Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements

Lee A. Bygrave[1]
Professor of Law, Norwegian Research Center for Computers and Law, Department of Private Law, University of Oslo.
l.a.bygrave@jus.uio.no

ABSTRACT:
In this paper, a critical examination is conducted of Article 25 of the European Union's General Data Protection Regulation (Regulation 2016/679). Bearing the title 'data protection
by design and by default', Article 25 requires that core data protection principles be integrated into the design and development of systems for processing personal data. The paper outlines the rationale and legal heritage of Article 25, and shows how its provisions proffer considerably stronger support for data protection by design and by default than is the case under the 1995 Data Protection Directive (Directive 95/46/EC). The paper further
shows that this strengthening of support is in keeping with jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union. Nonetheless, it is herein argued that Article 25 suffers from multiple flaws, in particular a lack of clarity over the parameters and methodologies for achieving its goals, a failure to communicate clearly and directly with those engaged in the engineering of information systems, and a failure to provide the necessary incentives to spur the 'hardwiring' of privacy-related interests.
Taken together, these flaws will likely hinder the traction of Article 25 requirements on information systems development.

Keywords
Privacy by design, data protection by design, privacy-enhancing technology, anonymisation, encryption, General Data Protection Regulation

1. Work on this paper has been conducted under the aegis of the project 'Security in Internet Governance and Networks: Analysing the Law' (SIGNAL), funded by the Norwegian Research Council and UNINETT Norid AS. All URL references cited herein were last accessed 20 June 2017. Thanks are due to Christopher Kuner for providing valuable advice on aspects of section 2.3 of the paper. Nonetheless, the usual disclaimer applies.
10.18261/issn.2387-3299-2017-02-03
Volume 4, No. 2-2017, pp. 105–120
ISSN online: 2387-3299
RESEARCH PUBLICATION

1 INTRODUCTION

A hallmark of the recent reform of European Union (EU) law on the protection of personal data is the introduction ofmore explicit and expansive requirements concerning data protection by design and by default. These requirements inhere principally in Article 25 of the General Data Protection Regulation (GDPR),[2] which shall apply from 25May 2018, thereby replacing the 1995 Data Protection Directive (DPD).[3] Article 25 (set out in full in section 3 below) imposes a qualified duty on controllers of personal data to implement technical and organisational measures that are designed to ensure that the processing of personal data meets the Regulation's requirements and otherwise to ensure protection of data subjects' rights. The duty extends to ensuring default application of particular data protection principles and default limits on data accessibility. As elaborated further on, a similar (but not identical) duty is laid down in Article 20 of the 2016 Directive on Data Protection and Law Enforcement.[4]

The provisions of GDPR Article 25 are amongst the most innovative and ambitious norms of the EU's newly reformed data protection regime. They are directed essentially at information systems development, with the aim of ensuring that due account be taken of privacy-related interests throughout the lifecycle of such development. They may be seen as a manifestation of the increased emphasis in the GDPR on making data protection
'count' and, concomitantly, on making data controllersmore accountable.[5] Their rationale is rooted in a belief that building data protection principles into information systems architecture
will substantially improve the principles' traction. Part and parcel of this rationale is an implicit recognition of the potential of information systems architecture to shape human conduct more effectively than through the mere imposition of legislation or contract
– a potential popularised in the notions of 'Lex Informatica' and 'West Coast Code'.[6] With the embedment of legal norms in the architecture comes the promise of enhancing, if
not automating, their *ex ante* application, thereby reducing the 'catch-up-with-technology' problem that often hampers legislators' regulatory efforts.

Article 25 springs out of a policy discourse that commonly goes under the nomenclature 'Privacy by Design' (PbD). Although PbD is not necessarily fully commensurate with the requirements of Article 25 (a point elaborated further on), the thrust of their respective
ideals is similar. Like Article 25, PbD aims to ensure that privacy-related interests

2. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

3. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

4. Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

5. See e.g. GDPR Articles 5(2), 24(1) and recital 11 of the preamble.

6. The seminal literature in this regard being Joel R. Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997) 76 *Texas Law Review* 553; Lawrence Lessig, *Code, and Other Laws of Cyberspace* (Basic Books 1999).

are neither forgotten nor marginalised in the initial design and subsequent development of information systems. Again, like Article 25, PbD applies not just to the design of software or hardware; it extends to business strategies and other organisational practices
as well.[7] Closely linked to it is an older policy discourse centred on the creation of 'Privacy-Enhancing Technologies' (PETs) – i.e. technological mechanisms that promote respect for privacy-related interests.[8] Both discourses feed into a broader interdisciplinary endeavour aimed at embedding key human values – particularly those central to virtue ethics – in the process of technology design.[9]

Over the last decade, PbD ideals have become a staple part of data protection authorities'
agenda. In 2010, the 32nd International Conference of Data Protection and Privacy Commissioners unanimously passed a resolution recognising 'Privacy by Design as an essential component of fundamental privacy protection' and encouraging 'the adoption of Privacy by Design's Foundational Principles … as guidance to establishing privacy as an organization's default mode of operation'. The Article 29Working Party on the Protection

of Individuals with regard to the Processing of Personal Data – an advisory body composed of representatives of the data protection authorities of EU member states – has followed up this resolution in policy pronouncements concerning internet technology.[10] In the United States of America (USA), the Federal Trade Commission has pushed PbD ideals both through policy proposals and through settlement agreements with corporations.[11] And, as GDPR Article 25 shows, the European Commission, Parliament and Council have embraced PbD ideals to such an extent as to provide them with substantial legislative backing.

7. See further e.g. Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (August 2009; revised January 2011); available at <https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf>; Peter Schaar, 'Privacy by Design' (2010) 3 *Identity in the Information Society* 267; Demetrius Klitou, 'A Solution, But Not a Panacea for Defending Privacy: The Challenges, Criticism and Limitations of Privacy by Design' in Bart Preneel and Demosthenes Ikonomou (eds), *Privacy Technologies and Policy: First Annual Privacy Forum, APF 2012* (Springer Verlag 2014) 86-110.

8. Further on the evolution, parameters and interrelationship of PET and PbD discourses, see Lee A. Bygrave, 'Hardwiring Privacy' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation, and Technology* (Oxford University Press 2017) 754-775.

9. See e.g. Norbert Wiener, *The Human Use of Human Beings: Cybernetics and Society* (Doubleday Anchor 1954);
Batya Friedman, Peter H. Kane Jnr and Alan Borning, 'Value Sensitive Design and Information Systems' in Kenneth Einar Himmar and Herman T. Tavani (eds), *The Handbook of Information and Computer Ethics* (Wiley 2008) 69-101; Sarah Spiekermann, *Ethical IT Innovation: A Value-Based System Design Approach* (Taylor & Francis 2016).

10. See e.g. Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinion 8/2014 on Recent Developments on the Internet of Things (WP 223; 16 September 2014).

11. See e.g. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (December 2010); Federal Trade Commission, Agreement Containing Consent Order, In the Matter of Google Inc., FTC File No. 102-3136 (13 October 2011).

2 LEGAL ANTECEDENTS TO GDPR ARTICLE 25

2.1 Legislation

Article 25 has no exact equivalent in the Data Protection Directive. The latter contains, however, provisions with a similar thrust as Article 25, albeit with a pronounced security focus. Recital 46 of the Directive's preamble refers to a need to take 'appropriate technical and organisational measures' for safeguarding data protection interests 'both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorised processing'. The recital goes on to stipulate that 'these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected'. Article 17 is in a similar vein, but with an even more pronounced security emphasis. Indeed, all the protective measures listed in Article 17 directly concern information security, which is a necessary though insufficient element of a comprehensive data protection regime.

The equivalent provisions of the Directive on privacy and electronic communications are less tied to security concerns.[12]While Article 4(1) of the Directive continues the security focus of the DPD by requiring a 'provider of a publicly available electronic communications service' to 'take appropriate technical and organizational measures to safeguard

security of its services', recital 30 in the preamble provides direct encouragement for design
measures that go beyond a security remit: 'Systems for the provision of electronic communications
networks and services should be designed to limit the amount of personal
data necessary to a strict minimum'. Another relevant provision that is not tethered to security is Article 14(3) which requires the adoption of measures 'to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data'. This provision parallels Article 3(3)(c) of Directive 1999/5/EC which mandates that radio equipment and telecommunications terminal equipment incorporate 'safeguards to ensure that the personal data and privacy of the user
and of the subscriber are protected'.[13]

Looking beyond EU legislation, we find few legal norms dealing directly or indirectly with data protection by design and by default. At the national level, Germany's Federal Data Protection Act of 1990 comes closest to embracing the thrust of GDPR Article 25.[14] Under the nomenclature 'Datenvermeidung und Datensparsamkeit' (data avoidance and data economy), section 3a of the Act requires information systems to be designed with the
aim of processing as little personal data as possible. Elaborating on this requirement, it stipulates that personal data shall be pseudonymised or anonymised insofar as is reasonable
in relation to the desired level of protection.

12. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic
communications sector [2002] OJ L 201/37.

13. Directive 1999/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity [1999] OJ L91/10.

14. *Bundesdatenschutzgesetz – Gesetz zum Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20
Dezember 1990*, as amended.

At the international level, the sole treaty dealing specifically with data protection – the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic
Processing of Personal Data[15] – omits specific requirements on data protection by design and by default. However, the 2016 proposal to modernise the Convention introduces
a set of provisions in Article 8bis embracing some such requirements, but using different formulations than found in GDPR Article 25.[16] Particularly noteworthy in this regard is that the Article 8bis requirements fail to make clear provision for data protection 'by default' – unlike GDPR Article 25(2), elaborated in section 3 below.

2.2 Case law

The European Court of Human Rights (ECtHR) has been relatively early in embracing ideals similar to those manifest in Article 25. This occurred in 2008 in *I v Finland*.[17] In this case, the Court unanimously found Finland to have violated its positive obligations to secure respect for private life pursuant to Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR),[18] due to its failure to secure, through technological-organisational measures, the confidentiality of patient data in a public hospital. The applicant was a woman who was infected with HIV and who suspected that hermedical records generated whilst she was hospitalised had been accessed

by unauthorised third persons. Her complaint turned chiefly on the fact that the hospital concerned had operated a health records system without putting in place a mechanism for comprehensively logging who consulted the health records and for storing the log details such that it was possible to ascertain subsequently whether the records had been accessed without proper authorisation.While Finnish law provided protections for patient data – including compensation to data subjects for damage they suffered in the event of unauthorised disclosure of the data – the ECtHR held that Finland had to provide more than data protection *de jure* in order tomeet its positive obligations under ECHR Article 8:

15. Opened for signature 28 January 1981; in force 1 October 1985; ETS 108 (hereinafter also 'Convention 108').
16. See Draft modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS 108], drawn up by the Council of Europe's Ad hoc Committee on Data Protection (version of September 2016). Article 8bis(2) of the proposal stipulates that a state party shall require 'controllers and, where applicable processors' to 'examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interferencewith those rights and fundamental freedoms'. Article 8bis(3) requires a state party to provide 'that controllers, and, where applicable, processors, implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing'. Article 8bis(4) permits a state party, 'having regard to the risks arising for the interests, rights and fundamental freedoms of the data subjects', to modify its lawgiving effect to the requirements of the preceding provisions 'according to the nature and volume of the data, the nature, scope and purpose of the processing and, where appropriate, the size of the controller or processor'.
17. Appl. No. 20511/03, Judgment of 17 July 2008.
18. Opened for signature 4 November 1950; in force 3 September 1953; ETS 5.

'The Court notes that the mere fact that the domestic legislation provided the applicant with an opportunity to claim compensation for damages caused by an alleged unlawful disclosure of personal data was not sufficient to protect her private life. What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place. Such protection was not given here'.[19]

Although the Court made no reference to 'data protection by design and by default' or closely linked notions, such as 'privacy by design' or 'privacy-enhancing technology', the basic thrust of its judgment necessitates adoption of a mindset and methods in line with these notions. Further, one can read into the above-cited paragraph of the Court's judgment

a requirement for data accessibility limits that, as a point of departure, guarantee confidentiality of data.[20] Accordingly, the overall result of *I v Finland* is effectively to make data protection by design and by default an integral requirement of a state's positive obligations

to secure respect for the right(s) laid down in ECHR Article 8, at least in relation to ensuring the confidentiality of data relating to a person's health.

Whether this result may be extended to the processing of other types of personal data than health data or to cover other functionalities than ensuring data confidentiality is less certain. The Court made much of the special nature of health data, noting that their protection

'is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention', 'a vital principle in the legal systems of all the Contracting Parties to the Convention', and 'crucial' not just for the privacy of the data subject 'but also to preserve his or her confidence in the medical

profession and in the health services in general'.[21] The Court further stated that these considerations

'are especially valid as regards protection of the confidentiality of information about a person's HIV infection, given the sensitive issues surrounding this disease'.

Thus,

held the Court, '[t]he domestic lawmust afford appropriate safeguards to prevent any such
communication or disclosure of personal health data as may be inconsistent with the guarantees
in Article 8 of the Convention'.[22] The special status of such data notwithstanding,
there is little reason to hold that other types of personal data do not qualify for similar protection
de facto (on top of protection *de jure*). This is especially so for categories of personal data that are commonly regarded as relatively sensitive, such as those listed in Article 6 of

19. Ibid, para. 47. As the Court pointed out, the preparatory works to the Finnish data protection legislation also emphasised that data protection *de jure* was insufficient: 'the data controller had to make sure that data were protected *de facto'*. Ibid, para. 19. The paucity of *de facto* privacy protection, though, was not the only problem; a due process difficulty inhered in the case as well, in that the lack of logging undermined the applicant's ability to litigate before the Finnish courts because it deprived her of concrete evidence that her health records had been accessed unlawfully. As the Court stated, '[i]t is plain that had the hospital provided a greater control over access to health records by restricting access to health professionals directly involved in the applicant's treatment or by maintaining a log of all persons who had accessed the applicant's medical file, the applicant would have been placed in a less disadvantaged position before the domestic courts': ibid, para. 44.
20. This is akin to the requirement under GDPR Article 25(2), set out in section 3 below.
21. Ibid, para. 38. See too *Z v Finland*, Appl. No. 22009/93, Judgment of 25 February 1997, paras. 95-96.
22. Ibid, para. 38.

Convention 108.[23] Yet, the processing of more ordinary types of personal data may necessitate
the implementation of 'practical and effective protection' (using the above-cited language of the Court) in particular circumstances – e.g. when the processing can easily give rise to unfair discrimination. There is also little reason to hold that such protection cannot extend to functionalities other than ensuring data confidentiality – e.g. ensuring that the amount of personal data collected is limited to what is necessary to achieve the purpose(s)
for which the data are gathered and further processed (i.e. data minimisation).

The Court of Justice of the European Union (CJEU) has not yet ruled directly on the subject matter of GDPR Article 25, nor has it handed down a judgment requiring *de facto* protection of personal data in such a direct way as the ECtHR has done. However, it has fired several shots across the path of internet-related technology deployment. The first two such shots sunk proposals in Belgium to employ deep packet inspection aimed at countering digital piracy.[24] Although the CJEU refrained from actively promoting data protection by design and by default in these cases, it effectively stopped the deployment of privacy-intrusive technology. Thereafter, the CJEU fired a shot at a commonly used internetmechanism in the famous *Google Spain* case.[25] The Court's judgment did not bring
down Google's search engine. Nor did it require any substantial 'hardwiring' of privacy interests into the engine's 'West Coast Code'. Nonetheless, by rejecting Google's argument
that its search engine operations are value-neutral, robotic applications of algorithms outside the scope of data protection law, the CJEU required Google (and other search engine operators) to reconfigure systemic aspects of those operations so that they are more
privacy friendly. It thereby indirectly nurtured the aims of GDPR Article 25. Moreover, as elaborated in the next section, the CJEU has also indirectly nurtured these aims in the *Digital Rights Ireland* case.[26]

2.3 Data protection by design and by default as constitutional norm in EU law?

Whereas data protection by design and by default is an essential part of a state's positive obligations to secure respect for the right(s) laid down in ECHR Article 8, at least in relation to safeguarding the confidentiality of health data, its precise status under EU law remains somewhat unclear. Obviously, it inheres as a qualified requirement in secondary EU legislation – most notably, the General Data Protection Regulation and the Directive on Data Protection and Law Enforcement. But does it also inhere in Articles 7 or 8 of the EU Charter of Fundamental Rights (EUCFR),[27] or in Article 16 of the Treaty on the

23. That is, data concerning a person's 'racial origin, political opinions, religious or other beliefs', or their 'criminal convictions', in addition to data concerning their 'health or sexual life'.

24. Case C-70/10, *Scarlet Extended v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Judgment of 24 November 2011, ECLI:EU:C:2011:771; Case C-360/10, *SABAM v Netlog*, Judgment of 16 February 2012, ECLI:EU:C:2012:85.

25. Case C-131/12, *Google Spain v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Judgment of 13 May 2014, ECLI:EU:C:2014:317.

26. Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd and Seitlinger and Others*, Judgment of 8 April 2014, ECLI:EU:C:2014:238.

27. [2000] OJ C 364/1. EUCFR Article 7 replicates the right(s) set out in ECHR Article 8(1); EUCFR Article 8 lays down a right to the protection of personal data.

Functioning of the European Union (TFEU),[28] independently of secondary legislation? In other words, is data protection by design and by default a constitutional norm in the EU legal system, closely associated with the fundamental rights of privacy and data protection?

As elaborated in the following, the status of data protection by design and by default pursuant to the ECHR and the attendant case law of the ECtHR is relevant here. At the same time, caution needs to be exercised when applying Strasbourg norms to cast light on EU law. As a point of departure, the CJEU is not legally bound by Strasbourg jurisprudence, nor is the ECHR formally part of the EU legal system.[29] While the CJEU does cite and follow ECtHR decisions (also in a data protection context), its utilisation of the latter is far from consistent.[30] Further, CJEU jurisprudence is increasingly self-referential and concomitantly less inclined to cite Strasbourg case law.[31] Nonetheless, EUCFR Article 52(3) sets out what Advocate-General Kokott has termed a 'homogeneity clause' aimed at ensuring that the protection of Charter rights does not fall below the level of protection offered by the Convention rights.[32] Article 52(3) provides:

> In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

Moreover, the Explanation on this provision states that 'the meaning and the scope of the guaranteed rights are determined not only by the text of those instruments, but also by the case law of the European Court of Human Rights'. Strictly speaking, the Explanations are not legally binding, yet they are to be 'given due regard' by the CJEU pursuant to EUCFR Article 52(7) and TEU Article 6(1). Indeed, the CJEU has held that EUCFR Article 7 'contains rights corresponding to those guaranteed by Article 8(1) of the ECHR' and that 'Article 7 of the Charter must therefore be given the same meaning and the same scope as Article 8(1) of the ECHR, as interpreted by the case-law of the European Court of Human

Rights'.[33]

28. [2012] OJ C 326/47. Article 16(1) replicates EUCFR Article 8(1).

29. See e.g. Case C-617/10, *Åkerberg Fransson*, Judgment of 23 February 2013, EU:C:2013:105, para. 44. Note also
Opinion 2/13 in which the CJEU has held that the agreement on EU accession to the ECHR is not compatible with Article 6(2) of the Treaty on European Union (TEU [2012] OJ C 326/1): Opinion 2/13 on the Accession of the European Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms, EU:C:2014:2454.

30. See further e.g. Bruno de Witte, 'The Use of the ECHR and Convention Case Law by the European Court of Justice' in Patricia Popelier, Catherine Van deHeyning and Piet VanNuffel (eds),*Human Rights Protection in the European Legal Order: The Interaction between the European and the National Courts* (Intersentia 2011) 15-34, 19 (aptly characterising CJEU utilisation of ECtHR decisions as 'eclectic and unsystematic').

31. See e.g. Jasper Krommendijk, 'The Use of ECtHR Case Law by the Court of Justice after Lisbon: The View of Luxembourg Insiders' (2015) 22(6)*Maastricht Journal of European and Comparative Law*812; Gráinne de Búrca, 'After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?' (2013) 20(2) *Maastricht Journal of European and Comparative Law* 168.

32. AG Kokott in Case C-110/10 P, *Solvay*, Opinion of 14 April 2011, ECLI:EU:C:2011:257, para. 95.

33. Case C-400/10 PPU, *J. McB v. L. E.*, Judgment of 5 October 2010, EU:C:2010:582, para. 53.

In light of these legal sources, together with the decision of the ECtHR in *I v Finland*, it may cogently be claimed that data protection by design and by default inheres in EUCFR Article 7, at least insofar as protection of the confidentiality of health data is concerned. At the same time, it would make little sense to claim that a different result pertains with respect to EUCFR Article 8(1) and (2) both of which deal specifically with data protection and are, according to the Explanation on them, based on, *inter alia*, ECHR Article 8, Convention
108 and the DPD. Admittedly, the right in EUCFR Article 8 is not fully commensurate with the right(s) in CFR Article 7,[34] but they are closely tied together and frequently applied in tandem by the CJEU.[35] Moreover, although the CJEU has failed to provide much detailed guidance on the content of EUCFR Article 8, it has strongly implied that the
'essence' of the provision requires adoption of 'technical and organisational measures' to ensure that personal data are given 'effective protection' against 'risk of abuse and against
any unlawful access and use'. [36]

If, as suggested above, data protection by design and by default is part of the EU's constitutional
fabric, this may have repercussions for how stringently the provisions of GDPR Article 25 (and, indeed, the equivalent provisions in the Directive on Data Protection and Law Enforcement) are to be construed and applied.

3 ANALYSING GDPR ARTICLE 25

3.1 The logic and thrust of Article 25

Article 25 reads as follows:

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order tomeet the requirements
of this Regulation and protect the rights of data subjects.

34. See e.g. Herke Kranenborg, 'Article 8' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights:*
A Commentary (Hart Publishing 2014) 223, 228-229; Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).

35. See e.g. the judgment in *Google Spain* (n 25). See also the judgment in *Digital Rights Ireland* (n 26), especially
para. 53 (noting that 'the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter').
36. Judgment in Digital Rights Ireland (n 26) paras. 40 and 66; see too para. 67. This line is siimilar to the thrust of
the ECtHR judgment in *I v Finland*, yet goes perhaps even further than the latter as it is not limited to contexts involving the processing of health data but extends to the processing of personal data more generally (including traffic and location data generated through use of electronic communications networks).

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing
are processed. That obligation applies to the amount of personal data collected, the extent of their
processing, the period of their storage and their accessibility. 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.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

The provisions of Article 25 are replicated in Article 20 of the Directive on Data Protection and Law Enforcement, albeit with two minor differences. One difference is that Article 20 omits reference to certificationmechanisms. The other difference occurs in the elaboration
of Article 20 in recital 53 of the preamble to the Directive where it is stated that the implementation
of the measures referred to in Article 20 'should not depend solely on economic considerations'.

The overall thrust of GDPR Article 25 is to impose a qualified duty on controllers to put in place technical and organisational measures that are designed to implement data protection principles effectively and to integrate necessary safeguards into the processing
of personal data so that such processing will meet the Regulation's requirements and otherwise ensure protection of data subjects' rights. The duty builds on and elaborates the
more generally formulated provisions on 'responsibility of the controller' in Article 24. It is formulated in very similar terms to the duty to ensure adequate security of processing under GDPR Article 32. Yet, unlike the latter, the duty under Article 25 extends to ensuring
– apparently without qualification – default application of particular data protection principles and default limits on data accessibility.

Remarkably, the respective versions of the draft provisions for Article 25 (originally numbered Article 23) that were initially adopted by the European Commission, Parliament
and Council were more similar than they were different.[37] The principal differences concerned:
(i) who must implement the stipulated measures (whereas the Commission and Council imposed a duty on controllers only, the Parliament extended obligations to processors
as well); (ii) the specification of measures (unlike the Commission and Parliament, the Council made express mention of 'data minimisation and pseudonymisation' as examples
of appropriate measures); (iii) the considerations that are to be taken into account

when implementing measures (whereas the Commission and Council permitted consideration
of the implementation cost, the Parliament did not; the latter was otherwise more wide-ranging in its elaboration of considerations than were the former); (iv) the use of certification schemes to demonstrate compliance with Article 25 (the Council mentioned such schemes whereas the Commission and Parliament did not); and (v) the role of 'data protection by design' in public procurement tenders (the Parliament made 'data protection

37. See e.g. European Parliament, *Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (A7-0402/2013; PE501.927v05-00).*

by design' a prerequisite for such tenders, the Commission and Council did not). As shown
further on, the bulk of these differences have been papered over, either in the provisions of
Article 25 or by resorting to elaborations of Article 25 in recital 78 of the preamble.

The duty imposed by Article 25(1) is qualified by an extensive list of contextual factors. These will be determined to a significant extent (but not exclusively) by the data protection
impact assessment that controllers are required to conduct pursuant to Article 35. There is
accordingly a close relationship between impact assessments and Article 25 requirements.

However, the requirement to undertake an impact assessment arises only where processing
'is likely to result in a high risk' to persons' rights and freedoms (Article 35(1)), whereas the duty imposed by Article 25 does not.

Elaborating on the measures required by Article 25(1), the reference to 'pseudonymisation'
as an example of a suitable measure is supplemented by other examples listed in recital 78. At the same time, Article 25(1) stipulates that the measures concerned must be
'designed to implement data-protection principles'. The latter denote primarily the principles
listed in Article 5 of the Regulation. This is confirmed by the reference to 'data minimisation'
as an example (listed in Article 5(1)(c)).Whether Article 25 embraces other data protection principles than those listed in Article 5 is amoot point and arguably of academic
interest only, as the pith of such principles is adequately covered by Article 5, at least at an
operational level. Further guidance on the parameters of Article 25 measures is expected to
come from codes of conduct prepared by industry bodies (Article 40(2)(h)), from certification
schemes (Article 25(3) in combination with Article 42), and from advice provided by data protection authorities.

It bears emphasis that the measures referred to in Article 25(1) are not just technical but also organisational. In other words, they embrace more than the design and operation

of software or hardware; they also encompass business strategies and other organisational-
managerial practices. This is in line with common conceptions of PbD.[38] However, Article 25 is not necessarily in complete keeping with PbD discourse. A possible divergence
emerges with respect to the pitch or length of the measures required by Article 25, this being tethered in large part to the standards of the Regulation. Cavoukian's seminal conception
of PbD is different, at least at first blush. She considers her 'foundational principles' of PbD as not only embracing the 'fair information practices' of data protection law, but also going well beyond them – in her view, they 'significantly raise the bar' of legal norms.[39] Yet, the norms to which Article 25 is tethered tend to be more ambitious, stringent
and wide-ranging than the standard 'fair information practices' to which Cavoukian probably refers, particularly those practices typically prescribed in US data protection laws.[40] In effect, then, the conception of data protection by design and by default in Article
25, despite its legal tethering, might well be pitched at a similar level to Cavoukian's legally

38. See e.g. Cavoukian (n 7); Schaar (n 7).
39. Ann Cavoukian, 'A Regulator's Perspective on Privacy By Design' (2012); available at <http://www.futureofprivacy.org/privacy-papers-2012>.
40. See generally Lee A. Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press 2014) 107-116.

untethered conception of PbD. On the other hand, it might also reach further than other North American conceptions of PbD.[41] This underlines the need to take care in using the terms 'data protection by design and by default' and 'privacy by design' interchangeably, particularly in transatlantic discourse.

The 'by design' requirements of Article 25(1) differ from the 'by default' requirements of Article 25(2) in several respects. The former cover a potentially wider range of data protection
measures than the latter, which focus, in effect, simply on keeping data 'lean and locked up'. And while the former appear to be process-oriented to a considerable degree (this follows partly from its 'design' focus), the latter are more concerned with results that guarantee – at least as a point of departure – protection with respect to data minimisation and confidentiality. In other words, the latter go well beyond a soft paternalism that simply nudges information systems development in a privacy-friendly direction without seeking to 'hardwire' privacy enhancement in concrete ways. This follows too from the arguably enhanced normative status of data protection by design and by default in light of
the case-law considerations outlined towards the end of section 2.3.

Article 25(1) measures are to be taken at both the design stage and processing stage. The
same necessarily applies for Article 25(2) measures even if Article 25(2) does not specifically
spell this out. On their face, both sets of measures are to be taken by controllers only. Controllers are basically defined as entities that determine or co-determine the purposes, conditions and means of processing personal data (Article 4(7)). Article 25(1) formulates the design stage in terms of when the controller assumes controller status ('the time of the

determination of the means for processing'). However, recital 78 brings Article 25 ideals to
bear on other actors than just controllers – namely, 'producers' of products, services and applications that involve processing of personal data. These actors are subject to less stringent
requirements ('should be encouraged') than those imposed on controllers. Article 25 requirements are also brought to bear on processors inasmuch as controllers are only permitted
to use processors 'providing sufficient guarantees to implement appropriate technical and organisational measures' (Article 28(1)); see too recital 81).Thus, the Regulation evinces an expectation that the duty imposed by Article 25 on controllers will be passed both 'downstream' to processors and 'upstream' to technology developers.

The Article 25 duty plays a role in the application of numerous other GDPR provisions, although this is (unhelpfully) not made clear in Article 25 itself. For instance, Article 83(2)(d) stipulates that in determining the imposition of fines for breach of the Regulation, 'due regard' shall be taken of, *inter alia*, 'the degree of responsibility of the controller or processor
taking into account technical and organisational measures implemented by them' pursuant to Article 25. Further, the requirement imposed by Article 34 on a controller to communicate a personal data breach to the data subject may be relaxed if the controller 'has implemented appropriate technical and organisational protection measures' (Article 34(3)(a); see too recitals 87 and 88). And in assessing whether processing of personal data
for another purpose is compatible with the initial purpose for which the data is collected,

41. Compare, for instance, the debate over whether or not the Platform for Privacy Preferences (P3P) – a tool developed by the World Wide Web Consortium for automated dialogue between websites and browsers over their respective sets of privacy preferences – may properly qualify as a PET: see further Bygrave (n 8) 760 and references cited therein.

account shall be taken of, *inter alia*, 'the existence of appropriate safeguards, which may include encryption or pseudonymisation' (Article 6(4)(e)).

Moreover, recital 78 states that the 'principles of data protection by design and by default'
are to play a role in public procurement tenders: the principles 'should… be taken into consideration' in this context. The latter phrasing falls short of making data protection by design and by default a prerequisite for such tenders, but is otherwise confusingly ambiguous
as to how much weight the principles should be given.

3.2 Difficulties

Article 25 suffers from multiple weaknesses. One obvious weakness is the vagueness and
complexity of its language. This is augmented by a paucity of authoritative clear guidance
on the parameters and methodologies for achieving data protection by design and by default – a problem that also afflicts discourse on PbD.[42] This is likely to create difficulties for the enforcement of Article 25. Invoking stiff sanctions for breach of Article 25(1) will not be easy given the very general (and process-oriented) way in which its obligations are
formulated. At the same time, the limited utility of wielding a stick necessitates relying on other incentives to abide by Article 25 requirements. Some such incentives do exist, but they are few and far between. The provisions of Articles 83(2)(d), 34(3)(a) and 6(4)(e)

set out in section 3.1 above are relevant examples. However, their role as incentives in this
respect is indirect and obtuse.

Additionally, the vagueness and complexity of the legalese in Article 25 impedes the 'regulatory conversation' (Black)[43] between not just EU legislators and other members of the legal community but, more crucially, between EU legislators and data protection authorities on the one side and, on the other side, the community of persons who actually
work at the 'coalface' of information systems development. As I have noted elsewhere in relation to the latter community, the legalese in Article 25 functions, in effect, as a form of encryption vis-à-vis persons who are without formal legal qualifications and expertise in this area of law.[44] This hinders the ability of Article 25 to galvanise the engineering community to work in the direction wished. While the ideals of PbD and Article 25 are not entirely alien to that community, which has occasionally articulated and acted upon privacy concerns of its own accord, it is, on the whole, a notoriously self-centric community
and relatively impervious to external, non-technocratic values. There is considerable evidence to suggest that it is far from embracing the ideals of PbD and Article 25 to the degree that the latter requires.[45]

42. Further on this lack of clarity, see Bygrave (n 8) 756-762.

43. Julia Black, 'Regulatory Conversations' (2002) 29 *Journal of Law and Society* 163.

44. Bygrave (n 8) 772. This is just one aspect of a larger 'communication' problem facing the GDPR. See further Chris Reed, 'You talkin' to me?' in Dag Wiese Schartum, Lee A. Bygrave and Anne Gunn Berge Bekken (eds), *Jon Bing: En Hyllest / ATribute* (Gyldendal Akademisk 2014) 154–170; Dag Wiese Schartum, 'Intelligible Data Protection Legislation: A Procedural Approach' (2017) 17(1) *Oslo Law Review* 48.

45. See further Lilian Edwards, 'Privacy, Security and Data Protection in Smart Cities: ACriticalEU LawPerspective'
(2016) 2(1) *European Data Protection Law Review* 28, 51 and references cited therein; Bygrave (n 8) 764-765 and references cited therein.

The traction of Article 25 on information systems development is likely also to be hindered by its limited reach. As pointed out above, Article 25 measures are primarily imposed on data controllers only. Yet, we cannot assume that basic design decisions in information systems development will be exclusively or predominantly taken by entities acting in a controller capacity. Exacerbating this shortcoming is that Article 25(1) formulates the design stage as the time when the controller assumes controller status – a
phase that might not equate with the time when a particular data-processing device is actually designed and manufactured.

The Article 29 Working Party on the Protection of Individuals with regard to the Processing
of Personal Data has taken an expansive view of the 'controller' category in relation to entities involved in developing or supplying devices and platforms for the emergent 'Internet of Things'.[46] The CJEU also took an expansive view of the 'controller' category in the *Google Spain* case.[47] This notwithstanding, it is highly doubtful that Article 25 embraces all relevant elements of the engineering and design community. Take, for instance, the Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C). Both are centrally involved in the development of basic internet standards, many of which have a significant impact on the daily processing of huge amounts of personal data.[48] Yet, it can scarcely be claimed that either organisation qualifies as a 'controller' pursuant to the GDPR. Moreover, there are numerous information systems development processes in which it is extremely difficult to delineate clear lines of responsibility and liability

according to the actor categories laid down in data protection law. The development of cloud-computing platforms is one example; the development of 'smart car' technology and, more generally, the 'Internet of Things' are others.[49] The drafters of the Regulation seem to be aware of these shortcomings inasmuch as the Regulation stipulates that 'producers' of products, services and applications involving the processing of personal data 'should be encouraged' to take account of Article 25 ideals when carrying out their work (recital 78). This stipulation, though, is tucked away towards the tail-end of a long and densely worded recital in the Regulation's preamble; it is also less stringently formulated than the requirements placed on controllers. The propriety *lex ferenda* if not *lex lata* of this relaxation in stringency is questionable given the arguably enhanced normative status of data protection by design and by default outlined in section 2.3 above.

Market factors are likely to create further difficulties for the traction of Article 25 on information systems development. The Regulation seems either to assume the existence of a healthy market for PETs and other PbD products/services or that Article 25 will help to create such a market. Indeed, Article 25 might well be important for adding a new category of market, additional to the four traditional privacy markets identified by Acquisti

46. Article 29 Working Party (n 10).

47. *Google Spain* (n 25) paras. 32-40.

48. See further Harald Alvestrand and Håkon Wium Lie, 'Development of Core Internet Standards: The Work of IETF and W3C' in Lee A. Bygrave and Jon Bing (eds), *Internet Governance: Infrastructure and Institutions* (Oxford University Press 2009) 126-146.

49. More generally on these difficulties, see e.g. Edwards (n 45); Christopher Millard (ed), *Cloud Computing Law* (Oxford University Press 2013).

and his colleagues.[50] The four traditional privacy markets are, briefly: (i) markets in which data aggregators buy/sell data from/to other organisations; (ii) markets in which consumers exchange information for 'free' services/products; (iii) markets inwhich consumers attempt to sell their data; and (iv) markets in which consumers attempt to purchase protection for their data. The market envisaged by Article 25 is closely related to, and leverages off, the latter market, but could also be seen as a market in itself, as it is one in which data controllers (rather than consumers) are trying to purchase PETs and PbD products/services and otherwise stimulate their production. The problem for this new market, however, is threefold: first, there is not yet a burgeoning competitive market for PETs and PbD products/services;[51] secondly, controllers might not have the necessary market power to stimulate the generation of PETs and PbD products/services; thirdly, production, dissemination and widespread utilisation of such PETs and PbD products/services are likely to be stymied by pervasive methods of business and government that are fundamentally at odds with strong forms of privacy hardwiring. The latter problem exacerbates the former two. We see the contours of these difficulties exemplified in the ongoing debate over the propriety of strong encryption products in light of the desires of government law enforcement agencies to gain ready access to the 'clear text' of otherwise encrypted data. We see them also exemplified in Google's efforts to hinder online ad-blocking products from gaining market

traction, and, arguably, in Facebook's acquisition of WhatsApp.[52] Thus, the Regulation's reliance on controllers to shape the market and technology foundations for information systems development in a privacy-friendly direction is vulnerable to derailing by powerful counter-interests.

4. CONCLUSIONS

On paper, Article 25 is an ambitiously conceived provision that seeks to reach into the heart of the machinery of our information age and reshape it to respect important values. As such, it has much to commend it. Unfortunately, its ability to reshape this machinery is likely to be significantly undermined by a variety of weaknesses, including fuzzy legalese and a more general lack of clarity over the parameters and methodologies for achieving its goals, a paucity of salient and strong incentives to abide by its requirements, and a failure to communicate clearly with those working directly with the design and development of information systems. Augmenting these weaknesses is the fact that the thrust of Article 25, at least if followed through stringently, is at odds with the basic *modus operandi* of many powerful organisations, both in the private and public sectors.

50. Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The Economics of Privacy' (2016) 54(2) *Journal of Economic Literature* 442, 473.

51. See further Bygrave (n 8) 762-763 and references cited therein.

52. See furtherMaurice Stucke and Allen Grunes, *Big Data and Competition Policy* (Oxford University Press, 2016) 54, 262.

Despite these shortcomings, Article 25 is, at the very least, valuable as a catalyst for the *mental* hardwiring of privacy-related interests. As Koops and Leenes note, the real utility of Article 25 should be seen in terms of 'a substantive requirement calling upon data controllers to consistently keep privacy at the front of their minds when defining system requirements'.[53] Following on in this vein, it is unreasonable to expect Article 25 to provide detailed guidance for such systems development, apart from defining goal posts and setting out legal incentives for moving towards them; the detailed guidance must be developed elsewhere. In this regard, Article 25 should be seen as a weighty conversation-starter in the necessary dialogue between data protection authorities and privacy advocates on the one side and data controllers, processors and engineers on the other, over the way forward in the technological and organisational hardwiring of privacy-related interests.

53. Bert Jaap Koops and Ronald Leenes, 'Privacy regulation cannot be hardcoded. A critical comment on the "privacy by design" provision in data-protection law' (2014) 28 *International Review of Law, Computers & Technology* 159, 168.