processed for ensuring that processing activities are conducted lawfully, fairly and in a transparent manner in relation to the data subject? How are personal data collected for being fully linked to specified, explicit and legitimate purposes and for not being further processed in a manner that is incompatible with those purposes? How are personal data collected and processed for being adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed? How does the controller ensure that personal data are accurate and, where necessary, kept up to date? How does the controller verify that personal data are kept in a form which permits identification of data subjects for no longer than what is necessary for the purposes for which the personal data are processed? Which specific measures the controller has put in place for ensuring that personal data are processed in a manner that ensures appropriate security of the personal data? Answers to these questions have to be evaluated on effectiveness criteria in order to understand where further improvements are necessary. Certainly, measuring effectiveness will be contextual and will depend on the nature, context and scope of the processing. Moreover, it requires a professional judgement made by data protection experts, including both legal and technical experts with risk management skills. A model for the measurement of the effectiveness is highly likely to morph out from business best practices and to be then approved by DPAs inside data protection certification mechanisms,[57] as defined by Articles 24, 25.3 and 42 GDPR. While this may have some advantages, we should consider the role that data subjects and DPAs should play with a view of evaluating effectiveness of appropriate technical and organisational measures.

53 Merriam-Webster Dictionary <https://www.merriam-webster.com/dictionary/effectiveness> accessed 26 April 2018.

54 GDPR, recital 11.

55 Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] EU:C:2014:317, para 34.

56 This concept is strictly related to the Accountability principle as defined in art 5, para 2 of the GDPR.

57 For example, the International Organization for Standardization has drafted several international standards related to privacy in information technologies (such as the ISO/IEC 29100:2011). Such standards that still need to be refined with privacy countermeasures and scale for assessing the effectiveness of controls to be taken into consideration 'at the time of the determination of the means for processing and at the time of the processing itself'.

Ultimately, in terms of enforcement, the requirement that the DPbD technical and organisational measures must be *effective* will be the one that allows supervisory authorities to measure compliance with DPbD obligations[58]. It is also the legal requirement that indicates the DPbD obligation is one 'of result' and not one of 'best efforts'.

4. Risk-based Approach

Article 25.1 requires controllers to consider and develop knowledge about different elements embedded in the DPbD principle when designing specific data protection safeguards and when monitoring the data processing operation. WP29 noted that '[t]he so-called 'risk-based approach' is not a new concept' since it was already well-known under Directive 95/46/EC.[59] WP29 suggested that rudiments of risk-based approach can be found in Articles 17 and 20 of Directive 95/46/EC, respectively addressing security obligations and the DPA prior checking procedure. As per Gellert, who builds on the school of regulatory scholars, namely Black and Baldwin, the risk-based approach is knowledge intensive and requires to explore risks associated with different elements, in particular the nature, scope, context of the processing.[60] In particular Gellert, suggests that two elements, namely '[k]nowledge and the collection thereof play a central role to any activity concerned with managing risk'.[61]

In more practical terms, it could be suggested that 'taking into account' requires controllers to engage in a thought exercise and enquire into different elements associated with the processing that may trigger a certain risk (eg, context and nature of personal data, risks to rights). To this end, controllers should consider different scenarios that could play out as a result of the processing of personal data. As a first step, in this case would be the exercise during which a controller would generate knowledge about the processing (eg, define purpose(s) of the processing and types of data that are needed to attain the foreseen purposes). We suggest that 'taking into account' as a good practice would not only include weighing all the elements that are listed in Article 25 but also the documentation obligation foreseen in Article 30 of the GDPR.

Article 30 requires that controllers or their representatives 'maintain a record of processing activities under its responsibility'.[62] This record should include information relevant for the processing of personal data, such as the name and contact details of the controller, the purposes of the processing; a description of the categories of data subjects and of the categories of personal data; the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; and if possible it should also include a general description of the technical and organisational security measures.[63] This obligation is applicable only to certain controllers. In particular, Article 30 foresees that record keeping obligations do not apply to an entity employing fewer than 250 persons. This limitation is conditional and applies only if the foreseen processing is not likely to result in a risk to the rights and freedoms of data subjects. While making a decision with regard to the documentation of data processing operations as well as data governance controller should consider (eg, to keep documentation of a certain decision) that this may ease the obligation to demonstrate that processing is performed in compliance with the GDPR foreseen in Article 24 on the responsibility of controller.

a. 'The state of the art…of the means for processing'

In the most literal sense, the 'state of the art' means 'the level of development (as of a device, procedure, process, technique, or science) reached at any particular time usually as a result of modern methods'.[64] For example, the latest version of a smartphone can be considered to be the be state of the art, meaning that it includes the latest available technology.

---

58 Recital 11 GDPR promoting effective data protection, also refers to effective enforcement as a component of it.

59 Article 29 Data Protection Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' (2014) WP218 (Article 29 Working Party, 'Statement on the role of a risk-based approach').

60 Raphael Gellert, 'Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative' (2015) 5(1) International Data Privacy Law 15.

61 ibid, 7.

62 GDPR, art 30.1.

63 ibid.

64 Merriam-Webster Dictionary <https://www.merriam-webster.com/dictionary/state%20of%20the%20art> accessed 26 April 2018.
.

In the context of Article 25 of the GDPR, we recognize that elements included and tamed within the risk-based approach, such as 'state of the art', are of a contextual nature. We suggest that 'the state of the art... of the means for processing' imposes a quality requirement within management of uncertainties related to the processing of personal data. We are inclined to argue that 'the state of the art' should not be regarded as a vague concept, but rather as a benchmark requiring controllers to explore the most recent developments and knowledge associated with data processing. This may include technical solutions and organisational practices. Gathering knowledge and information about the 'state of the art' requires controllers to keep up to speed with various relevant developments in various fields, such as standardization (eg, regional or international standards), technology (eg, software and hardware solutions), cybersecurity (eg, data vulnerabilities, cyber threats), and research techniques (eg, medical research or biobanking). It can be suggested that this exercise of getting updated constitutes the learning or the 'collection' phase.[65] This phase provides controllers with discretion to choose which available measures in the market are the best suited (appropriate to the risk level) for their particular case of personal data processing. As the 'taking into account' criteria has to be fulfilled at the inception of the processing, thus prior to processing, as well as at its later stages, we deem that the 'collection' phase has to be exercised on a regular and continuous basis.

b. 'The cost of implementation'

Obviously, 'the cost of implementation' requires controllers to consider costs associated with the state of the art of organisational and technical measures available in the market for their foreseen processing operation. Different types of personal data processing as well as different contexts in which the processing takes places may require deploying different organisational and technical measures/features that are available in the market. While considering appropriate measures controllers should go beyond the merely cost-benefit analysis and consider measures that are proportionate to the risks associated with the processing of personal data and controllers' available resources. The GDPR does not require controllers to spend a certain percentage of the investment on 'appropriate' organisational and technical measures. The exact amount that is invested in these measures should depend on the nature, scale, context of the processing as well as on information sets that are going to be processed. Some suggest that this amount should reach about 37% of the expected loss that could result from a cybersecurity breach, but in practice, unfortunately it is much lower.[66]

c. 'The nature, scope, and context of processing'

When determining appropriate technical and organisational measures, Article 25 GDPR requires to consider *the nature* of a particular data processing operation. This phrase is used on several instances in the GDPR but it is not wholly clear what 'the nature of the processing' stands for. The first reference to the nature of processing can be found in Article 20 of the Data Protection Directive, which foresaw that prior checking should be carried out not only where specific risks to the rights and freedoms of data subjects are anticipated but also where Member States adopt legislative acts governing the nature of the processing.[67] Then, WP29, in its statement on a risk-based approach, explained that 'due regard [has to be paid] to the nature and scope of such processing' as the two elements constitute an integral part of the application of data protection principles.[68] WP29 also noted that the two 'are inherently scalable'.[69]

There is a difference between the concepts 'nature of processing' and 'nature of data'. The latter requires controllers to consider what type of data they process. In principle, the GDPR follows the same rationale embedded in the Data Protection Directive - all personal data can be divided into two categories: personal data and special categories of personal data.[70] It is considered that determining the nature of the

65 Gellert (n 61).

66 Lawrence A Gordon, Martin P Loeb and Lei Zhou, 'Investing in Cybersecurity: Insights from the Gordon-Loeb Model' (2016) 7(2) Journal of Information Security 49-59.

67 Directive 95/46/EC, art 20.

68 Article 29 Working Party, 'Statement on the role of a risk-based approach' (n 60).

69 ibid.

70 The GDPR clarifies the concept of 'personal data' by including references to an identification number, location data, an online identifier and genetic identity. At the same time, the GDPR introduces new/different types of personal data, including genetic data, biometric data, and data concerning health. Determining the sensitivity of personal data is a key factor when choosing appropriate organisational and technical measures.

data is significant when determining the context of the processing.

Therefore, we are inclined to believe that the nature of the processing refers to the intrinsic features of the processing. In other words, the nature of the processing requires to consider the way processing of personal data is carried out. To determine the nature of the processing the controllers could raise the following questions: what means are used for the processing operation (eg, automated)? Is the processing going to result in profiling of individuals that will allow evaluating the personal aspects relating to an individual whose data are being processed? Are there any third parties that are included in the processing? Is the processing carried out by a cloud-based infrastructure? Does the processing include aggregation of data sets? Is the processing activity performed outside the EU?

The scope requires to consider the amount of data that is going to be processed.[71] It is an important consideration to make because its findings may result in additional obligations. For example, in cases where the processing of personal data may include large scale processing of special categories of data, the controller is obliged to conduct a DPIA. While recognizing that anticipating or knowing the scope of the operations may be difficult to know before launching the processing (eg, in case of a new app), we think that controllers should consider various scenarios *a priori*.

The ambiguity embedded in the word 'scope' allows for its different interpretation. In particular, one can consider the term 'scope' to be very close to the term 'context' of the processing activities. This viewpoint forces the data controller to consider the environment where personal data are processed. For example, it might be noted that different requirements, and obligations apply for household activities or in open information environments, in different material[72] or territorial[73] scopes or in public or private entities due to different level of risks. Therefore, we suggest that the 'scope' forces the data controllers to consider the processing activities from a holistic point of view taking into account various environmental aspects.

The context in which the processing takes place is also of great relevance when determining what are appropriate technical and organisational measures. For example, in situations where 'the core activities of the controller or the processor consist of processing operations [...] which require regular and systematic monitoring of data subjects on a large scale' controller (as well as processors) are required to appoint a Data Protection Officer (DPO).[74] In other words this means, that in case of large scale surveillance systems, controllers should appoint a DPO. WP29, in its Opinion 8/2010 on applicable law, explained that context of the processing is determined by the nature and place of normal activities and 'not the place where data are sent or located'.[75] Other details crucial for the context could include: an employment situation, the processing of children's data or health related data. These contextual details may raise the bar for the appropriate technical and organisational measures in comparison to processing operations in other sectors or contexts.

The three elements, namely the scope, nature and context should always be considered cumulatively in order to determine the context of the processing.[76] These elements are contextual and they complement each other and to some extent they overlap. For example, eGovernment applications or cloud based solutions may provide certain nature of the processing as well as allow for rather precise estimates about the scale of the processing, such as the processing on the cloud based solutions can be easily scalable whereas eGovernment services will aim at processing personal data of citizens and residents of a particular country or region. The processing that entails pseudonymised data may provide for specific nature or context of the processing. As the three elements are not cut in stone and may change throughout the processing operation, they need to be (re)evaluated on a regular basis. ENISA suggests focusing on one of these elements when developing a data processing strategy.[77]

71 For example, see: Article 29 Data Protection Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679' (2018) WP250rev.01, 33.

72 GDPR, art 2.

73 GDPR, art 3.

74 GDPR, art 37.1(b).

75 Article 29 Data Protection Working Party, 'Opinion 8/2010 on applicable law' (2010) WP179, 16.

76 Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' (2017) WP 248 rev.01, 17.

77 ENISA Report (n 46).

d. 'Purposes of processing'

When determining appropriate technical and organisational measures controllers should consider what is the purpose of the processing and why this processing activity is necessary. Article 5.1(b) of the GDPR requires controllers to ensure that personal data are 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes'. Consequently, purpose specification is considered to be the cornerstone of the EU data protection framework. WP29 in its Opinion on purpose limitation has further explained that the purpose of the processing has to be clear, specific and at the same time to provide relevant details of the processing..[78] It has also deduced that identification of purposes of the processing is a precondition for the identification of appropriate safeguards, including technical and organisational measures. Furthermore, WP29 argued that by defining purposes of the processing, the controller submits himself to the law and limits the use of the collected data.[79] WP29 recommended that the internal purpose specification process is documented.[80]

e. 'The risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing'

The use of the term 'risk' sparked discussions on its meaning within the GDPR among different stakeholders, including practitioners, policy makers, academics, engineers, and representatives of data protection authorities as well as civic society organisations. The GDPR in Articles 23 – 31, that outline general obligations (ie, Sections 1 of Chapter IV), refers to 'risks' in general. Whereas in the subsequent Articles 34, 35 and 36 the GDPR refers to 'high risks'. This differentiation is significant because it means that any processing of personal data should be subject to the principles of Data Protection by Design and Default. Only processing that entails high risk requires to conduct a DPIA.[81] Following up on this observation, we deduce that 'the risks of varying likelihood and severity' in Article 25 refer to any risks arising from the processing of personal data.[82]

Black has observed that regulating risks as well as regulators' attempts to mitigate risks have become common practice, even though there is no common understanding of the term 'risk'.[83] Not surprisingly, the GDPR also regulates several aspects of the protection of the right to personal data protection 'through' risk. However, there is little consensus about how to define risk of the processing. While some scholars suggest that risk can be put in certain formulas and expressed as objective and subjective risk,[84] it seems that Article 25 builds on Slovic's observations that 'risk does not exist 'out there', independent of our minds and cultures, waiting to be measured'.[85] In particular, it requires considering the impact of the personal data processing operations to individuals' rights and freedoms.

Perhaps what is the most important here is to understand that the concept of 'risk to the right' can be approached from different perspectives and dimensions. For example, van Dijk et al argue that the different modalities of 'risk to the right' include: 1) governmental perception of risk vs. right; 2) organisations' perception of a right as a risk; 3) case law striking balance between different rights and risks, usually on the basis of the proportionality principle; and 4) risk perception by civil society or the general public at large.[86] Van Dijk et al also suggest that the perception of risk should be based on the commutative understanding of different risks as relying on a par-

78 Article 29 Data Protection Working Party, 'Opinion 03/2013 on purpose limitation' (2013) WP203.

79 ibid.

80 ibid.

81 Art 35 of the GDPR also provides further specification as to the meaning of 'high risks'.

82 Paul Slovic and Elke U Weber explain that risk can be understood in the following way: 1) risk as a hazard: 'Which risks should we rank?', 2) risk as probability: 'What is the risk of getting AIDS from an infected needle?', 3) risk as consequence: 'What is the risk of letting your parking meter expire?', 4) risk as potential adversity or threat: 'How great is the risk of riding a motorcycle?'.

83 Julia Black, 'The role of risk in regulatory processes' in Robert Baldwin, Martin Cave, and Martin Lodge (eds), *The Oxford Handbook of Regulation* (Oxford University Press 2010).

84 Following Knights' seminal work in finance theory dating from 1920s, risk is conventionally measured according to the following formula: Risk = Impact (ie, magnitude of adverse consequences)*Perceived probability. Also see Baruch Fischhoff, Stephen Watson and Chris Hope, 'Defining risk' , (1984) 17(2) Policy Sciences 123. Based on Black ibid. Adrian Munteanu, 'Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma. Managing Information in the Digital Economy: Issues & Solutions' (Proceedings of the 6th International Business Information Management Association (IBIMA) Conference, 19-21 June 2006) 227-232 <https://ssrn.com/abstract=917767> accessed 16 April 2018.

85 Paul Slovic and Elke U Weber, 'Perception of Risk Posed by Extreme Events' (Center for Decision Sciences (CDS) Working Paper Columbia University, 2002).

86 Niels Van Dijk, Raphaël Maurice Gellert and Kjetil Rommetveit, 'A risk to a right? Beyond data protection risk assessments' (2015) Computer Law & Security Review: 1-21.

ticular approach, eg, scientific or technical knowledge, may represent a limited or biased understanding of risks.[87] This interpretation aligns with the scholarly literature studying risk perception.[88]

More clarification on the phrase 'risk to a right' is brought by WP29. In its document explaining a risk-based approach, WP29 notes that

> risks, which are related to potential negative impact on the data subject's rights, freedoms and interests, should be determined taking into consideration specific objective criteria such as the nature of personal data (e.g., sensitive or not), the category of data subject (e.g., minor or not), the number of data subjects affected, and the purpose of the processing.[89]

WP29 highlights that while the phrase 'rights and freedoms', primarily concerns the rights to privacy and protection of personal data of individuals, controllers should take into account other rights that may be crammed by the processing.[90]

4. 'At the time of the determination of the means for processing and at the time of the processing itself'

The positive obligation in Article 25.1 must be executed 'at the time of the determination of the means for processing and at the time of the processing itself'.[91] This means that, in practice, controllers are required to consider the principle of Data Protection by Design throughout the data management cycle. First, controllers must take appropriate technical and organisational measures to implement the principle of Data Protection by Design at the time of making a decision about the launch of a system and its security measures. Second, they will have to do so also at the later stages, throughout the processing activity. Therefore, controllers should consider obligations arising from DPbD also after the processing has been initiated. This, to some extent, further strengthens DPbD as a general principle that applies to future as well as ongoing data processing operations. It can be speculated that the regulators opted in for this wording to ensure that controllers that have personal data processing operations running still consider and adhere to this principle.

Furthermore, the 'taking into account' element of DPbD reflects the proportionality principle, which inherently provides for flexibility as regards the outcomes. Indeed, many of the elements included in the risk-based approach require analysing the context of processing which may be subject to change under different circumstances.

5. Interim Conclusion

On the one hand, this section has 'demystified' the DPbD principle by deconstructing it into enforceable elements, but on the other hand, it showed how complex complying with DPbD obligations (and ultimately enforcing them) can be in practice. Our analysis demonstrated that, in a way, the entire weight of the GDPR rests on the 'shoulders' of Article 25.1. This does not, however, mean that complying with the requirements of the GDPR suffices to be DPbD compliant. But it could mean, theoretically at least, that complying with the DPbD principle is the key for the GDPR compliance in general.

We argued that essentially, Article 25.1 entails a positive obligation to act for the controller, in the sense of implementing both state of the art *organisational* and *technical* measures, to ensure that the *requirements of the GDPR* are *embedded in the processing activity*, in an effective manner (it is also an obligation of result), both at the time of initiating the processing activity and throughout it. The controller has to do so by taking into account the nature, scope and context of processing and other criteria detailed in the provision. The analysis also pointed out that, while not directly liable under Article 25.1, processors will have to comply with DPbD obligations by virtue of the nature of their activity and as a consequence of their obligations under Article 28 of the GDPR.

The controller (and, where applicable, the processor) has the freedom to choose appropriate technical

87 ibid.

88 Donald MacGregor and Paul Slovic, 'Perceived acceptability of risk analysis as a decision-making approach' (1986) 6(2) Risk Analysis 245–256, 218; Paul Slovic, 'Informing and educating the public about risk' (1986) 4 Risk Analysis 403–415; Paul Slovic, Baruch Fischhoff and Sarah Lichtenstein, 'Why study risk perception? (1982) 2 Risk Analysis 83–93.

89 Article 29 Working Party, 'Statement on the role of a risk-based approach' (n 60).

90 ibid.

91 GDPR, art 25.

and organisational measures, as long as they are adequate and effective in achieving objectives of DPbD. We argued that, in any case, 'the appropriate technical and organisational measures' under Article 25.1 GDPR may very well be different than the ones required by Article 32 GDPR.

Our observations allow concluding that indeed, in order to implement the principle of Data Protection by Design, controllers have to be proactive and evaluate risks of the processing operation as well as continuously learn about developments in the field of personal data protection. We agree with Irion and Luchetta who noted that the DPbD as a 'solution has the charm' by emphasizing that 'with the increasing sophistication of the processing of personal data, controllers can also be expected to take more advanced steps to ensure compliance'.[92] When implementing this principle the main challenge will be the establishment of meaningful thresholds for a risk-based regulation as it entails numerous interdependent elements.[93]

In the sense that DPbD further strengthens the core principles set forth in Article 5 of the GDPR, we also agree with Gellert who suggests that the principle of Data Protection by Design has been introduced not only to manage the risk inherent in the processing operations, but also to overcome shortcomings of the traditional EU data protection principles.[94] Lastly, partially in line with the van Dijk et al suggestion that 'privacy-by-design or data protection-by-design of which the latter is introduced in the proposed Data Protection Regulation as the follow-up of the data protection impact assessment and based on its results', we argue that the principle of Data Protection by Design should be seen in the continuum of the other legal obligations stemming from the GDPR.[95]

IV. Data Protection by Default

1. Two Interrelated yet Distinct Concepts: Data Protection by Design and Data Protection by Default

Before delving into Article 25.2 of the GDPR, it is necessary to draw a line between the legal concepts of Data Protection by Design and Data Protection by Default. The text of the GDPR is of little help in this respect.

The legislator uses the phrase 'principles of Data Protection by Design and by Default' in the text of the GDPR without differentiating between the two legal obligations.[96] Recital 78 provides an explanation of the DPbD principle as well as the stages during which it should be considered and then refers to the applicability of the principles of Data Protection by Design and by Default in the context of public tender, even though there has been no elaboration on the Data Protection by Default principle. Only in Article 25 of the GDPR, the regulator draws a distinction between the two concepts, respectively in paragraphs 1 and 2.

The concepts of Data Protection by Design and Data Protection by Default are interrelated but carry a different meaning.[97] Data Protection by Design refers to the *design and existence of embedded safeguards and mechanisms* that protect the right to data protection throughout the lifecycle of the application, service or product, as discussed above. Data Protection by Default refers to the *implementation of such safeguards as a default setting*. In its Opinion on the utilisation of drones, the WP29 suggests that adopting data protection and privacy by default would entail choosing privacy settings on services and products 'which by default avoid the collection and further processing of unnecessary personal data'.[98] The EDPS has rightly underlined that while the 'by design' element refers to integration of data protection 'from the very inception of new products and services that entail the processing of personal data', the 'by default'

92 Kristina Irion and Giacomo Luchetta, 'Online personal data processing and EU data protection reform: Report of the CEPS Digital Forum' (2013) 23 <https://www.ivir.nl/publicaties/download/TFR_Data_Protection.pdf> accessed 9 February 2018.

93 ibid.

94 Raphael Gellert, 'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection' (2016) 2(4) EDPL 481-492.

95 Van Dijk, Gellert and Rommetveit (n 87).

96 GDPR, recital 78.

97 While the GDPR implies that DPbD and DPbDf are two distinct legal obligations, the principles of PbD and PbDf were not treated as distinct concepts from their inception. For instance Cavoukian considers Privacy by Default ('as default setting') as one of the foundational principles of Privacy by Design. Ann Cavoukian, 'Privacy by design. Take the challenge.' (Information and privacy commissioner of Ontario, 2009).

98 Article 29 Data Protection Working Party, 'Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones' (2015) WP231, 14.

element refers to the selection of the most privacy friendly configuration by default.[99] Similarly, according to ENISA, Data Protection by Default 'means that in the default setting the user is already protected against privacy risks' and 'this affects the choice of the designer which parts are wired-in and which are configurable'.[100]

There are different interpretations of the relationship of the DPbD and DPbDf. Bygrave treats DPbDf as an extension of the DPbD duty, namely, as a duty to ensure 'default application of particular data protection principles and default limits on data accessibility'.[101] Costa and Poullet assign a greater role to the obligation of Article 25.2, as they see DPbDf as a powerful instrument with broad spectrum that gives EU citizens back control over the use of their personal data.[102] The two authors argue that in the context of social networks, implementation of the Data Protection by Default principle would entail keeping individual profiles private by default.

Data Protection by Default presupposes Data Protection by Design mechanisms.[103] Interestingly, the same may not hold true *vice versa*. For example, a web-browser can be a means to limit (to some extent) online tracking of Internet users by designing data protection friendly settings, such as the automatic deletion of cookies and web-browsing history after a session is closed, or by sending a Do-Not-Track signal to web-content providers and advertisers. The design and development of such mechanisms are linked to Data Protection by Design. The mere existence of such settings however does not mean that the principle of Data Protection by Default is implemented, unless the data protection friendly settings are activated by default. In that sense, 'by default', to some extent is dependent on Data Protection by Design mechanisms, whereas Data Protection by Design, is independent of default settings.

In practice, since both principles are legal obligations under Article 25 GDPR, the controller would need to comply with both DPbD and DPbDf. However, the lack of definitions and a formalised distinction of the two concepts in the text of the GDPR might give rise to questions regarding granularity ('does one-size-fit-all approach' work?), the question of wired-in functionality or configurable settings[104] and in general diverse interpretations leading to legal uncertainty for controllers on the exact content of their legal obligations stemming from Article 25 GDPR.[105]

2. Data Protection by Default in the GDPR

The legal obligation of Article 25.2 of the GDPR requires data controllers to implement measures that would *by default* ensure that only data that are necessary for specific purposes are processed.[106] DPbDf is a relevant concept to 'privacy by default', but as explained in the previous section, the difference lies in the subject matter of the protection. While 'Data Protection by Default' focuses on the right to protection of personal data, 'privacy by default' seeks to secure individuals' (or group) privacy.[107]

a. Default Rules and 'Active Choosing'

The concept of 'by default' protection relates to the scholarship of default rule-setting and choice architecture. On many occasions of our everyday lives, regulators, service providers, and other entities already make many choices that concern individuals (also referred to as citizens, consumers or end-users). Such entities that are in a position to devise default rules

99 European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on a proposal for a Directive of the European Parliament and of the Council on payment services in the internal market amending Directives 2002/65/EC, 2006/48/EC and 2009/110/EC and repealing Directive 2007/64/EC, and for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions' (2013) 4.

100 ENISA Report (n 46) 11.

101 Bygrave (n 5).

102 Luiz Costa and Yves Poullet, 'Privacy and the regulation of 2012' (2012) 28(3) Computer Law & Security Review 254-262.

103 This premise has also been supported by the WP29 in the Opinion 01/2015 which provides that 'the application of data protection by default measures entails that, beforehand, the principle of data protection by design is respected by manufacturers and operators' (n 99) 14.

104 Read for instance Marit Hansen's work, which raises such questions in Marit Hansen, 'Data Protection by Default in Identity-Related Applications' (2017) <https://hal.inria.fr/hal-01470500/document> accessed 5 June 2018. Simone Fischer-Hübner, Elisabeth Leeuw and Chris Mitchell, 'Policies and Research in Identity Management' (3rd IFIP WG 11.6 Working Conference, IDMAN 2013, London, UK, 8-9 April 2013) 4-17.

105 ibid.

106 GDPR, art 25.2.

107 An example of how by default settings protect group privacy is the case of a group of individuals using the same device to access the Internet. In some cases the individuals cannot be singled-out. However their right to privacy still needs to be safeguarded and default privacy-friendly settings can provide such safeguards. Read further on the concept of group privacy: Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds) (2016). *Group privacy: New challenges of data technologies* (vol 126, Springer 2016).

are called *choice architects*.[108] An example of a default rule could be a pension scheme, to which the employer signs up its employees. Usually, the employee has a possibility to make a different choice, but as a starting point (ie, by default), an option has already been made by his employer on his behalf. On the opposite side of default rules, lies *active choosing*. Active choosing requires, as the term implies, a positive action from the concerned individual, which in this case needs to indicate its preference on the decision at stake.

Behavioural studies have shown that default rules tend to 'stick' because of certain reasons.[109] For example, the individuals might ignore the default rules (being idle), have no strong preference, or not sufficient knowledge to make a decision.[110] It might also be the case that concerned individuals regard default rules as suggestions or recommendations from policy makers, regulators, or service providers, who have acted as choice architects in that particular case.[111] On the other hand, active choosing may provide more freedom to the individual who has to make a choice, as there is no default rule, that might influence or even determine the choice. In addition, the obligation for active choosing, may, in principle, force the individual to educate himself before making the choice. Another argument is that in case where choice architects lack necessary information to make an informed choice, active choosing could protect individuals from erroneous choices, made by others.

b. Data Protection by Default and Active Choosing in the GDPR

Taking this discussion to the field of data protection, it can be suggested that concepts of 'default rules', 'active choosing' and 'consent' share similar considerations and characteristics. The GDPR defines consent as

> any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[112]

In practice this means that for consent to be valid, an active behaviour, such as active choosing, is necessary. In relation to the concept of default rules, those are, as mentioned in the previous section, directly related to the concept of data protection by default. The GDPR provisions regulating consent and Data Protection by Default assign different types of meaning and obligations to these concepts. Consent can serve as a ground legitimising the processing as foreseen in Article 6 of GDPR.[113] The regulator assigns legal significance to consent as a concept legitimising the processing of personal data by placing a particular weight on active choosing as a means to express one's preference with regard to the processing of his or her personal data. At the same time, consent is not the only legal ground that can ensure lawfulness of the processing. According to Article 6 of GDPR, performance of a task carried out in the public interest, legitimate interest of the controller or a third party, the protection of vital interests of the data subject, and compliance with legal obligations are the also grounds for lawful processing. These grounds lack the element of active choosing by a data subject and imply instead actions for which the decision is taken by data controllers. In such cases, the significance of Data Protection by Default is even more heightened.[114]

Considering the requirement of Data Protection by Default (Article 25 GDPR), a different type of provision is assigned. DPbDf is one of the obligations that controllers should implement once grounds for lawful processing are established. The regulator, acting as a choice architect, chose protection of personal data as a default rule, by establishing an obligation for the data controller to implement appropriate measures for the protection of the personal data of the data subjects. The choice of by default protection corresponds to the discussions on the importance to protect individuals' personal data, even if individuals take no action to ensure such protection.[115] In addition, data subjects often expect that controllers for certain services, such as eBanking or eGovernment

108 Cass Sunstein, 'Deciding by Default' (2013) 162(1) University of Pennsylvania Law Review 5.

109 ibid.

110 ibid.

111 Eric Johnson and Daniel Goldstein, 'Defaults and donation decisions' (2004) 78(12) Transplantation 1713.

112 GDPR, art 4.11.

113 Art 6 of the GDPR is one of the fundamental provisions of the GDPR, in the sense that without grounds for lawful processing, any data processing activity of the data controller is in violation of the law (GDPR).

114 This does not mean that Data Protection by Default is of less significance, when consent is the ground for lawful processing.

115 Cavoukian, 'Privacy by Design. The 7 Foundational Principles' (n 5).

services, will protect their personal data. For example, the Eurobarometer survey showed 67% of the EU citizens think that 'online companies, individuals and public authorities all have a responsibility in protecting their online personal data'.[116] It can be suggested that this belief is an intrinsic part of the EU data protection framework that *by default requires controllers to protect individuals' personal data.*

3. The Elements of DPbDf

The principle of Data Protection by Default has been anchored as a legal obligation in Article 25.2 of the GDPR. Essentially, the *controller* must implement appropriate technical and organisational measures to ensure that *by default only data which are necessary for the purposes of the processing activity are processed*, by taking into account the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

The elements of the DPbDf principle are:

a. The controller shall implement appropriate technical and organisational measures;

b. Ensuring that by default, only personal data which are necessary for each specific purpose of the processing are processed;

c. Implementing appropriate technical and organisational measures is applicable to:

- the amount of personal data collected
- the extent of their processing;
- the period of their storage; and
- their accessibility (including the goal of not making the data available to an indefinite number of persons).

a. 'The controller shall implement appropriate technical and organisational measures'

Similarly to the principle of DPbD, the entity responsible for compliance with the obligation of Data Protection by Default is the data controller. In other words a positive obligation to act rests with the controller. However, this provision is relevant for data processors as well, taking into account Article 28 of the GDPR.[117] Implementation of Data Protection by Default by the processor, could be a competitive advantage as it would help the controller comply with an obligation to implement DPbDf measures. For instance, if a controller chooses a processor who already implements DPbDf and DPbD measures, the compliance effort by controller could be reduced, or at least facilitated.

The content of the DPbDf obligation relates to the implementation of 'appropriate' technical and organisational measures, similarly to the DPbD obligation.[118] In this case, the selection of technical and organisational measures is left to the controller, as long as they are *appropriate* to achieve the legal obligation of Article 25.2 GDPR. As we see in Section IV.3.b., the purpose of these measures must be to ensure protection 'by default' of the personal data being processed, in particular with regard to the data minimisation principle. Such goal can only be achievable by engineering DPbDf in the processing operation.

b. Necessity and Data Minimisation: 'by default, only personal data which are necessary for each specific purpose of the processing are processed'

The aim of the DPbDf obligation is to ensure that processing is limited only to personal data, which are necessary for each specific purpose of processing. The provision associates 'by default' protection to the *purpose* of processing. The EDPS has commented on the *seemingly* limited scope of Data Protection by Default principle, stating that in its Commission Proposal version, it did not add much to the general principles of data processing and in specific the data minimisation principle.[119]

The question that then arises is what is the relationship of Data Protection by Default to the purpose limitation principle. And more specifically, whether

116 The second reply with also high percentage was 'You', meaning the individual itself (data subject) needs to take care of its own information. European Commission, 'Special Eurobarometer 431 Data Protection' (Report, 2015) <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf> accessed 9 February 2018.

117 See s III.1 of this contribution.

118 The analysis in s III.1 is applicable to the DPbDf provision as well.

119 European Data Protection Supervisor, 'Consultation on Reform Package'(2012) <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf> accessed 9 February 2018. The Commission proposal (2012) art 23.2 on Data Protection by Default provided: 'The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals'.

Data Protection by Default is limited to data minimisation principle or it affords a broader scope. As discussed above, Article 5.1(b) provides that personal data shall be collected for 'specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes'. Article 5.1(c) provides that personal data shall be processed for adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.

Comparatively analysing the wording of the principles outlined in Article 5 with the obligation of Article 25.2, it follows that Data Protection by Default is established as one of the (mandatory) means that allows the data controller to comply with both the principles of purpose limitation and data minimisation. Practically, this entails that controllers would need to make sure that they collect by default personal data that is adequate, relevant and limited to what is necessary, but also that the data are collected for specified, explicit, and legitimate purposes.

c. Additional Specifications for the 'Necessity' Requirement: 'the amount of personal data collected, the extent of their processing, the storage period and their accessibility'

Article 25.2 includes additional specifications on the scope of the DPbDf obligation. The conditions counterbalance what seems as a limitation of Data Protection by Default only to the data minimisation principle. The Data Protection by Default obligation applies to the amount of personal data collected, the extent of their processing, the storage period and their accessibility. Those specifications also further clarify the necessity condition of Article 25.2 ('only personal data which are necessary for each specific purpose of the processing'). In other words:

- the necessary personal data for each specific purpose will be determined in relation to the amount of data (data minimisation),[120]
- extent of their processing (purpose limitation),[121]
- period of their processing (storage limitation),[122] and
- accessibility (principle of integrity and confidentiality).[123]

Therefore, it can be argued that the purpose limitation, the storage limitation and the principle of integrity and confidentiality are equally relevant for the implementation of the DPbDf obligation, together with the data minimisation principle.

The last sentence of Article 25.2 requires that the measures taken by controllers must also ensure that by default personal data are not made accessible to an indefinite number of natural persons without the individual's intervention.[124] This condition is primarily linked to the accessibility criterion, as discussed above. The wording is nonetheless somehow unusual. Two issues arise: one is about the meaning of the *indefinite* number of natural persons. Presumably, the threats to the rights of the individuals may as well arise when processed by a definite number of natural persons, even by a single natural person. The wording 'indefinite number' at first however does not seem to reflect the aim to use protect against any kind of threat from making accessible the data. In addition, what can actually be considered as indefinite number of persons is also questionable. Can the billions of users of a popular social network be considered as 'indefinite number of natural persons', given that the social network operator may be aware of their number? Taking into account the rationale and aim of DPbDf, that is to offer by default protection to data subjects with regard to the processing of their personal data, one should not adopt the literal interpretation of the wording of 'indefinite number of natural persons', but rather read the provision as meaning the potential accessibility to the data by a number of natural persons, *larger than the data subject intended or would have reasonably expected*. The second issue is what constitutes 'intervention' by the individual. Intervention is neither defined in the GDPR nor encountered in such context in the text of the Regulation. This could lead to variety of interpretations, potentially undermining the legal obligation of DPbDf.[125]

120 GDPR, art 5.1(c).

121 GDPR, art 5.1(b).

122 GDPR, art 5.1(e).

123 GDPR, art 5.1(f).

124 Art 25.2 (last intent), GDPR, 'In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons'.

125 For example, an analogy can be made with the concept of consent in electronic communications (despite it was already defined in the ePrivacy Directive 2002/58/EC). The WP29 had to issue guidance with specific examples to clarify what constitutes consent in the context of the ePrivacy Directive. Article 29 Data Protection Working Party, 'Working Document 02/2013 providing guidance on obtaining consent for cookies' (2013) WP 208.

Intervention implies an action from the data subject, that signifies its wish to make accessible the personal data to an indefinite number of individuals. This could for example be, the changing of the default Do-Not-Track setting from No tracking to allow tracking.

4. The Ongoing Debate Over the Added Value of DPbDf

The issue of which should be the default rule in the case of data protection has been the focus of several debates. The arguments that are against such default protection originate from different standpoints, which, nonetheless, reach the same conclusion to reject data protection by default. A part of the scholarship, which supports the argument of informational self-determination argues that an individual (data subject in this case) may not exercise effectively his or her right to informational self-determination, once a choice (even one that is beneficial for its rights) is already made on his behalf.[126] Another argument against Data Protection by Default that is reiterated by industry representatives relates to the cost of implementation of privacy friendly defaults and the loss of commercial opportunities, such as tailored advertising. Nevertheless, such views on cost of implementation, originate often from the false standpoint that Data Protection by Default puts an additional burden on already existing obligations. Data Protection by Default does not however add new content to the obligations of the controllers; it only affects the *timing* of compliance; that is from the very start of data processing (alike DPbD).[127]

Arguments, in favour of Data Protection by Default mainly stem from the nature of the rights at stake. The right to protection for personal data, as enshrined in the EU Charter and the Treaty for the Functioning of the European Union, is a fundamental right in the EU which should be protected by the default settings. In addition, Data Protection by Default can potentially safeguard children, minors, elderly and other groups that can be considered to be in a weaker position than an average (adult) individual. The EDPS noted that indeed a few users know how to 'control access to the information they post, nevermind how to change the default privacy settings'.[128] Consequently it has consistently supported privacy-friendly default settings (eg, with regard to social networks[129] and RFID).[130]

The debate above preceded the discussion of the EU data protection reform, and yet the decision of the regulator was to include Data Protection by Default as a mandatory requirement for data controllers. The questions that arise relate to the implementation of the provision and its limitations. As explained above, we consider that the subject matter of the obligation as such is not *process-oriented* but rather *result-oriented* (the controller should ensure that by default only personal data that fulfill the requirements of Article 25.2 are processed). Reading the provision as stand-alone could lead to the misconception that the mere implementation of measures by the data controller would suffice to fulfil the obligation of Article 25.2 of the GDPR. However, the Data Protection by Default obligation should be read in combination with principles outlined in Article 5 of the GDPR, such as data minimisation, purpose specification and purpose limitation. Therefore, we deduce that DPbDf requires not only taking such measures, but it also focuses on their actual outcome, that is, whether they protect individuals' personal data.

5. Interim Conclusion

This section underlined the differences between the concepts of DPbD and DPbDf. It showed that Data Protection by Default is a more technical and concentrated concept.

The DPbDf principle requires the *controller* to implement appropriate technical and organisational measures to ensure that *by default only data which*

126 This argument relates to the discussion on data protection by default entailing (or not) pre-configured settings. The alternative to pre-configured settings being forcing users to configure the settings when they first use or install a system. Hansen (n 105). Leeuw and Mitchell (n 105).

127 There has also been the view that *defaults* do not work in privacy in specific see, Lauren E Willis, 'Why Not Privacy by Default?' (2014) 29 Berkeley Tech LJ.

128 European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy' (2010) <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf> accessed 9 February 2018.

129 ibid.

130 European Data Protection Supervisor (2008) 'Opinion on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'Radio Frequency Identification (RFID) in Europe: steps towards a policy framework' COM(2007) 96 [2008] OJ 101/1.

are necessary for the purposes of the processing activity are processed, by taking into account the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. We argued that while at first glance DPbDf is mainly linked to the data minimisation and purpose limitation principles, it is also equally relevant for the principles of data retention and confidentiality/accessibility.

Finally, several arguments in favour and against imposing Data Protection by Default obligations were discussed, showing that ultimately, after the adoption of the GDPR, they only remain relevant for the implementation of the provision and its limitations. The effective or ineffective implementation of Article 25.2 will ultimately show the usefulness of DPbDf obligations.

V. Concluding Remarks

Understanding that the content of the DPbD principle requires implementing GDPR-specific requirements, with a focus on data protection principles and the rights of the data subject, in the design of processing operations highlights why DPbD is different than the concept of Privacy by Design, even though their underlying objective is the same: embedding safeguards to protect the rights of individuals from the conception of a system using personal data.

In this article we analysed the concepts of Data Protection by Design and Data Protection by Default that have turned into legal obligations for controllers after the revision of the EU data protection framework. These obligations aim at ensuring integration of data protection measures throughout the lifecycle of certain processes and technologies, online services and applications that process personal data. Our analysis leads us to conclusion that - from a legal perspective - DPbD and DPbDf constitute a meta requirement system embedding the General Data Protection Regulation principles in every personal data processing operation.

We challenged the claim that the abstractness of Article 25 undermines efficiency of DPbD and DPbDf implementation by demonstrating how much is known about the elements embedded in the two concepts. Our analysis suggests that DPbD and DPbDf require implementing already existing obligations resulting from intrinsic features of personal data processing. The two principles strengthen and further reinforce the long established data protection principles and obligations, as set forth in the Data Protection Directive and reiterated and elaborated in the GDPR. Article 24 governing responsibility of controllers should be considered when implementing both DPbD and DPbDf measures. Complying with the two legal obligations also helps the data controller and the data processor in choosing and demonstrating the application of data protection principles and that the security measures are effective and appropriate.

We think that despite the promise that the lifecycle approach carries, the implementation of DPbD and DPbDf remains a challenge due to numerous elements included in both concepts. Some of these elements originate from the lack of formal distinction of the two legal obligations. A number of issues has already been explained and addressed by the EU data protection authorities within the setup of WP29. Whereas some of them, in particular the ones embodying a risk-based approach, still need further guidance. We recognize that even though a few requirements might be generalised, most of the requirements of DPbD and DPbDf principles are contextual and depend on the circumstances (ie, nature, scope and context) of each processing.

In particular, general requirements stated in the entire Regulation have to be translated in specific security measures and data protection controls. The pivot of the DPbD obligation is the specific risk assessment that has to be performed both at the time of the determination of the means for processing and at the time of the processing itself. Moreover, we pointed out that often the correct implementation of DPbD and DPbDf requires revisions in the logic involved in any automatic personal data processing activities, for the aim of designing systems and processes truly able to serve mankind[131] and not to generate threats to users' rights and freedoms.

Finally, we suggest that DPbD and DPbDf principles serve interests of both data subjects and data controllers. These principles carry potential to raise awareness of data subjects' rights and allow them to make more informed and better evaluation of data controllers and their personal data processing within various systems. For controllers (and processors)

131 GDPR, recital 4.

implementation of DPbD and DPbDf can be a competitive advantage within the Digital Single Market as well as outside the EU. At the same time, while recognizing the value of this system approach we regret that that DPbD and DPbDf address controllers and not the actual software developers or producers of hardware. Only when the latter are included in the framework, data subjects would receive comprehensive and meaningful protection of their personal data.

Future works could focus on building up a step-by-step methodology that would consider different aspects and requirements that have to be translated into specific system and process requirements.