UiO : Faculty of Law
University of Oslo

Complying with Privacy by Design in Article 25.1 of the General Data Protection Regulation

A critical analysis of what a controller must do to comply with Article 25.1 and what is reasonable to expect from a controller in this regard in the light of current conditions for achieving compliance

Candidate number: 7002

Submission deadline: 15 May 2017

Number of words: 16 189

Table of contents

List of abbreviations

A29WP	Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data
DPbD	Data Protection by Design
DPD	Data Protection Directive
ENISA	European Union Agency for Network and Information Security
EU	European Union
GDPR	General Data Protection Regulation
PbD	Privacy by Design
PETs	Privacy Enhancing Technologies
PIA	Privacy Impact Assessment

1 Introduction

The amount of data collected and processed is ever increasing and personal data carries huge economic value.[1] There are various strong interests for maximising the utility of the data being processed. The aim of privacy law is to uphold privacy related rights for the persons whose data are being processed. Compliance with privacy law is affected by two important factors, i.e. the digital context in which processing of personal data take place, and that privacy often is in conflict with other interests. The digital context entails rapid changes, not only of the technology itself but also in the way privacy is perceived.[2] Technology shape privacy and the law regulating it and vice versa in a way that creates tension between technology and law with very little symbiotic elements.[3] The rapid progression in technology has outperformed the pace of legal framework response.[4] There have been various attempts, in the form of both state regulation and industry self-regulation, to come to terms with the inadequacies of the legal response in the field of privacy, none however presenting acceptable results neither individually nor combined.[5] One example of such an attempt is Privacy Enhancing Technologies (PETs).[6] PETs aim to uphold compliance with privacy law by converting legal requirements into computer code or at least enhance privacy. The deployment of PETs has however not nearly been as frequent as intended.[7] Though there are various reason for the failure of PETs, one reason within the European Union (EU) could be that utilisation of PETs rest upon a voluntary basis under the current EU privacy law regime primarily based on the Data Protection Directive (DPD).

The European legal framework on privacy is about to undergo major changes as DPD is soon to be replaced by the recently adopted General Data Protection Regulation (GDPR) entering into force by 24 May 2016 and shall apply from 25 May 2018. Among several novelties within GDPR, Art. 25.1 explicitly require the implementation of Privacy by Design (PbD), which according to the European Commission "[…] will become an essential principle."[8] PbD, which can be described as encompassing both organisational and technical aspects (the latter corresponding in many ways with PETs), is a new attempt to enable legislation to keep up with technology rather than being several steps behind all the time.[9] In contrast to the

[1] Bygrave, *Data Privacy Law: An International Perspective*, 5.

[2] Lerner, *The Architecture of Privacy*, 4.

[3] Lerner, *The Architecture of Privacy*, 12-13.

[4] van Lieshout et. al., "Privacy by Design", 58.

[5] Kroener and Wright, "A Strategy for Operationalizing Privacy by Design", 355.

[6] van Lieshout et. al., "Privacy by Design", 58.

[7] van Lieshout et. al., "Privacy by Design", 58.

[8] European Commission press release 21 December 2015.

[9] Bygrave, "Hardwiring Privacy", 2.

current privacy regime based on the DPD, undertaking technical and organisational measures with the aim to uphold legal requirements, is no longer resting on a voluntary basis. With Art. 25.1 GDPR, EU is a pioneer in the field of privacy law. Indeed, though PbD in itself is not a new concept, is a novelty in the way it is currently considered and accepted as a part of law and through the proactive rather than reactive approach, and by 2014 PbD was still not incorporated as a part of any legislation worldwide.[10]

There are many reasons for introducing PbD apart from creating a more symbiotic co-existence between legal code and computer code.[11] PbD might also be useful addressing the increasing frequency of security breaches.[12] From a European perspective, PbD was initiated partly to combat the margin of appreciation currently enabled by the DPD and as a way to enhance the level of compliance with EU privacy law.[13] However, if PbD should have the desired effects on the level of compliance, controllers as the addressees of Art. 25.1 must be able to understand what they are expected to do. Given that PbD is a new phenomenon in the legislative sphere, the challenge of understanding the obligations becomes even greater.

1.1 Research focus

Embracing PbD, set out to enhance compliance with European privacy law, seems to be all but a simple process when assessing what is required by Art. 25.1:

"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."

The construction of Art. 25.1 raises several questions. What exactly does technical and organisation measures apart from 'pseudonymisation' entail in practice? Which data protection principles other than 'data minimisation' should be accounted for? What is meant by 'appropriate'? How much weight can be afforded to each explicitly mentioned interest, e.g.

[10] Kroener and Wright, "A Strategy for Operationalizing Privacy by Design", 355.

[11] Lerner, *The Architecture of Privacy*, 13.

[12] Hustinx, "Privacy by Design", 3.

[13] Koops and Leenes, "Privacy regulation cannot be hardcoded", 161.

‘the costs of implementation’? And how should the various factors be balanced against each other, e.g. ‘the costs of implementation’ and ‘state of the art’? When shall the implementations take place with regard to processing operations? What does integrating the necessary safeguards into the processing to meet the requirements of GDPR actually entail? Should controllers strive towards converting as many of the requirements in GDPR as possible into the means for processing?

The first research focus is to establish what controllers are obliged to do in order to comply with Art. 25.1 of the GDPR. The various legal preconditions in Art. 25.1 will be analysed with the aim to identify and concretise what a controller can and should or could do in order to comply with Art. 25.1. The questions regarding technical and organisational measures will be answered by findings of concrete examples that could be implemented in practice. Some measures are likely to be of greater significance than others, and that category of measures could therefore form part of a basis for what every controller must implement to avoid non-compliance. As the construction of Art. 25.1 seems to imply that what is necessary to implement to comply depend quite a lot on the specific context of each processing operation, special attention will be payed to ‘appropriate’ which is likely to be a central element in that regard. In fact, Art. 25.1 seems to task controllers with undertaking some sort of proportionality-like assessment, weighing various conflicting interests against each other, that ought to result in choices of what measures that are appropriate to implement in the pursuit for compliance. As the interests mentioned in Art. 25.1 are more or less in conflict with one another, it seems that the legislator intended to give controllers a certain amount of discretion in the choices of what measures to implement. This assessment will also be analysed, in particular in connection to the analysis of what might be inferred by ‘appropriate’.

The process towards complying with Art. 25.1 and undertaking this proportionality-like assessment, will inevitably be influenced by several factors. The vaguer the legal requirements are the more dependent controllers become of proper guidance. If controllers are to fully embrace implementing technical measures into the means of processing, the available software becomes an important factor. If the controllers do not produce the software themselves, they must be able to at least influence the production if to enable privacy friendly means of processing. The presence of incentives, as well as the capacity of supervisory authorities to assist, monitor and enforce, should also be decisive factors on the level of success that can be expected from the coming for implementations of PbD. The second research focus is to analyse such surrounding factors that could either facilitate or hamper the efforts of the controller to comply with Art. 25.1. This analysis will then form basis for an attempt to deduce what could be reasonable expectations to place upon controllers. Such reasonable expectations might have an impact on future overall assessments on compliance undertaken by supervisory authorities. Accordingly, reasonable expectations may also serve

as guidance for controllers regarding their level of ambition when striving to comply with Art. 25.1.

1.1.1 Limitations

This thesis will exclusively deal with EU privacy law, primarily focusing on GDPR, and PbD as it is being presented in Art. 25.1.

1.1.2 Terminology

Privacy and data privacy, or data protection as it is called within EU, are two similar but not always identical concepts and with some aspects, data privacy encompasses more than what might typically be regarded as privacy.[14] PbD is called Data Protection by Design (DPbD) in Art. 25.1 of the GDPR. There seems to be some uncertainty whether or not PbD is identical with DPbD as there are those who claim that they are in fact two different concepts.[15] Others treat PbD and DPbD as one and the same.[16] According to Bygrave, though PbD and DPbD is indeed very similar, it is "[…] risky to treat the terms as completely synonymous."[17] Regardless of this uncertainty, for the purpose of this thesis PbD will be treated as identical with DPbD, and privacy and data privacy will not be differentiated between.

1.2 Methodology

Given that GDPR is not yet applicable, and as PbD is a novelty in the field of privacy law, there is no existing case law that can be used for interpretation. The main source of information apart from GDPR itself is therefore available doctrine and research articles on PbD and EU privacy and data protection law with focus on the GDPR. As PbD in Art. 25.1 is a new phenomenon from a legislative perspective, there will subsequently be some degree of uncertainty regarding interpretation of obligations. Research articles and doctrine will thus serve the purpose of indicating what degree of uncertainty that is present in every issue addressed, ranging from consensus to conflicting interpretations. A low level of uncertainty might indicate that a certain requirement is sufficiently clear as to provide basis for an obligation on the controller, and vice versa. Research articles and doctrine is also a vital part of analysing each issue addressed in this thesis. Though most research articles on PbD is written before the final version of Art. 25.1 was adopted, they still have significant bearing on the matter, partly because PbD as a concept has existed for decades outside the sphere of

[14] Bygrave, *Data Privacy Law: An International Perspective*, 4.

[15] Hildebrandt and Tielemans, "Data protection by design and technology neutral law", 517.

[16] Danezis et. al., "Privacy and Data Protection by Design", 12. *See also* Schartum, "Making privacy by design operative", 153 note 12.

[17] Bygrave, "Hardwiring Privacy", 5.

legislation, and partly because there have been numerous drafts and proposals of GDPR which bear many similarities with the final version.

1.3 Structure

Chapter two deals with the legal requirements for PbD in Art. 25.1 of the GDPR. The first part looks into whether or not PbD in Art. 25.1 is intended to be directly enforceable. This will indicate how serious a controller must embrace PbD. The second part addresses 'technical and organisational measures' that controllers must implement with the ambition to concretise what such measures could consist of and which measures controllers should respectively could implement in the strive to comply with Art. 25.1. The third part of chapter two is an attempt to analyse 'appropriate' in order to clarify what it could mean from various different angles, both covering the overall picture when undertaking a proportionality assessment and more in detail what appropriate could be in practice. Chapter three deals with the proportionality-like assessment as well as the conditions that have the greatest impact on such an assessment that the controller is tasked with when choosing which measures to implement and which to disregard in the strive towards achieving compliance with Art. 25.1. These conditions are vagueness of the legal requirements, potential for enforcement of non-compliance, present incentives for implementing PbD, available means for processing and controllers position to influence these means, the proportionality-like assessment that controllers must undertake and the difficulty balancing various conflicting interests against each other, and the available guidance for how to successfully implement appropriate measures. In my view, such surrounding conditions greatly affecting the potential to implement the correct measures, should have an impact on what can be expected from controllers in this regard, i.e. the conditions can be used to calibrate expectations. Apart from a few elements, future assessments of compliance with Art. 25.1 should have an overall character as this is how Art. 25.1 is constructed. Therefore, what to expect in regards to controller performance should impact potential assessments of compliance. This will be elaborated upon in chapter four together with consequences for potentially unsatisfactory conditions for successful implementation of PbD.

2 What is required by Art. 25.1 GDPR

The first observation is that the entire Art. 25.1 actually consists of but one very long sentence. The structure is very complicated with several subordinate clauses making the process of understanding Art. 25.1 everything but simple. In order to better understand the obligations resting upon the controller, the legal preconditions in Art. 25.1 could be analysed one at a time. Whether or not PbD in Art. 25.1 is intended to be directly enforceable rather than being more of a vision to strive towards can serve as a starting point. The outcome will indicate how serious a controller must take the requirements of Art. 25.1.

2.1 What risks does non-compliance entail?

According to Art. 83(4)(a) of the GDPR it is apparent that infringement of Art. 25 is a possibility. Potential infringement is backed up by heavy sanctions. In fact, under Art. 83(4) a controller can "be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher." Thus, it seems clear that compliance with Art. 25.1 is not only intended by the legislator but also combined with rather hefty and enforceable remedies, at least in theory. When the supervisory authority is to assess potential infringements of the obligations in Art. 25 they shall, according to recital 150, in each individual case take into account "[…] all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement." In addition, the obligation for the controller to implement appropriate technical and organisational measures is repeated in Art. 24.1 combined with an obligation for the controller to "[…] demonstrate that processing is performed in accordance with this Regulation." In other words, the controller is under obligation to actually demonstrate compliance with GDPR. Therefore, a controller cannot solely rely on the abstract legal requirements for justifying doing nothing in relation to the issue of implementing PbD. However, complying with the obligations of the controller pursuant of Art. 25.1 remains a rather vague and therefore challenging endeavour.

2.2 Technical and organisational measures

From the wordings of Art. 25.1 it is apparent that the controller must take certain steps on both a technical and organisational level when implementing PbD. Spiekerman defines PbD "[…] as an engineering *and* strategic management approach that commits to selectively and sustainably minimize information systems' privacy risks through technical *and* governance controls."[18] The view of the European Commission is that the principle of PbD "[…] means

[18] Spiekerman, "The challenges of Privacy by Design", 38.

that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal."[19] According to Cavoukian[20], PbD must consist of effort at all relevant fronts, neither solely relying in technology nor policy in "[…] a suite of privacy protections that brings together regulatory instruments, consumer awareness and education, accountability and transparency, audit and control, and market forces.[21] In order to successfully implement PbD that lives up to the task of protecting privacy, one must have focus on seven principles that Cavoukian presents as the essence of PbD. First, one must aim for a *proactive and preventive approach* - as opposed to classic regulatory setup PbD is supposed to have an *ex ante* aura, i.e. constituting a proactive and preventive rather than a reactive and remedial approach.[22] Controllers must also strive towards *enabling privacy as default mode, enabling a symbiotic approach rather than a confrontational* (win-win scenario), and make sure PbD is *an integral part of the processing of data* where privacy shall be the default mode in any system, providing privacy protection as an automatic response where the user is passive, i.e. there is no need for action in order to ensure one's privacy.[23] Finally, controllers must work towards making PbD an *ever-present factor* from the cradle to the grave of every system, uphold *trust through verification and* enable *incorporation of visibility and transparency* into the code, and make sure privacy is a *core part of any organisational culture*.[24] According to Kroener & Wright, for a controller to establish what must be done, the context of the processing operations and the risks towards the rights of the data subjects must be analysed through a Privacy Impact Assessment (PIA).[25]

2.2.1 What are technical measures?

For a controller, the short version of the obligation of implementing technical measures is encoding proper commands that correspond to certain legal requirements into the software in which the processing of personal data is carried out. The technical measures component of PbD correspond in many ways to PETs, which could consist of functionalities such as anonymity, pseudonimity, unlinkablility and unobservability.[26] The European Commission perceive PETs as "[…] a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired

[19] COM(2010) 609 final note 30, 12.

[20] Ann Cavoukian is the former Privacy Commissioner of Ontario Canada and is considered to be the one of the primary influences and advocates of PbD.

[21] Cavoukian, "Privacy by Design", 251.

[22] Cavoukian, "Privacy by Design", 249.

[23] Cavoukian, "Privacy by Design", 250.

[24] Cavoukian, "Privacy by Design", 250.

[25] Kroener and Wright, "A Strategy for Operationalizing Privacy by Design", 361-362.

[26] van Lieshout et. al., "Privacy by Design", 61.

processing of personal data, all without losing the functionality of the information system."[27] PbD is however in this regard to be understood in a broader perspective than PETs. Rather than merely introducing technical measures, the information system itself must be designed in such a way as to account for and safeguard privacy as PbD "[…] refers to the underlying philosophy of protecting privacy in the early design stage of technological development."[28] Thus, one way to see PbD is to treat privacy protection as "[…] a system requirement that must be treated like any other functional requirement."[29] Subsequently, one issue that will prove challenging is that privacy "[…] is generally not the primary requirement of a system and it may even come into conflict with other (functional or non-functional) requirements."[30]

Art. 25.1 offers but little guidance on what could be meant by technical measures in a practice apart from providing the examples of pseudonymisation and data minimisation. As these are mere examples, solely implementing pseudonymisation and account for the principle of data minimisation is likely insufficient in order to comply with Art. 25.1 with regards to technical measures. The responsibility for the controller is emphasised in recital 78 and in order for him to assure and manifest compliance with the Regulation he should adopt both internal policies and implement certain measures. The burden resting on the controller is then followed by an attempt to make 'implementing measures' more concrete, whereas "such measures could consist, *inter alia*, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features." The fact that the word *could* is being used, especially combined with *inter alia*, can be interpreted as either providing examples of measures that, if deemed necessary, must be implemented or that there simply is no *must* regarding the implementation of PbD. To what extent legal requirements are supposed to be hard-coded into software and how much discretion controllers are allowed regarding implementation, as long as the requirements of the Regulation are met, is not addressed in recital 78.

Clarifying why PbD should be implemented might provide some guidance on what to do regarding technical measures. On the matter of the end-results it has been suggested that "the goals of technical measures to protect privacy are to make it difficult (if not practically impossible) to link a piece of information to a natural person, to limit the processing of personal data to defined uses, and to give users control over their personal data once their data

[27] COM/2007/0228 final, *under* 2 'what are pets?'

[28] Koops, Hoepman and Leenes, "Open-source intelligence", 678.

[29] Koops, Hoepman and Leenes, "Open-source intelligence", 678.

[30] Danezis et. al., "Privacy and Data Protection by Design", 11.

are disclosed."[31] To reach such goals and to avoid breach of privacy requirements as often as possible, the system should be designed to embrace automatic enforcement.[32] Such an approach is in line with the first of Cavoukian's seven PbD principles. According to Schartum, the technical measures (computerized aspects) in upholding privacy by automation is "[…] by far the most important privacy-supporting element."[33]

2.2.2 What are organisational measures?

Just as with the technical aspects, organisational measures can be represented through a myriad of activities and actions. The central aspect is ensuring the organisation is sufficiently influenced by the notion of upholding and protecting privacy and as processing of personal data requires both software and human resources, the aspects of technical and organisational measures are entwined. As there are various interpretations of privacy, organisations need to clarify the interpretation of privacy and make sure it is well known among all employees. In other words, privacy must be incorporated in the core of the organisation.[34] The primary step is according to Spiekerman for the organisation to understand what it is they actually seek to protect.[35] The organisation must foster "[…] the right mindset of those responsible for developing and running data processing systems."[36] Upholding privacy must flow naturally through any organisation, and PbD "[…] should penetrate the actual working culture and the decisions taken in an organisation."[37] Such a corporate culture of privacy can be achieved through "[…] internal policies and guidelines regarding data processing, regular monitoring and auditing of business processes, appointing a chief privacy officer and privacy and data protection committees, the training of staff and formulating corporate values that reflect the importance of privacy protection."[38] Among the things above, chief privacy officer is quite similar to the rule in Art. 35 of the GDPR requiring the appointment of a Data Protection Officer (DPO).

As organisational measures encompass proper processing in accordance with the general principles of EU privacy law for processing personal data in Art. 5.1, the controller must make sure that this is the case in practice as well. Protection against unauthorized processing in Art. 5.1(f) can be dealt with through various organisational steps such as internal access

[31] Koops, Hoepman and Leenes, "Open-source intelligence", 678.
[32] Bygrave, "Hardwiring Privacy", 2.
[33] Schartum, "Making privacy by design operative", 154.
[34] Cavoukian, "Privacy by Design", 250.
[35] Spiekerman, "The challenges of privacy by design", 39.
[36] Koops and Leenes, "Privacy regulation cannot be hardcoded", 168.
[37] Tsormpatzoudi, Berendt, and Coudert. "Privacy by Design: From Research and Policy to Practice, 205.
[38] van Lieshout et. al., "Privacy by Design", 62.

rules and contractual obligations. In addition, there ought to be some kind of process upholding accountability.[39] To provide for this the organisation must, as indicated in recital 78, adopt internal polices corresponding to the legal requirements.[40] One useful organisational measure is Enterprise Privacy Polices, i.e. basically tools describing how the organisation will achieve compliance with data privacy law and to provide means for accountability.[41] Such policies can facilitate the process of specifying the conditions for data collection and processing and for which purposes, essential components for complying with privacy law requirements.[42] Accountability also depend upon "mechanisms to put privacy policies into effect, including tools, training, and education" as well as providing for systematical oversight and external reviews so that operations indeed match the rules.[43] According to Spiekerman, PbD requires strong engagement on management level which cannot be taken for granted without accountability in the system.[44] As the controller under Art. 5.2 is accountable for and shall be able to demonstrate compliance with the general principles relating to processing of personal data, accountability is a vital component in a proper PbD-regime, which in turn could manifest taking the issue of privacy for data subjects seriously.[45]

2.2.3 When must the measures be implemented?

With Art. 25.1 the legislator has intended for the controller to be responsible not only during the actual processing of data but "at the time of the determination of the means for processing" as well. Such a duality must be understood in order to have an effective compliance. PbD in Art. 25.1 does seemingly have a classic *ex post*-perspective but it is combined with an *ex ante*-perspective, as the controller might violate Art. 25.1 if not adhering to requirements already at the stage where means for processing is to be determined, i.e. long before any actual processing of personal data takes place. In order to realise the goals of PbD there ought to be a lean more towards *ex ante* rather than *ex post*.[46]

According to Schaar, implementation of PbD must take place at the very beginning of creating a new software and continue being a central aspect in the development of the software all through the life span, if one wants to avoid a difficult and costly process.[47]

---

[39] Kroener and Wright, "A Strategy for Operationalizing Privacy by Design", 362.

[40] Cavoukian, Taylor and Abrams, "Privacy by Design", 409.

[41] Koops, Hoepman and Leenes, "Open-source intelligence", 682. *See also* van Lieshout et. al., "Privacy by Design", 62.

[42] Koops, Hoepman and Leenes, "Open-source intelligence", 683.

[43] Cavoukian, Taylor and Abrams, "Privacy by Design", 409.

[44] Spiekerman, "The challenges of privacy by design", 39.

[45] Guagnin et al., *Managing Privacy Through Accountability*, 6.

[46] Bygrave, "Hardwiring Privacy", 2.

[47] Schaar, "Privacy by Design", 267.

Making privacy protection central features in the software already from the start is far less likely to provide future legal friction as opposed to system capabilities "[…] simply grafted on to the technology late in the development process."[48] Such an approach will save both time and money, as "[…] new technological systems often contain hidden dangers which are very difficult to overcome after the basic design has been worked out."[49] In other words, patches might not be a viable option when implementing PbD through engineering. In contrast, it has been suggested that there is really no available data to support that privacy would improve and the costs for implementation will be reduced if implemented in the beginning of a development face rather than being patched on at a later stage.[50] Regardless, while there is potential for implementing PbD already at the creation of new information systems, it is not possible fully applying it on already existing systems. For existing systems adaptations seems inevitable.

2.3 What is 'appropriate'?

The requirement of 'appropriate' seem to be a key word when trying to establish what a controller must do in order to comply with Art. 25.1. Some things are simply better achieved through technology, e.g. 'revocable privacy' which concern data minimisation, building upon the claim that law is sometimes insufficient dealing with certain issues.[51] Embracing revocable privacy could therefore be an example of an appropriate measure.

Appropriate is similar to proportionate and though there are no explicit reference to proportionality in Art. 25.1, there was such a reference in an earlier version of the GDPR, where the controller under Art. 23.1 was obliged to "[…] implement appropriate ***and proportionate*** technical and organisational measures and procedures […]".[52] Though proportionality no longer is mentioned in Art. 25.1 it can be helpful bearing in mind the principle of proportionality when deciding which measures to implement, not least given the strong position of proportionality within EU law in general. Balancing various interests against each other, as required in Art. 25.1, is in my view an exercise in proportionality. According to Hildebrandt and Tielemans, the choice of "[…] the term 'appropriate' shows that the controller still has discretion concerning which technical measures or procedures he will implement."[53] As 'appropriate' then might be an indicator of a certain margin of

[48] Lerner, *The Architecture of Privacy*, xv [preface].

[49] Schaar, "Privacy by Design", 267.

[50] Rubinstein and Good, "Privacy by Design", 1335-1336.

[51] Koops, Hoepman and Leenes, "Open-source intelligence", 681.

[52] European Parliament legislative resolution of 12 March 2014 on the proposal for a General Data Protection Regulation.

[53] Hildebrandt and Tielemans, "Data protection by design and technology neutral law", 517.

appreciation awarded the controller in the quest of balancing various interests against each other when choosing which measures to implement, such a balancing act must be done in a proportionate way to justify the outcome. If indeed implementing measures that are appropriate, and the choices what to implement and what not to are a product influenced by proportionality in each individual context and therefore can be properly justified, appropriate could also correspond to a minimum level of undertaken measures with regard to obligations for the controller.

2.3.1 Measures with high potential and low cost of implementation

Focusing on the best suited legal requirements that are also relatively cheap and easy to implement in a PbD-regime might be a way to embrace proportionality. The lesser the effort for implementing certain legal requirements in ones PbD-regime, the lesser the chance of success for arguing why implementation has not been made based on the principle of proportionality. Koops et al. have identified some requirements in DPD as"[…] having the most potential for a techno-regulation approach"[54], i.e. purpose specification (Art. 6(b) DPD), legal basis (Art. 6(a) and 7), collection and use limitation/data minimization (Art. 6(c)), data quality (Art. 6(d)), rights of data subject (Art. 12) and security safeguards (Art. 17). Could the requirements identified in DPD as having the most potential for techno-regulation also be construed as being appropriate since they can more easily be transformed into computer code and thus having effect at a relatively low cost? If the measures are proportionate, they are most likely appropriate. The greater the number of legal requirements covered by an organisations PbD-regime the greater the chance for successfully arguing against implementing any given measure related with costly and difficult implementation based on the principle of proportionality.

2.3.2 Implementation depending of context

What to implement depends on what is to be achieved and the context in which it will be applied.[55] In fact, PbD must be interpreted through context, balance of various interests and expertise among engineers as there is "[…] no one way of solving the problems."[56] This will obviously make it hard to establishing exactly what a controller must do to comply with PbD with regard to specific measures. Instead, there must be a proportionate overall assessment of the context resulting in choices of which measures to implement. The controller must therefore identify the context in which the processing operations take place. In addition, it is vital, according to the European Union Agency for Network and Information Security

[54] Koops, Hoepman and Leenes, "Open-source intelligence", 683-684.

[55] Koops, Hoepman and Leenes, "Open-source intelligence", 681.

[56] Gürses, Troncoso and Diaz, "Engineering Privacy by Design", *under* 'abstract', 1.

(ENISA), identifying and defining the goals of each and every PbD-process.[57] The controller must also be aware of all relevant potential risks that might arise from current or future processing operations. PIAs can be used to identify the context, potential risks and goals of a PbD-process.[58]

2.3.3 Role of Privacy Impact Assessment?

PIAs concern not only technical but organisational measures as well.[59] Main objectives of a PIA are to identify risks, solutions and stakeholders in order to consult stakeholders, formulate and implement recommendations and enable reviews, audits and accountability measures.[60] Identifying and properly addressing "[…] the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing […]" is a central element in Art. 25.1. In the overall proportionality assessment where the controller shall determine which measures are appropriate and therefore should be implemented, the risks posed by the processing will certainly have a substantial impact. A similar approach called 'Functional Requirements Analysis' is based on treating data minimisation as an essential component, modelling attackers, threats and risks, analysing security requirements and implementing and testing the design.[61] Regardless of what means are used for identifying such risks, they must be identified. Hence, if there are no other alternatives for analysing risks, the controller should definitely consider the usefulness of PIAs. Indeed, it has been claimed that PIAs actually form part of the PbD-approach.[62] PIAs can also serve the purpose of manifesting compliance, something that is required by Art. 24.1 GDPR. In fact, proper execution of a PIA can "[…] reduce or even eliminate any liability, negative publicity and loss of reputation."[63]

PIA is clearly a helpful tool identifying what must be done in respect of privacy. However, it is not mandatory in relation to PbD. In fact, there is no explicit reference to any connection between PIA and PbD in neither Art. 25.1 nor Art. 35 (regarding PIA) in the final version of GDPR. That said, the non-existing connection between PIA and PbD in relation to legislation is likely a product of compromise as such a connection indeed has been on the legislative agenda. In a proposal from the European Parliament in March 2014, the then current provision on PbD (Art. 23.1 of the proposed GDPR) stated that "[w]here the controller has

[57] Danezis et. al., "Privacy and Data Protection by Design", 11.

[58] Danezis et. al., "Privacy and Data Protection by Design", 11.

[59] van Lieshout et. al., "Privacy by Design", 62.

[60] Danezis et. al., "Privacy and Data Protection by Design", 12.

[61] Gürses, Troncoso and Diaz, "Engineering Privacy by Design", *under* 3.3, 18.

[62] van Lieshout et. al., "Privacy by Design", 58.

[63] Wright, "The state of the art in privacy impact assessment", 55.

carried out a data protection impact assessment pursuant to Article 33, the results shall be taken into account when developing those measures and procedures."[64] Thus, undertaking a proper PIA and act accordingly to address the result of the analysis might be in the interest of any controller pursuing manifestation of compliance regardless of the fact that it is not mandatory undertaking a PIA in order to comply with Art. 25.1 of GDPR.

2.3.4 Role of Data Protection Officer?

Appointing a DPO under Art. 37 is not mandatory for every organisation.[65] Moreover, regardless if an organisation is mandated to appoint a DPO or not, there is no explicit connection establishing the need for a DPO in order to fulfil the obligations under Art. 25.1. There is no mentioning of Art. 25.1 or PbD in Art. 39 dealing with the required tasks of a DPO. However, such a connection between PbD and DPO used to exist in earlier version of the GDPR. Recital 75a of the proposed GDPR stated that DPOs must have "[…] at least the following qualifications: extensive knowledge of the substance and application of data protection law, including technical and organizational measures and procedures; mastery of technical requirements for privacy by design, privacy by default and data security."[66] Clearly there was an intention from part of the legislative community to connect DPOs with the process of PbD and even though such a connection was stricken in the final version of GDPR, the significance of having a DPO in the process of complying with PbD must not be neglected. Having a DPO is clearly an advantage for the process of assessing what must be done regarding PbD as a DPO under Art. 37(5) is expected to have "[…] expert knowledge of data protection law and practices […]." Though the explicit connection between DPO and PbD is no longer in force, the legislator must have envisioned an intimate collaboration between the DPO and the controller in the process of implementing PbD as recital 97 states that "[…] a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation." In fact, the presence of a DPO has even been labelled as "[…] a cornerstone in the implementation of PbD"[67]. Furthermore, DPOs are expected to have a certain amount of independence in relation to the employer, something that can prove useful supposed to "[…] promote the dialogue between different departments and eventually strike the balance between different interests under the common goal of implementing privacy/data protection by design."[68] A DPO can

[64] European Parliament legislative resolution of 12 March 2014 on the proposal for a General Data Protection Regulation.

[65] Prior versions of the GDPR had a fixed cap where the obligation set in for organisations with more than 250 employees. The final version of GDPR does not however hold any such limitation.

[66] Kroener and Wright, "A Strategy for Operationalizing Privacy by Design", 358-359.

[67] Tsormpatzoudi, Berendt, and Coudert. "Privacy by Design: From Research and Policy to Practice", 205.

[68] Tsormpatzoudi, Berendt, and Coudert. "Privacy by Design: From Research and Policy to Practice", 206.

also be a valuable asset when it comes to identifying and handling potential risks for violating the rights of data subjects which is a central feature in Art. 25.1.

2.3.5 In order to meet the requirements of the Regulation?

The way in which Art. 25.1 is formulated, "[…] in order to meet the requirements of this Regulation and protect the rights of data subjects […]", raises a few questions. For example, is meeting the requirements of the GDPR not identical with protecting the rights of the data subjects? The fuzzy wording is making the already complex notion of PbD even more blurry. Moreover, is PbD to be interpreted as an obligation to encompass all the requirements in the entire GDPR? Perhaps there are some things in the GDPR than cannot be achieved without implementing PbD? Or is it more a reminder for the controller than when undertaking his balancing act between various interests when implementing PbD, he can never go along with measures that violate any of the requirements in GDPR? If so, why would such a reminder be necessary? Is not each requirement sufficient in itself as a rule with enforceable consequences? It has been stated that "various data protection requirements should be considered as important candidates for being protected through privacy by design […]"[69] Thus, every single requirement in GDPR simply cannot be suited for being encompassed by PbD. This at least gives us the clue that the phrasing in Art. 25.1 is not to be interpreted as encouraging controllers to seek to put everything in the PbD pot. However, that leaves us with the question hanging – what is the meaning of the wording? It seems a bit farfetched solely serving the purpose of a reminder for the controller to not violate any other requirement in GDPR through the coming PbD-regime. One thing is sure at least, it offers no guidance to the interpretation and assessment of what might be 'appropriate' measures apart from a potential reminder that any PbD-regime must not violate any other requirement within GDPR.

2.3.6 Any guidance from earlier versions of the GDPR?

The following is provided amendments for the then current proposal for GDPR and PbD (former Art. 23.1 corresponding to current Art. 25.1) by the European Parliament (amended version of March 2014):

"Having regard to the state of the art ~~and the cost of implementation~~ , ***current technical knowledge, international best practices and the risks represented by the data processing,*** the controller ***and the processor, if any,*** shall, both at the time of the determination of the ***purposes and*** means for processing and at the time of the processing itself, implement appropriate ***and proportionate*** technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the

[69] Koops, Hoepman and Leenes, "Open-source intelligence", 686.

protection of the rights of the data subject***, in particular with regard to the principles laid down in Article 5. Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. Where the controller has carried out a data protection impact assessment pursuant to Article 33, the results shall be taken into account when developing those measures and procedures***."[70]
The proposal, in contrast to the final version, explicitly mention proportionality and refers especially to Art. 5 of the draft (Principles relating to personal data processing) i.e. *lawfulness, fairness and transparency*, *purpose limitation*, *data minimisation*, *accuracy*, *storage minimisation, effectiveness, integrity*, and *accountability*. Now, the final version of GDPR contain but few of the proposed references and their importance must therefore have been reduced. However, the draft proposal can serve as basis for interpretation of what a controller should focus upon to achieve compliance with PbD. For example, the European Parliament obviously did not want to have any emphasis on the cost of implementation but since this requirement ended up in the final version it is clear that in establishing what measures is appropriate, the cost is a relevant factor. If a certain measure is very costly in regards of implementation, any controller should have a chance of success for arguing why that measure was opted out in relation to the costs. Though no longer required by GDPR, undertaking a PIA that embraces accuracy, confidentiality, integrity, physical security and deletion of personal data might be an important step towards fulfilling implementation of appropriate technical and organisational measures.

The former article dealing with PbD, Art. 23.1, also explicitly mention that particular regard shall be awarded "[…] to the entire lifecycle management of personal data from collection to processing to deletion." In recital 61 of the proposal it is clarified that PbD "[…] requires data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal." It seems that the life cycle reference in Art. 23.1 is mainly targeting the means for carrying out processing, as former recital 61 continues stating that "[…] this should also include the responsibility for the products and services used by the controller." While the responsibility resting on the controller for trying to create or adjust the means for processing data prior of, during and after any processing operations still remain under current Art. 25.1, any potential obligations for software and hardware producers have been relaxed under the final version of GDPR. Current recital 78 merely states that "[…] producers of the products, services and applications should

[70] European Parliament legislative resolution of 12 March 2014 on the proposal for a General Data Protection Regulation. *Italics and bold letters added for visualisation.*

be encouraged to take into account the right to data protection when developing and designing such products, services and applications and […] to make sure that controllers and processors are able to fulfil their data protection obligations". As provided by recital 78, controllers are only able to fulfil their data protection obligations if they have access to proper tools. Given that the influence on and the development of the means for processing is in the hand of producers rather than controllers, the obligation regarding life cycle approach for controllers cannot be greater than the controllers power to influence the design of the means for processing data. Potential non-compliance must therefore only be an issue if proper tools are available and the controller still opts to dismiss using such tools (if such usage is not disproportionately costly).

2.3.7 Relevance of non-exhaustive list of examples

While the final version of Art. 25.1 is less specific than the previous proposals it nevertheless contains some specifications on what might be deemed as an appropriate measure, i.e. pseudonymisation and what kind of principles the legislator awards special attention, i.e. data minimisation. Clearly they are mere examples evident from the use of the expression *such as*, but while the legislator does not intend to suggest that by implementing pseudonymisation and data minimisation a controller will have fulfilled his obligations, the examples must be interpreted as having such a significance that explicit references to them ended up in the final version. While providing more examples, recital 78 seems however to elaborate upon the same rationale as Art. 25.1. Thus, appropriate measures "[…] could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features." As indicated by *inter alia* in recital 78, the list of examples is non-exhaustive and one cannot therefore rely upon only focusing on the examples mentioned. Among other things in the recital could likely by anonymization, as it is similar to pseudonymisation but in addition an even safer approach. Other examples could be storage minimisation and deletion of data as soon as possible. However, by the same rationale as mentioned above in relation to Art. 25.1 and in the absence of more specific guidance, one can assume that if the mentioned measures are needed or even useful for the protection of privacy in any processing operation, they should definitely be awarded significance. As it seems quite clear that most PbD-implementations are context based, the rationale behind the examples in Art. 25.1 and recital 78 might just be an attempt to isolate any general requirements that will apply for most or all processing operations. It could therefore be wise for any controller to attempt implementation on all the given examples building upon the logic that the clearer a requirement, the stricter the obligation to comply with it.

2.3.7.1 Pseudonymisation and anonymization

PbD is not the only novelty introduced by GDPR. Pseudonymisation, in removing linkage so that identification is not possible without addition of separate information, is a middle way between anonymous data on the one hand and directly identifiable data on the other.[71] To fully embrace it, the process of pseudonymising personal data shall take place as soon as possible in any processing operation.[72] The technique can according to recital 28 "[…] can reduce risks to the data subjects." While anonymization is the safest of the two techniques pseudonymisation have potential for "[…] significantly reduce the risks associated with data processing, while also maintaining the data's utility."[73] The utility is higher compared to completely anonymised data. Pseudonymisation is a quite rare example of incentives provided by the legislator for implementing PbD. In fact, creating incentives to apply pseudonymisation is explicitly stated in recital 29 as a clear aim of the GDPR. Thus, "[…] the GDPR relaxes several requirements on controllers that use the technique."[74] One example is the potential exception from the principle of purpose limitation in Art. 5. Processing for another purpose can according to Art. 6(4) be compatible with the purpose for which the personal data are initially collected if certain requirements are met, *inter alia* "the existence of appropriate safeguards, which may include encryption or pseudonymisation."[75] Another example is the notification requirements in Art. 34, where controllers in the case of security incidents that "[…] is likely to result in a high risk" to the rights of the data subjects must notify each affected data subject. As psudonymisation "[…] reduces the risk of harm to data subjects, controllers that use it may be able to avoid notification of security incidents."[76] This concept is clearly worth contemplating for controllers as it is one of few situations where safeguarding privacy is not to the same extent in conflict with other interests or requirements.

While many things regarding PbD remain unclear, the intention is in contrast rather obvious as the legislator wants controllers to embrace pseudonymisation. Thus one could fairly safe draw two conclusions from this. First, given that pseudonymisation is a kind of compromise between anonymity and utility, the controller should be free to choose between either pseudonymisation or anonymization or opting to use them both. Taking into account the legislators will to compromise between anonymity and utility and the fact that pseudonymisation is forcefully promoted and combined with incentives, the second

---

[71] Maldoff, Gabriel, "Pseudonymization", *under* 'GDPR encourages "pseudonymization" of personal data'.

[72] Recital 78.

[73] Maldoff, Gabriel, "Pseudonymization", *under* 'GDPR encourages "pseudonymization" of personal data'.

[74] Maldoff, Gabriel, "Pseudonymization", *under* 'GDPR encourages "pseudonymization" of personal data'.

[75] Art. 6(4)(e)

[76] Maldoff, Gabriel, "Pseudonymization", *under* 'Controllers can use pseudonymization to help meet the GDPR's data security requirements.'.

conclusion would be that utilising pseudonymisation/anonymization is not a free choice. Adding the fact that pseudonymisation is explicitly mentioned as an example of an appropriate measure in Art. 25.1, this technique should not be dismissed by any controller. In a sense, it appears that pseudonymisation is one of the clearest practical examples of an obligation for controllers to undertake. Justification for not using this technique must surely be based on establishing that it is absolutely unnecessary and that the rights of the data subjects is significantly safeguarded through other existing measures.

2.3.7.2 Data minimisation

While anonymization and pseudonymisation deals with manipulation of data as to reduce or eliminate potential for identification, data minimisation is aimed to minimise collection and processing of data. Thus, pseudonymisation/anonymization and data mimimisation tend to work in a cumulative rather than in an alternative way. In other words, one does not really rule out the other, they are both vital components to adhere to the requirements of Art. 25.1. This cumulative relation is also hinted by the wording in Art. 25.1.

It has been suggested that data minimisation is a vital component for implementing PbD through engineering, i.e. a technical measure that likely must be implemented in order to comply with PbD.[77] Schaar suggests that PbD should be interpreted as building upon data minimisation as one of its core foundations.[78] Data minimisation is in contrast with the current development in the modern society, as the tendencies are an increase in collection of data and subsequently sharing it with other entities.[79] One thing seems clear however in that Art. 25.1 GDPR "[…] prohibits controllers from using technologies that collect more personal data than is strictly necessary for technological functionality or that undermine data confidentiality"[80]. That said, recognising the importance of data minimisation, it is quite odd that it is not explicitly mentioned in the DPD. This lack of mention can have the effect that the proportionality requirement ends up getting completely reversed effect of what is intended as data collection can be empowered rather than hindered through the purpose specification arguing the necessity of the data combined with the notion of control through informed consent and access rights as mitigators.[81] This risk is now dealt with by GDPR. Though the final version of GDPR still lack a proper definition of PbD, it does however have explicit reference to the principle of data minimisation.[82] It has been suggested, prior of the final

[77] Gürses, Troncoso and Diaz, "Engineering Privacy by Design", *under* 'abstract', 1.

[78] Schaar, "Privacy by Design", 271.

[79] Gürses, Troncoso and Diaz, "Engineering Privacy by Design", *under* 2.1, 4.

[80] Bygrave, "Hardwiring Privacy", 19.

[81] Gürses, Troncoso and Diaz, "Engineering Privacy by Design", *under* 2.1, 4.

[82] Gürses, Troncoso and Diaz, "Engineering Privacy by Design", *under* 2.1, 5.

version of GDPR, that PbD can come into conflict with the principle of data minimisation.[83] The fact that data minimisation is now explicitly connected with PbD and thus must be taken into consideration might reduce the risk of such a conflict.

Given the importance of data minimisation and the explicit reference in GDPR it seems that controllers do wise in embracing the principle, preferably in as intimate connection with default settings as possible, in the pursuit towards implementing PbD.

2.3.7.3 Default settings

From Cavoukian's seven principles of PbD, privacy as default setting is especially eligible for making information systems more privacy friendly and can be manifested e.g. through 'no' as the default option regarding requests for consent for GPS tracking.[84] Default as one way to uphold PbD in certain cases, is supported by the fact that Art. 25.2 GDPR implicitly states that privacy should be considered through default settings. Default settings is a way to successfully uphold the principle of data minimisation.[85] While no longer explicitly mentioned in neither Art. 25.2 nor recital 78, in a prior proposed version of GDPR recital 61 states that privacy by default requires settings "[…] which should by default comply with the general principles of data protection, such as data minimisation and purpose limitation."[86] However, according to Schartum default is only an issue regarding situations concerning consent "[…] when data subjects make choices having an impact on their privacy" thus limiting the importance of default in the sense of part of complying with PbD.[87] On the other hand, default has been said to be a vital component in upholding privacy in a digital environment, not least since many users, i.e. data subjects, have but limited IT skills and knowledge.[88] By the wording of Art. 25.2 it seems that the legislator deemed negating access to personal data "[…] without the individual's intervention […]" especially important. Opting for default settings where possible would perhaps be a wise path to take for any controller striving to comply with PbD. Privacy as default setting also clarifies consent and makes the presence of active consent more clear.

---

[83] Koops and Leenes, "Privacy regulation cannot be hardcoded", 166.

[84] Schartum, "Making privacy by design operative", 155.

[85] Koops, Hoepman and Leenes, "Open-source intelligence", 678.

[86] European Parliament legislative resolution of 12 March 2014 on the proposal for a General Data Protection Regulation.

[87] Schartum, "Making privacy by design operative", 155.

[88] Schaar, "Privacy by Design", 267.

2.3.7.4 Transparency

As proposed in recital 78, transparency with regard to the functions and processing of personal data could be an appropriate measure for a controller to take under consideration. Transparency is important from several perspectives, e.g. for enabling data subjects to exercise their rights under privacy law and for authorities and regulatory bodies to be able to monitor and enforce the law.[89] Transparency has to be present before, during and after any processing of personal data, and it "[…] ensures that all privacy-relevant data processing including the legal, technical and organisational setting can be understood and reconstructed at any time."[90] Various measures could contribute to upholding transparency, e.g. "[…] logging and reporting, an understandable documentation covering technology, organisation, responsibilities, the source code, privacy policies, notifications, information of and communication with the persons whose data are being processed."[91] Thus, transparency is a basis for accountability but also for cooperation, which is mandated under GDPR, e.g. between supervisory authorities and controllers.[92] Transparency could therefore prove useful for a controller not only from a cooperative view enabling assistance and enforcement through monitoring, but as a way to demonstrate taking privacy seriously towards data subjects. In enabling data subjects to exercise their rights, the controller can at the same time demonstrate the organisation's strive to uphold privacy which can come in handy in an overall assessment of compliance with PbD.

[89] Danezis et. al., "Privacy and Data Protection by Design", 1.

[90] Danezis et. al., "Privacy and Data Protection by Design", 7.

[91] Danezis et. al., "Privacy and Data Protection by Design", 7.

[92] Danezis et. al., "Privacy and Data Protection by Design", 7.

3 Conditions for complying with PbD not optimal

Some requirements are likely to address more or less any processing operation and a controller might be wise to embrace such measures that are explicitly mentioned, e.g. pseudonymisation and adhere to the principle of data minimisation. However, some necessary and appropriate measures depend upon the context in which processing of personal data is carried out. To make sure the collective sum of implemented measures suffices to complying with Art. 25.1, controllers may depend upon guidance from secondary sources, having access to proper tools (software), and relevant information as to successfully balance between various conflicting interests in a proportionate way in the presence of a rather allowing margin of appreciation. In other words, the controller faced with a tricky situation especially when being obliged under Art. 24.1 to demonstrate through technical and organisational measures "[…] that processing is performed in accordance with this Regulation."

The aim for this chapter is to analyse the present conditions for attempting to comply with Art. 25.1 in the light of the vagueness of the legal requirements. From such an analysis one could then deduce some kind of reasonable expectations on what controllers could achieve under present conditions in order to calibrate future assessments of compliance with Art. 25.1.

3.1 PbD in Art. 25.1 is a rather vague concept

At the time of prior versions of GDPR, it seemed unclear exactly how controllers should manage to incorporate privacy through the design process.[93] This perceived uncertainty seems to have persisted in the final version of GDPR. As Koops and Leenes put it, PbD can be interpreted either as way for regulators to put focus on a privacy mindset or as implying "[…] hard-coding the data-protection rules into machine-executable code as much as possible."[94] The concept of PbD is general and unprecise, not least regarding implementation through engineering, which will create great challenges for software engineers.[95] It has been referred to as an 'abstract notion'.[96] Kroener and Wright underline the fact that there is no explicit definition of PbD in the earlier versions of GDPR.[97] This absence of definition seems to have persisted, and Spiekerman put forward similar criticism claiming PbD is "barely specified".[98] Indeed, it has even been suggested that PbD might be of mere symbolic value, reduced to a guardian for the free flow of information and upholding consumer confidence.[99]

---

[93] Koops and Leenes, "Privacy regulation cannot be hardcoded", 160.

[94] Koops and Leenes, "Privacy regulation cannot be hardcoded", 160.

[95] Gürses, Troncoso and Diaz, "Engineering Privacy by Design", *under* 'abstract', 1.

[96] Koops, Hoepman and Leenes, "Open-source intelligence", 678.

[97] Kroener and Wright, "A Strategy for Operationalizing Privacy by Design", 359.

[98] Spiekerman, "The challenges of privacy by design", 38.

[99] Gürses, Troncoso and Diaz, "Engineering Privacy by Design", *under* 2.2, 5.

The vagueness is a bit problematic as the more clearly defined the legal requirements are the easier it is to convert law into computer code.[100] Bygrave describes it as "apart from the intimated potential disconnects between controllers and engineers, there is a problem with the vagueness of some of the hardwiring requirements placed on controllers."[101] Schartum suggests that although some challenges in designing PbD might be intertwined with regards to organisational and technical measures, such vagueness creates difficulties towards arriving at a "[…] sufficiently concrete design methodology" as "[…] each area requires a different methodological approach".[102] One logical assumption can then be that, bearing in mind the *degree of responsibility of the controller* in Art. 83, the harder it is complying with the requirements in Art. 25.1 GDPR the less of a risk for non-compliance must be present.

3.1.1 Conflict between law and the precise nature of computer code

The vagueness of the law is really demonstrative for underlining the major difference between legal code and computer code, as the former allows for interpretation while the latter through automation does not. The "[…] vague and discretionary nature of many of the rules in data privacy law creates major difficulties for hardwiring initiatives that attempt to replicate faithfully those rules as computer code and thereby to automate them".[103] While computer code must be precise and enable only predesignated choices to be made by users, law is constructed on the basis that things are rarely absolute and the application of law must allow a certain amount of interpretation and margin of appreciation.[104] Given these differences in nature between computer code and legal code, converting the latter into the former is not always doable. Controllers would surely like to avoid creating computer code based on uncertain legal requirements due to the "[…] risk of having to make expensive system redesigns and software amendments if the court of justice subsequently establishes a different rule."[105] In fact, the flexible application of many legal requirements and the subsequent need for contextual interpretation and guidance from case law and other relevant sources is perhaps the greatest obstacle to overcome.[106] As with law in general and privacy law in particular, we are dealing with "[…] an extremely nuanced field that often depends on the subjective evaluations of the legitimacy of certain actions (and those evaluations can change rapidly depending on outside factors)."[107] This problematic relationship between law and computer

[100] Schartum, "Making privacy by design operative", 159.
[101] Bygrave, "Hardwiring Privacy", 19.
[102] Schartum, "Making privacy by design operative", 153.
[103] Bygrave, "Hardwiring Privacy", 15.
[104] Koops, Hoepman and Leenes, "Open-source intelligence", 686.
[105] Schartum, "Making privacy by design operative", 159.
[106] Koops and Leenes, "Privacy regulation cannot be hardcoded", 166.
[107] Lerner, *The Architecture of Privacy*, xv [preface].

code has been described as a "[…] serious policy dilemma that makes it unrealistic to assume that privacy by design can be developed to its intended potential".[108] Thus, if the legal requirements is made too specific in detail the outcome can be more or less the same as in the case the requirements are too vague.[109] It seems that the golden middle way between vague and specific can be the way forward. [110] This tension between the precise nature of computer code and the general way in which legal requirements is formulated based on the need for interpretation, enables the assumption that far from every legal requirement can be transformed into technical measures.

3.1.2 To what extent shall rules be transformed into software?

How to design and to what extent privacy should be designed into software is all but clear.[111] Apart from explicitly mentioned measures and principles and rules clearly suitable for technical implementation, how much of the collective legal requirements in GDPR should a controller seek to convert into computer code? The European ENDORSE project, set out to implement all legal requirements of EU privacy law into software, provides to the conclusion that the challenge of hardcoding privacy was far greater than anticipated and involved so much more than merely transforming legal code into software code.[112] Given the various challenges with transforming legal code into software code, Koops and Leenes conclude that only "[…] simple and very specific rules may be suitable for hardcoding […]" and that PbD "[…] should not be interpreted as a general requirement […] to embed as many data protection requirements as possible in the design of the system."[113] Rather they suggest that the scale shall lean more towards organisational measures in pursuing compliance with PbD.[114] These findings seem to be in line with the inherent conflict between the need for precision in computer code and the general nature of the law based on the need for interpretation.

3.1.3 There is a gap between PbD and engineering

The issue of implementing PbD into digital systems is complicated by the various requirement types in information technology systems. For each legal requirement the engineer is faced with an advanced analysis in an effort to determine through what kind of IT system

[108] Schartum, "Making privacy by design operative", 152.
[109] Bygrave, "Hardwiring Privacy", 16.
[110] Bygrave, "Hardwiring Privacy", 17.
[111] Koops and Leenes, "Privacy regulation cannot be hardcoded", 160.
[112] Koops and Leenes, "Privacy regulation cannot be hardcoded", 162.
[113] Koops and Leenes, "Privacy regulation cannot be hardcoded", 167.
[114] Koops and Leenes, "Privacy regulation cannot be hardcoded", 167.

requirements should implementation by encoding be made; system level, runtime or language requirement.[115] There is rarely any symbiosis between privacy and IT system requirements.
This gap between PbD and engineering is not only a product between the different natures of law and computer code but also part and parcel of policy makers on the one hand and engineers on the other hand having different understandings of the concept of PbD and therefore are not fully aware of the situation for the other party.[116] The legislator through GDPR, repeating previous patterns, simply "[…] falls short of communicating clearly and directly with the engineering community".[117] Indeed, the gap between law and engineering is not a new phenomenon and can be visualised by the very modest deployment of PETs in the past.[118] Regulation of the digital world is a complicated story and it has been suggested that solving many of the issues is futile "[…] without lawyers who understand tech and techies who understand policies."[119] In order to achieve an intimate collaboration between lawyers and software engineers one might have to embrace a different perspective - the emergence of a new discipline could be necessary.[120] Until then, controllers will have to rely upon whatever guidance is currently available.

3.2 Effective enforcement and powerful remedies

As previously elaborated upon, the legislator clearly envisaged that non-compliance with Art. 25.1 shall be a very real possibility indeed and the enforcement have been backed up with rather hefty remedies as well. That GDPR enable powerful sanctions for non-compliance is quite clear, and it has been stated that this is an important condition for upholding compliance.[121] On the other hand, "[…] there is no necessary link between tougher enforcement powers and better compliance."[122] According to Bygrave, "[c]ompliance levels are a function of numerous factors of which enforcement powers and the ability to use such powers are just two."[123] However, in the matter of enforcement there are a few question marks. Effective enforcement relies upon supervisory authorities being capable of monitoring processing operations as well as being well informed of what the controllers must do, in order to assess if efforts made are sufficient for compliance. Supervisory authorities must be able to use the enforcement power. This seem however not to be the case as, according to Danezis et. al., the supervisory authorities "[…] lack the capacity to effectively and systematically

[115] Koops and Leenes, "Privacy regulation cannot be hardcoded", 164.
[116] Gürses, Troncoso and Diaz, "Engineering Privacy by Design", *under* 'introduction', 2.
[117] Bygrave, "Hardwiring Privacy", 20.
[118] Bygrave, "Hardwiring Privacy", 10. *See also* Koops, Hoepman and Leenes, "Open-source intelligence", 678.
[119] Paul Ohm in Lerner, *The Architecture of Privacy*, x [foreword].
[120] Paul Ohm in Lerner, *The Architecture of Privacy*, x [foreword].
[121] Danezis et. al., "Privacy and Data Protection by Design", *under* 'Key Findings', iv.
[122] Bygrave, *Data Privacy Law: An International Perspective*, 190.
[123] Bygrave, *Data Privacy Law: An International Perspective*, 190-191.

monitor data processing or penalise premeditated or negligent wrongdoing."[124] It is questionable if supervisory authorities can maintain effective enforcement. Subsequently, compliance levels will therefore depend more upon other present conditions such as incentives for implementation and available guidance for how to implement appropriate measures.

Turning to the issue of supervisory authorities being well informed. From the fact that available guidance from the supervisory authorities is far from satisfying (as the general lack of guidance otherwise would not be an issue), one assumption could be that the authorities themselves struggle with comprehending the issue of compliance with PbD. In fact, one of the objectives of the ENISA report is actually to offer guidance to and facilitate monitoring of compliance with the privacy regulation for the supervisory authorities.[125] If the supervisory authorities themselves struggle to fully grasp the concept of PbD, how much can really be expected from controllers in regard to complying with PbD, especially since GDPR build upon supervisory authorities offering consultation to controllers in certain matters, e.g. under Art. 36? Given the present circumstances it seems rationale to expect a low frequency in administrative fines for non-compliance, which can affect future compliance with Art. 25.1 in a negative way.

3.3 Incentives for implementing PbD

PETs has up till now not been particularly widely embraced.[126] While PbD now is explicitly required in legislation the underlying reasons for the unsuccessful spread of PETs are still there. One major reason for the fallacy of PETs, apart from the voluntary approach in DPD and the gap between law and engineering, is the lack of legislative incentives.[127] Incentives for implementing measures under Art. 25.1 could be provided by other sources than legislation, e.g. from demands of the data subjects. However, according to Bygrave, the scarcity of PETs is partly due to convenience and ignorance towards safety risks amongst consumers.[128] Clearly, if consumers disregard safety risks, the incentives for controllers to implement technical measures are in this regard very limited at best.

The best example of provided incentives is pseudonymisation where GDPR offer advantageous conditions for controllers using the technique.[129] Apart from this, there are

[124] Danezis et. al., "Privacy and Data Protection by Design", 1.

[125] Danezis et. al., "Privacy and Data Protection by Design", iii and 2.

[126] Koops, Hoepman and Leenes, "Open-source intelligence", 678.

[127] Koops, Hoepman and Leenes, "Open-source intelligence", 678.

[128] Bygrave, "Hardwiring Privacy", 10.

[129] Maldoff, Gabriel, "Pseudonymization", *under* 'GDPR encourages "pseudonymization" of personal data'.

really no obvious incentives in force under GDPR. The lack of incentives other than the risk of sanctions – which might be somewhat lower than intended for various reasons – is a problem not to be ignored.[130] Non-existing incentives and an unclear perception of benefits "[…] are considerable barriers for the adoption of PbD solutions by organizations."[131] In fact, compliance with PbD heavily depend upon the existence of incentives.[132] Endeavours, such as PbD, often end "[…] in failure unless significant incentives (other than the threat of punitive sanctions) exist to spur the sought-for development", and such incentives is simply not present within GDPR.[133] With lack of incentives, vagueness of the regulation and several conflicting interests as well as disinterests, it is hard to see how PbD can reach greatness.[134] Any effort to comply with Art. 25.1 must therefore be expected to correspond to the given conditions for achieving such compliance. In fact, nothing within GDPR provide any real "[…] assurance that the ideals will be extensively applied 'in the machine'."[135] Accordingly, one of the main recommendation from ENISA is for policy-makers to "[…] support the development of new incentive mechanisms"[136].

3.4 Proper software tools available?

The obligations under Art. 25.1 are directed towards controllers.[137] However, while controllers are in charge of the software toolbox, the tools themselves are often created (in collaboration with) and supplied by others, i.e. manufacturers. Though this issue is addressed in recital 78, stating that "[…] producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and […] to make sure that controllers and processors are able to fulfil their data protection obligations", it seems producers are not bound to adhere to requirements in Art. 25.1 in any particular way. In other words, Art. 25.1 "[…] targets users of the relevant data processing techniques and technologies, not their designers or manufacturers."[138] How such *encouragement* is supposed to take place as mentioned in recital 78 is not specified. One view is that "[…] by making data controllers responsible (and liable), they will force developers to come up with the right types of technologies."[139] How successful such an approach is remains to be seen.

---

[130] Bygrave, "Hardwiring Privacy", 19.

[131] van Lieshout et. al., "Privacy by Design", 64.

[132] Danezis et. al., "Privacy and Data Protection by Design", *under* 'Key Findings', iv.

[133] Bygrave, "Hardwiring Privacy", 20.

[134] Bygrave, "Hardwiring Privacy", 19-20.

[135] Bygrave, "Hardwiring Privacy", 20.

[136] Danezis et. al., "Privacy and Data Protection by Design", 50.

[137] Bygrave, "Hardwiring Privacy", 16.

[138] Hildebrandt and Tielemans, "Data protection by design and technology neutral law", 517.

[139] Hildebrandt and Tielemans, "Data protection by design and technology neutral law", 517.

As controllers are in the hands of available software produced by others and software producers are not the recipients of the requirements in Art. 25, compliance becomes a hard task to perform. The availability of privacy-friendly information systems is rather scarce.[140] In addition, there is a general lack of knowledge of privacy principles among system developers and therefor most existing software tools lack the proper fundamentals for implementing PbD.[141] Moreover, necessary prior experience for designing systems that are privacy friendly is a scarce commodity, resulting in a lack of methodologies for implementing PbD.[142] Even where the controller explicitly orders a PbD-friendly software from a software supplier the limited knowledge among controllers hamper the chances for greater success.[143] The vagueness of legal requirements further reduces the odds for successfully ordering a PbD-friendly system. Indeed, the task of engineering privacy compliant systems has even been referred to as 'nearly impossible'.[144] Given the fact that GDPR solely addresses controllers, scarce supply of proper available software might only be mitigated by time and increase in demand for such tools. Thus, to what extent is it reasonable to ask controllers to try to achieve privacy compliant systems?

3.5 Balance of interests – a slippery slope

Obliged to implement measures under art 25.1 GDPR, the controller is to undertake some kind of assessment in the light of proportionality. When assessing what kind of measures to implements, the controller shall take "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". Though not addressed in Art 25.1, controllers as compared to DPOs do not have any legally stated independence vis-à-vis the employer. Apart from self-preservation in relation to potential sanctions, have the legislator intended controllers to undertake the balancing act in Art. 25.1 in an unbiased way?

Next issue that arises from the construction of Art. 25.1 is how the controller is supposed to balance the various interests against each other? How much weight can be afforded to each individual interest, e.g. state of the art technology versus costs? The controller is faced with a difficult task in the process to decide upon which measures should be implemented as all the

[140] Schartum, "Making privacy by design operative", 154.

[141] Danezis et. al., "Privacy and Data Protection by Design", 2.

[142] Gürses, Troncoso and Diaz, "Engineering Privacy by Design", *under* 'generalization', 17.

[143] Schartum, "Making privacy by design operative", 162.

[144] Danezis et. al., "Privacy and Data Protection by Design", 50.

factors mentioned in Art. 25.1 "[…] blur the picture."[145] In fact, "[…] balancing these factors is expected to be a challenging task, given that there is no further explanation on how to interpret and prioritise them in relation to one another."[146] The European Parliament have therefore raised concerns that this balancing act, especially the passage about 'taking into account the state of the art' and 'the cost of implementation', might provide an escape route for controllers as an invitation to dodge and avoid obligations.[147] Indeed, such concerns are not unwarranted as Art. 25.1 provides controllers with a great deal of manoeuvre space.[148] Seemingly, the costs for implementing PbD are great even for smaller businesses.[149] One interpretation is that Art. 25.1 forces a controller "[…] to implement technical solutions that are available if the cost is not prohibitive."[150] This interpretation does not provide much of a guidance, as 'prohibitive' is a very subjective notion. One logical conclusion could be that costs and utilising available technology should correspond to the context and the level of potential risk against the rights of the data subjects posed by future processing operations as well as the severity of infringing these rights. High risk operations and processing of sensitive data would subsequently warrant higher costs for implementation and utilisation of state of the art technology.

Conflicting interests might also include legal requirements and information system requirements. Subsequently, one issue that then must be addressed is that privacy "[…] is generally not the primary requirement of a system and it may even come into conflict with other (functional or non-functional) requirements."[151] In larger organisations, the varying views on privacy can become problematic as they might lead to different and sometimes conflicting priorities. A privacy expert might recommend opting for data minimisation while a security expert demands going for data integrity, which in turn might contradict the former as the latter "[…] may require a considerable amount of data that is accurate, consistent and reliable."[152] Without reliable guidance it is hard choosing the right path between various conflicting potential measures which both by themselves work towards achieving compliance with PbD. These issues can to some extent be mitigated by a DPO, as they apart from contributing to striking a balance between various interests also "[…] may link between

[145] Tsormpatzoudi, Berendt, and Coudert. "Privacy by Design: From Research and Policy to Practice", 204.
[146] Tsormpatzoudi, Berendt, and Coudert. "Privacy by Design: From Research and Policy to Practice", 202.
[147] Koops and Leenes, "Privacy regulation cannot be hardcoded", 162.
[148] Koops and Leenes, "Privacy regulation cannot be hardcoded", 162.
[149] Kaye, "'Privacy-by-Design' Is Crucial, but Not Easy or Cheap".
[150] Hildebrandt and Tielemans, "Data protection by design and technology neutral law", 517
[151] Danezis et. al., "Privacy and Data Protection by Design", 11.
[152] Tsormpatzoudi, Berendt, and Coudert. "Privacy by Design: From Research and Policy to Practice", 204.

different functions of an organisation and as such promote the interdisciplinary aspects of the principle Privacy/Data Protection by Design."[153]

An allowing margin of appreciation is not unproblematic as the majority of the interests conflicting with PbD and privacy likely are of great significance for a controller. The greater a conflict is the higher the costs for actually implementing specific privacy requirements into a system. PbD could also be at "[…] odds with powerful business and state interests, and simultaneously remains peripheral to the concerns of most consumers and engineers".[154] Furthermore, large databases are often very attractive for various entities such as corporate and governmental institutions.[155] A wholescale genuine PbD-regime "[…] can easily collide with that logic [of the 'internet economy'], which is based largely on the monetarization of monitoring".[156] There is an inherent conflict between restrictions through limiting collection to *core* data and anonymised processing on the one hand and utility, creation and profit on the other hand. Data can, according to Ohm, be either "[…] useful or perfectly anonymous but never both."[157] The balance between compliance with privacy law and utility must therefore be struck carefully, as pure automated privacy protection is likely to create a system […] that is either unnecessarily restrictive, thereby undermining the utility of the system, or too permissive, thereby leaving ample room for misuse (which might not be caught because oversight is reduced on the erroneous assumption that the system can govern itself)."[158] High standards regarding privacy will obviously impede data collection as well as subsequent use of this data. Not only do PbD measures come with a certain cost for implementation, it also restricts economic usage, e.g. advertising from "[…] targeting practices and peoples' presence on social networking sites."[159] As described by Spiekerman, "[…] PbD proponents hardly embrace these economic facts in their reasoning." [160] Adding to the difficulties, consumers and users rarely prioritise privacy.[161] Data subjects could not seldom be faced with the choice between upholding privacy and enjoying the full functionality of a service.[162] If privacy is not high on the user agenda, controllers lose another proper incentive for embracing PbD.

---

[153] Tsormpatzoudi, Berendt, and Coudert. "Privacy by Design: From Research and Policy to Practice", 205.

[154] Bygrave, "Hardwiring Privacy", 3.

[155] Gürses, Troncoso and Diaz, "Engineering Privacy by Design", *under* 2.2, 6.

[156] Bygrave, "Hardwiring Privacy", 11.

[157] Paul Ohm in Lerner, *The Architecture of Privacy*, x [foreword].

[158] Lerner, *The Architecture of Privacy*, xv-xvi [preface].

[159] Spiekerman, "The challenges of privacy by design", 39.

[160] Spiekerman, "The challenges of privacy by design", 39.

[161] Bygrave, "Hardwiring Privacy", 10.

[162] Schartum, "Making privacy by design operative", 156.

All these matters described subsequently lead to an assumption that any controller would as far as possible like to avoid implementing any privacy measure that is at odds with other important interests. The vaguer the legislation is and the less guidance being available the greater the risk for controllers opting not to implement any PbD measure that intrude upon any other important interest. When awarding controllers such a margin of appreciation the worries of the European Parliament become a very real issue and it is hard to envisage controllers to fully embrace PbD without proper guidance that clearly indicates what really ought to be done in order to comply with PbD. However, to make proper use of the margin of appreciation and minimise risk of non-compliance, controllers must have a solid base for making well balanced choices regarding potential risks of infringing rights of data subjects. A genuinely performed analysis can provide such a solid base which in turn also can be used to demonstrate good intent vis-à-vis supervisory authorities.

3.6 Available guidance for complying with PbD

Given the vague nature of Art. 25.1, the lack of any kind of case law and the lack of previous experience (given the fact that PbD is a new concept in legislation), proper understanding and implementation of PbD depend heavily on various kind of guidance. Guidance in general seems however to be a scarce commodity. In a statement from 2012 the A29WP[163], though embracing the concept as such, warrants a more thorough clarification of what PbD actually means.[164] There is no addressing how A29WP perceive PbD nor how it should be implemented in practical terms.

As one of the main recommendations for successful implementation and compliance with PbD, Danezis et. al. suggests that supervisory authorities, "[…] should play an important role providing independent guidance […]".[165] However, as previously mentioned it is unclear to what extent the supervisory authorities fully grasp the concept of PbD themselves. When searching for information on the Swedish supervisory authority, *Datainspektionen*, available information is very general in character. In the published guidelines, but a smaller section is devoted to PbD, and references are made to principles such as data minimisation and purpose for processing. It is stated that is preferable implementing measures at an early stage. Regarding technical and organisational measures, the guidance merely repeats the requirements in Art. 25.1, stating that what kind of measures that are needed depend upon the nature, scope and purpose of the data and the processing as well as the risks towards individuals that the processing might pose.[166] It continues stating that examples of such

[163] Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data.
[164] A29WP (2012), 11.
[165] Danezis et. al., "Privacy and Data Protection by Design", iv.
[166] "Förberedelser inför EU:s dataskyddsförordning", 9.

measures could be data minimisation or pseudonymisation followed by a brief explanation the two concepts.[167] That is all the guidance there is on PbD. The section covering PbD is less than one page. In fact, it is questionable if this information from the Swedish supervisory authority can even qualify as guidance on PbD as it but repeat the content of Art. 25.1. This lack of proper guidance is likely the case at most national supervisory authorities within EU.

The implemented measures must have the desired effect in order to achieve compliance with the law. For example, if focus have been on implementing several measures concerning data minimisation but it turns out storage is not an issue in the processing operations, what seems to be part of compliance with the law might in fact turn out far from it.[168] Guidance is key for successful implementation of and compliance with PbD. There are many observations on the fact that there is all but an abundance of practical and useful guidance. Schartum notes that transforming PbD into technical and organisational measures becomes rather tricky as "[…] its concrete implementation remains unclear at the present moment.[169] One of the greatest factors for creating the gap between the PbD principles and the operationalisation of these principles is according to Kroener and Wright that there simply is no sufficient detailed guidance.[170] Danezis et. al. states that there is no concrete guidance for software engineers for implementing certain design elements that will fulfil the legal requirements.[171] Tsormpatzoudi, Berendt, and Coudert claims that "[…] companies lack practical guidance on how to achieve the goals defined by the legislation."[172] The fact that there seem to be insufficient available and adequate guidance ought to reduce the general expectations upon realising PbD, and should be taken into consideration when assessing compliance in the future.

[167] "Förberedelser inför EU:s dataskyddsförordning", 9.

[168] Tsormpatzoudi, Berendt, and Coudert. "Privacy by Design: From Research and Policy to Practice", 204-205.

[169] Danezis et. al., "Privacy and Data Protection by Design", *under* 'executive summary', iii.

[170] Kroener and Wright, "A Strategy for Operationalizing Privacy by Design", 362.

[171] Schartum, "Making privacy by design operative", 163.

[172] Tsormpatzoudi, Berendt, and Coudert. "Privacy by Design: From Research and Policy to Practice", 202.

4 Consequences of current conditions and calibrating expectations

In one year from now GDPR is applicable as national law within every member state of the EU. Controllers are then expected to comply with the new concept of PbD. In order to do so they shall implement appropriate technical and organisation measures. What exactly controllers are supposed to do in practical terms is far from clear. The legal requirements are vague and available guidance is rather thin and not very frequent. There are many obstacles on the way towards compliance with Art. 25.1 through implementation of measures that fulfil the requirements of PbD. Controllers lack proper privacy oriented software tools and as Art. 25.1 targets controllers and not producers of software it is uncertain if this will change to the better in the near future. Controllers are obliged to balance various interests in a proportionate way when choosing which technical and organisational measures to implement. How such a process is supposed to take place while the controller is biased towards the employer is also quite unclear. Surely the influence from a DPO can have a certain mitigating effect on the controller's assessment, but in the end the DPO is also employed and even though stated in the GDPR that a DPO shall have certain independence in relation to the employer he is bound to have loyalty towards the source of income nevertheless. There are also major gaps in the understanding of the concept of PbD between various stakeholders, e.g. policy makers and engineers. The general lack of incentives for implementing PbD is a big flaw which for obvious reasons will work against successful implementation of PbD as it likely will not be met by a warm welcome by the addressees of Art. 25.1. While the incentives are not there, effective monitoring and enforcement could have had an impact on the outcome of the implementation of PbD, but seemingly the supervisory authorities do not have sufficient capacity in this regard. All the important conditions surrounding the controller in the implementation process are more or less unfavourable. Subsequently, the expectations on the outcome of the coming wave of PbD-implementations cannot be held particularly high. In my view, the expectations upon the controllers must be calibrated in a similar way, meaning that any assessment of compliance with Art. 25.1 simply must take into consideration all the flawed conditions being present. Compliance should, at least in the near future until conditions improve substantially, be viewed through present conditions and assessing compliance should be made in a proportionate and forgiving way rather than in a strict and bureaucratic way. The principle of proportionality has a solid foundation within EU law and should be adhered by supervisory authorities when assessing any controllers attempt to comply with Art. 25.1, as "[…] the proportionality principle must be observed not just by data controllers but also by [authorities] when exercising their respective decision-making competence."[173] This should be possible as the way in which Art. 25.1 is constructed,

[173] Bygrave, *Data Privacy Law: An International Perspective*, 150.

compliance should be assessed in 'the overall picture', i.e. has the controller implemented respectively disregarded measures in a proportionate way in the specific context and embraced most or all appropriate measures? Reiterating recital 150, supervisory authorities shall take into account "[…] all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement." In my view art. 25.1 give controllers leeway to disregard some measures that would mean disproportionate costs for implementation, that would cause great harm to the business interests, or that contextually have lesser significance than other measures et cetera while posing minimal risks for the rights of the data subjects. Given that surrounding conditions are far from optimal, the bar for 'acceptable level' in compliance assessments should therefore be lowered until the conditions improve. This does however not mean that the controller should relax too much.

Any controller that seek a reasonable good chance for having a PbD regime that will be deemed compliant with Art. 25.1 should obviously set out to do the best he can including seeking advice where such is available, e.g. from contact with supervisory authorities. Any choice to not implement a certain measure should be made in the light of proportionality where such measure will have a disproportionate negative consequence for the organisation, e.g. through very high costs for implementation. In order to do proper balanced choices and being able to argue successfully for opting not to implement certain measures, controllers should always undertake necessary analyses of risks and other relevant factors, especially since context in each individual case is an important factor. Having a DPO can improve chances for proper balanced choices as well as provide an indication of good intent in relation to undertaken implementations. The controller should make sure a privacy friendly culture is established and nourished within the organisation and that the means for processing personal data is privacy-calibrated. Thus, a controller does wise in, where indicated necessary, adhering as much as possible to pseudonymisation or anonymization, data minimisation, default settings and automatic enforcement, and transparency. The controller must also be continuously make sure that the organisation stays on track with regard to privacy and that PbD shall be adhered not only when processing of personal data is executed but before and after processing as well. Any new means for processing shall be in tune with PbD. If a controller makes sure all this is done and always have a good intent in every step of the way, it is hard envisaging supervisory authorities finding a case of non-compliance with Art. 25.1.

5 Conclusion

The legal requirements concerning PbD can be said to be vague at the very least. What a controller must do is quite unclear and there is insufficient guidance to mitigate the shortcomings of the law. Controllers shall make sure the means for processing is in tune with Art. 25.1 but the decisive influence over these means are in the hands of others, i.e. producers of hardware and software. This presents controllers with a rather tricky situation as Art. 25.1 addresses controllers. In fact, producers are likely not even bound be the requirements in Art. 25.1. On top of this, controllers must undertake a relatively unbiased proportionality assessment resulting in choices of which measures shall be implemented and which shall be left out. This is indeed a hard task given the present conditions and it would be unreasonable if these conditions would not be taken under consideration by supervisory authorities when assessing cases of compliance with Art. 25.1 in the future.

Looking beyond the less favourable conditions for implementation, some things are however clear enough as to serve as a basis for establishing potential obligations for the controller. What must be done depend quite a lot on the context in every single processing operation and the controller must therefore analyse the context in relation to risks, legal requirements and other important factors. One way of undertaking a proper analysis is through a PIA. Though PIA is not mandatory for compliance with PbD, it is a useful tool identifying the needs, the risks and the appropriate measures to implement. As such, PIA is a good way to manifest compliance or good intent actively seeking compliance. Another useful thing is to appoint a DPO who can serve to bridge the gaps between variations on the understanding of PbD within an organisation and what measures ought to be taken to achieve compliance. A DPO can also assist the controller in the process of balancing between colliding interests when choosing which measures to implement in the PbD regime. Further, the controller should support and encourage spreading awareness, information and unified interpretations of privacy and PbD throughout the organisation. Internal polices corresponding to the legal requirements and enabling a system for accountability and supervision are also important components for a functioning PbD-regime. This will improve the odds for successful compliance and reduce potential for mistakes and non-compliant measures. While every employee naturally will not become privacy experts, they will think twice more often and the level of communication between various categories of employees will increase. Especially important is collaboration between legal experts and engineers.

Turning to findings more concrete in nature it seems, regardless of contextual dependence, that some measures are likely appropriate in general. If failing to implement or at least consider implementing certain measures, non-compliance with risk for remedies could be a potential outcome. As the controller is allowed to consider the cost for implementation in the proportionality assessment, measures that have high effect and/or low costs for

implementation should definitely be considered. It is hard successfully arguiung against a claim for non-compliance in relation to disregarding a certain measure if the costs for implementing that measure had insignificant impact on the overall proportionality assessment. The same goes for legal requirements that are especially suitable for implementation through technical measures, as they most likely correspond to simple and very specific rules. Another category of technical measures that any controller should think hard and long before dismissing is the explicitly mentioned examples in Art. 25.1 and recital 78, i.e. 'data minimisation', 'pseudonymisation', 'default settings', and 'transparency'. Data minimisation is one of the safest way ensure that processing in general is not in breach of any privacy requirements. The novelty of pseudonymisation is one of the few examples of incentives for controllers to embrace PbD. Pseudonymisation can strike a balance between privacy and the value of data in contrast to anonymization following the claim that 'data can either be anonymous or perfectly useful'. Privacy as default settings is also a major concept advocated by GDPR. Default settings for privacy clarifies where active consent has been given and clearly upholds the principle of data minimisation. Transparency helps safeguarding the rights of the data subjects but also presents an opportunity for controllers to manifest a good intent not only in relation to data subjects but to authorities and policy makers as well. To what extent a controller should utilise these measures is of course not clear, but given that they are explicitly mentioned as examples of appropriate measures in GDPR and therefore must be significant, controller should definitely embrace them.

When assessing every measure of the PbD-regime, the controller shall also strive towards maximising automatic enforcement of the technical measures set to uphold privacy, with a focus on *ex ante* where possible. Upholding privacy by automation has been identified as one of the most important privacy-supporting elements. Compliance is however not only actively implementing certain measures but restraining from certain actions as well. Controllers must certainly avoid any kind of technology that collect more data than what is deemed necessary for the specific processing operation or required by functionality. The controller must not use technology that distorts data confidentiality either.

In light of the current non-optimal conditions that create obstacles instead of facilitating for controllers to strive towards complying with PbD and Art. 25.1, any expectations on what controller ought to be able to perform should be calibrated accordingly. It would be unfair expecting perfect compliance performances while vital conditions such as guidance is unsatisfactory at best. Supervisory authorities should take into account that the conditions for complying with Art. 25.1 is rather unfavourable, and subsequently assess compliance in a proportionate way. The bar of what constitute sufficient effort in order to comply with Art. 25.1 must be lower than if the conditions for complying were more favourable. Present conditions for compliance can therefore in a way serve as guidance for controllers regarding

the level of ambition in the strive for complying with Art. 25.1. Accordingly, any controller that in good faith sets out introducing a privacy friendly culture within the organisation combined with implementing explicitly mentioned measures, that undertakes necessary analyses and in a proportionate way embraces especially important measures that have high effect in relation to costs, that strives for automatic enforcement in an *ex ante* focus, and restrain from utilising privacy intrusive measures should, based on the rationale of reasonable expectations, be relatively safe from risks of non-compliance with Art. 25.1 and subsequent remedies.

Table of reference

Statutes

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (O J L 119/1, 4.5.2016). (GDPR)

Publications from authorities (chronological order)

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on Promoting Data Protection by Privacy Enhancing Technologies (PETs). Brussels, 2.5.2007 COM(2007) 228 final.

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. A comprehensive approach on personal data protection in the European Union. Brussels, 4.11.2010 COM(2010) 609 final.

ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 01/2012 on the data protection reform proposals. Adopted on 23 March 2012 00530/12/EN WP 191

European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading). Wednesday, 12 March 2014 – Strasbourg – Final edition. Procedure : **2012/0011(COD)** http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT%20TA%20P7-TA-2014-0212%200%20DOC%20XML%20V0//EN (accessed April 16, 2017)

European Commission press release 21 December 2015. MEMO/15/6385. http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm (accessed February 12, 2017)

Literature (alphabetical order)

Bygrave, Lee, *Data Privacy Law: An International Perspective*. Oxford: Oxford Scholarship Online, 2014. doi: 10.1093/acprof:oso/9780199675555.001.0001

Guagnin et al., *Managing Privacy Through Accountability*. Basingstoke, UK: Palgrave Macmillan Guagnin, 2012.[174]

Lerner, Elissa, ed. *The Architecture of Privacy: On engineering technologies that can deliver trustworthy safeguards*. Sebastopol: O'Reilly Media, Inc., 2015.[175]

Articles in electronic journals (alphabetical order)

Bygrave, Lee. "Hardwiring Privacy". *University of Oslo Faculty of Law* Research Paper No. 2017-02. Available at SSRN: https://ssrn.com/abstract=2901405 (accessed March 30, 2017).

Cavoukian, Ann. "Privacy by design: the definitive workshop. A foreword by Ann Cavoukian." *Springerlink.com* IDIS (2010) 3:247-251. doi: 10.1007/s12394-010-0062-y

Cavoukian, Ann, Scott Taylor and Martin Abrams. "Privacy by Design: essential for organizational accountability and strong business practices" *Springerlink.com* IDIS (2010) 3:405-413. doi: 10.1007/s12394-010-0053-z

Danezis, George, Josep Domingo-Ferrer, Marit Hansen, Jaap- Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, and Stefan Schiffner. "Privacy and Data Protection by Design – from policy to engineering." *European Union Agency for Network and Information Security* (2014). doi: 10.2824/38623. https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (accessed March 5, 2017).

---

[174] https://books.google.se/books?id=UbqmwIbAH44C&printsec=frontcover&dq=Managing+privacy+through+accountability&hl=sv&sa=X&ved=0ahUKEwiKrK3z18HQAhUBWhoKHZluDcoQ6AEIHTAA#v=onepage&q=Managing%20privacy%20through%20accountability&f=false (accessed November 24, 2016).

[175] https://books.google.se/books?id=rtl0CgAAQBAJ&pg=PP2&lpg=PP2&dq=The+Architecture+of+Privacy&source=bl&ots=8vYPE2aWHk&sig=RtEU0Y9RPw5QBBp2Y-dAcRdx65Q&hl=sv&sa=X&ved=0ahUKEwjg34eb1sHQAhVG7hoKHYUpBbk4ChDoAQgrMAI#v=onepage&q=The%20Architecture%20of%20Privacy&f=false (accessed November 24, 2016).

Hildebrandt, Mireille and Laura Tielemans. ”Data protection by design and technology neutral law” *Computer law & Security Review: The International Journal of Technology Law and Practice* Vol. 29 (2013): 509-521. doi: 10.1016/j.clsr.2013.07.004

Koops, Bert-Jaap, Jaap-Henk Hoepman and Ronald Leenes. “Open-source intelligence and privacy by design” *Computer law & Security Review: The International Journal of Technology Law and Practice* Vol. 29 (2013): 676-688. doi: 10.1016/j.clsr.2013.09.005

Koops, Bert-Jaap and Ronald Leenes. “Privacy regulation cannot be hardcoded. A critical comment on the ‘privacy by design’ provision in data-protection law.” *International Review of Law, Computers & Technology* Vol. 28, No. 2 (2014): 159-171. doi: 10.1080/13600869.2013.801589

Kroener, Inga and David Wright. ”A Strategy for Operationalizing Privacy by Design.” *The Information Society* 30:5 (2014): 355-365. doi: 10.1080/01972243.2014.944730.

van Lieshout, Marc, Linda Kool, Bas van Schoonhoven and Marjan de Jonge.),"Privacy by Design: an alternative to existing practice in safeguarding privacy." *Emerald Insight,* info, Vol. 13, Iss 6 (2011): 55-68. doi: 10.1108/14636691111174261

Rubinstein, Ira and Nathaniel Good. “Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents.” Berkeley Technology Law Journal Vol. 28, Issue 2 Fall (2013): 1333-1413. doi: 10.15779/Z38G11N

Schaar, Peter. “Privacy by Design.” *Identity in the Information Society* Vol.3(2) (2010): 267-274. doi: 10.1007/s12394-010-0055-x

Schartum, Dag. “Making privacy by design operative.” *International Journal of Law and Information Technology*. Vol.24 (2016): 151-175. doi: 10.1093/ijlit/eaw002

Spiekerman, Sarah. “The Challenges of Privacy by Design.” *Communications of the ACM*. Vol. 55(7) (2012): 38-40. doi: 10.1145/2209249.2209263

Tsormpatzoudi, Pagona, Bettina Berendt, and Fanny Coudert. ”Privacy by Design: From Research and Policy to Practice – the Challenge of Multi-disciplinarity” in Privacy Technologies and Policy. Third Annual Privacy Forum, APF 2015, Luxembourg, Luxembourg. October 7-8. *Springer International Publishing.* Series Volume 9484 (2015):

199-212. doi: 10.1007/978-3-319-31456-3

Wright, David. "The state of the art in privacy impact assessment." *Computer Law & Security Review.* Vol. 28(1) (2011): 54–61. doi: 10.1016/j.clsr.2011.11.007

Others/Internet (alphabetical order)

Förberedelser inför EU:s dataskyddsförordning. Vägledning till personuppgiftsansvariga. *Datainspektionen.*[176] http://www.datainspektionen.se/Documents/vagledning-forberedelser-pua.pdf (accessed March 13, 2017).

Gürses, Seda, Carmela Troncoso and Claudia Diaz. Engineering Privacy by Design. (2011) https://www.esat.kuleuven.be/cosic/publications/article-1542.pdf (accessed February 12, 2017).

Hustinx, Peter 2009. Privacy by design: The Definitive Workshop. Madrid, Spain. https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-11-02_Madrid_privacybydesign_EN.pdf (accessed November 24, 2016).

Kaye, Kate. 'Privacy-by-Design' Is Crucial, but Not Easy or Cheap. Advertising Age. Published October 06, 2014. http://adage.com/article/datadriven-marketing/privacy-design-crucial-easy-cheap/295145/ (accessed April 20, 2017)

Maldoff, Gabriel. Top 10 operational impacts of the GDPR: Part 8 – Pseudonymization. (2016) https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/ (accessed April 20, 2017)

[176] *Translated:* Preparations for the EU General Data Protection Regulation. Guidance for controllers. Published by the Swedish supervisory authority.