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

Lee A. Bygrave
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 INTRODUCTION
A hallmark of the recent reform of European Union (EU) law on the protection of personal data is the introduction of more 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), which shall apply from 25 May 2018, thereby replacing the 1995 Data Protection Directive (DPD). 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.
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 controllers more accountable. 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’. 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 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. 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. 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.

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 29 Working 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. 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.
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.

9. See e.g. Norbert Wiener, The Human Use of Human Beings: Cybernetics and Society (Doubleday Anchor 1954);
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).

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. 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’.

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. 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
13. Directive 1999/5/EC on radio equipment and telecommunications terminal equipment and the mutual
20 Dezember 1990, as amended.
This article is downloaded from www.idunn.no. © 2017 Author(s).
This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0
License (http://creativecommons.org/licenses/by/4.0/).

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 – 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. 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. 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), 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 to meet its positive obligations under ECHR Article 8:


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 interference with 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’.


18. Opened for signature 4 November 1950; in force 3 September 1953; ETS 5.

This article is downloaded from www.idunn.no. © 2017 Author(s).

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0 License (http://creativecommons.org/licenses/by/4.0/).

OSLO LAW REVIEW | VOLUME 4 | No. 2-2017 109

‘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 law must 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'. 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.


22. Ibid, para. 38.

This article is downloaded from www.idunn.no. © 2017 Author(s).
This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0 License (http://creativecommons.org/licenses/by/4.0/).

110 LEE A. BYGRAVE

Convention 108. 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. 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 internet mechanism in the famous Google Spain case. 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. 23 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), or in Article 16 of the Treaty on the Functioning of the European Union (TFEU), 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. While the CJEU does cite and follow ECtHR decisions (also in a data protection context), its utilisation of the latter is far from consistent. Further, CJEU jurisprudence is increasingly self-referential and concomitantly less inclined to cite Strasbourg case law. 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. 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’.27
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, but they are closely tied together and frequently applied in tandem by the CJEU. 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’. 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 to meet the requirements of this Regulation and protect the rights of data subjects.

This article is downloaded from www.idunn.no. © 2017 Author(s).
This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0 License (http://creativecommons.org/licenses/by/4.0/).
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 similar 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 certification mechanisms. 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 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 moot 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. 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. 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. 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 untethered conception of PbD. On the other hand, it might also reach further than other North American conceptions of PbD. 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, 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. 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) 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. 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.

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’. The CJEU also took an expansive view of the ‘controller’ category in the Google Spain case. 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. 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. 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.
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. 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 in which 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; 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. 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.


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


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’.