WHITE PAPER

Privacy by Design:

The Key to Unlock Your Compliance Strategy

SOPHIE STALLA-BOURDILLON
Senior Privacy Counsel
& Legal Engineer, Immuta

2019

IMMUTA

Global interest in privacy has led to a recent explosion in privacy-centric legislation.

Consequently, organizations of all sizes find themselves in the difficult position of having to implement and maintain compliance with a host of complex regulations rife with regional peculiarities.

Privacy by Design (PbD), and its EU version Data Protection by Design (DPbD), aim to implement privacy controls from the outset. As such, PbD can be an effective starting-point for a de-facto "common denominator" approach to compliance compatible with a large number of privacy frameworks. And yet, despite its potential, PbD receives scant attention. One reason for this may be the focus upon system design and technical information, which are often difficult to digest for compliance personnel.

But there is more to PbD than design patterns or strategies. Creating PbD workflows is critical to make compliance possible and scalable. Without PbD workflows, organizations are unable to combine the expertise needed to make informed decisions at the right moment, and to select and implement a comprehensive list of effective controls.

This short whitepaper aims to provide the beginnings of a framework for operationalizing PbD. The ultimate goal of this paper is to raise awareness about the potential of PbD and show how technical and compliance roles can closely collaborate, thereby contributing to the safe and responsible use of data analytics within organizations.

Note: The information contained in this presentation is not intended to be and should not be construed to be legal advice.Organizations should not rely on the information herein, and they should obtain legal advice from their own legal counsel or other professional legal services provider.

What is Privacy by Design?

Privacy by Design was conceptualized in the 1990s[1] to extend the requirements of the eight Fair Information Practices (FIPs), as developed by the organization for Economic Co-operation and Development.[2] In a nutshell, PbD is the idea that fair information practices should be embedded as early as possible into the design of information technology (IT) systems.

Embedding FIPs into IT systems or data analytics models first requires deriving generalizable and actionable requirements which can then be addressed by a variety of organizational and technical measures, which we refer to as "controls." Notably, each FIP can be translated into one or more PbD requirements, as demonstrated in Table 1 below.[3]

Deriving PbD requirements from FIPs

FAIR INFORMATION PRACTICES	PbD REQUIREMENTS
1. **Collection Limitation Principle.** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.	**Transparency, Lawfulness and Fairness**
2. **Data Quality Principle.** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.	**Data minimization** **Data accuracy**
3. **Purpose Specification Principle.** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.	**Purpose specification** **Purpose limitation**
4. **Use Limitation Principle.** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: a) with the consent of the data subject; or b) by the authority of law.	**Purpose limitation**
5. **Security Safeguards Principle.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.	**Security**

[1] See Ann Cavoukian, "The Seven Foundational Principles," Ryerson University, available at "https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/. See also "CFP2000," Conference on Computers, Freedom and Privacy, 2000, more information about which is available at http://www.cfp2000.org/. Note that the EU's Data Protection Directive of 1995 had already called in its Recital 46 for the taking of organizational and technical measures at the time "of the design of the processing system."

[2] "OECD Privacy Principles," available at http://oecdprivacy.org/.

[3] Note that the text of each principle is taken directly from the principles as set forth by the OECD, cited above.

FAIR INFORMATION PRACTICES	PbD REQUIREMENTS
6. Openness Principle. There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.	Transparency
7. Individual Participation Principle. An individual should have the right: a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b. to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c. to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and d. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.	Intervenability
8. Accountability Principle. A data controller should be accountable for complying with measures which give effect to the principles stated above.	Accountability

Table 1. Deriving PbD requirements from FIPs

Mapping tasks to PbD requirements

PbD requirements can then be rearranged into an **organizational workflow** to make the allocation of tasks possible between different roles and expertise, as demonstrated in Table 2.

PbD REQUIREMENTS	TASKS
Purpose specification	Express your purpose
Data minimization	Tailor the amount of data and duration of processing to purpose
Accuracy	Ensure accuracy of data
Lawfulness and fairness	Make sure processing means are lawful and fair
Purpose limitation	Preserve purpose over time
Security	Keep data and processing activities secure
Transparency	Keep processing activities transparent
Intervenability	Enable individuals to exercise their rights
Accountability	Take measures to demonstrate compliance with all prior principles

Table 2. Mapping tasks to PbD requirements in order to derive organizational workflow

Mapping controls to PbD requirements

It is important to remember that these PbD requirements should be conceived as goals. As a result, there is no single best way to meet these goals and thereby to perform these tasks. Ultimately, the right controls must be selected and implemented for each PdD requirement, as demonstrated in Table 3 below.

PbD REQUIREMENTS	TASKS	CONTROLS
Purpose specification	Express purpose	ex: 1) ask business owner to express purpose, 2) ask compliance to check legitimacy of purpose.
Data minimization	Tailor amount of data, number of data movements, and duration of processing to purpose	ex: 1) ask data user to identify relevant data for specified purpose, 2) execute data policies (e.g., masking, differential privacy, etc.) upon data to make sure data user only gets access to what they need.
Accuracy	Ensure accuracy of data	ex: 1) set up a process to check accuracy of data, 2) ensure data cannot be altered when consumed through read-only access.
Lawfulness and fairness	Make sure processing means are lawful and fair	ex: set up a process for assessing individuals' expectations for each use case.
Purpose limitation	Preserve purpose over time	ex: implement purpose-based access control.
Security	Keep data and processing activities secure	ex: 1) encrypt in transit and at rest, 2) implement read-only access to underlying data when possible, 3) regularly mask potential identifiers, 4) enforce strict access controls.
Transparency	Keep processing activities transparent	ex: 1) create transparent pipeline, 2) produce meaningful information for users.
Intervenability	Enable individuals to exercise their rights	ex: create an interface to interact with users and enable them to submit such requests directly.
Accountability	Take measures to be in a position to demonstrate compliance with all prior principles	ex: 1) enable fine-grained auditing and notification, 2) produce regular and relevant reports on data activities.

Table 3. Mapping controls to PbD requirements

Controls should be implemented right from the design stage and involve the mixing of different types of expertise.

Generally speaking, controls can be of four types: directive (specifying tasks), preventive (constraining behavior before its inception), detective (monitoring to identify issues), and corrective (mitigating when issues are identified). These four types of controls can be combined into two high-level categories: process (determining which role should intervene, when and how) and system controls (such as self-executing or automated decisions). Making sure these two types of controls are combined together is a better approach than relying upon one of them in isolation.

Producing what's known as a "RACI"[4] matrix before the start of a processing activity is also useful to allocate roles and responsibilities per task and thereby per PbD requirement.[5] Table 4 is only one example of a possible high-level RACI matrix for a data science project.

PbD requirements	**Business owner**	**Data user**	**Complaince personnel**	**Data source administrator**	**IT**
Express purpose	A, R	C	C	I	
Tailor amount of data, number of data movements and duration of processing to purpose	A	R	C	I	R
Ensure accuracy of data	A	C		R	R
Make sure processing is lawful and fair	A	R	C	R	
Preserve purpose over time	A	R			R
Keep data and processing activities secure	A	R			R
Keep processing activities transparent	A	R	R		R
Enable individuals to exercise their rights	A		R		R
Take measures to be in a position to demonstrate compliance with all prior principles	A	R	R		R

Table 4. Example of a high-level RACI for a data science project

[4] See Mark Fulford, "How a RACI Matrix Can Enhance Your Risk Management Program," April 17, 2018, available at https://ballastsecure.com/resource/how-a-raci-matrix-can-enhance-your-risk-management-program.

[5] Responsibilities should be conceived as a spectrum and a distinction should be drawn between: being responsible (R) (i.e., having the role to perform the task), being accountable (A) (i.e., owning the risk of the task and therefore having to supervise the performance of the task), being consulted (C) (i.e., having the role to provide feedback while the task is being performed) and being informed (i.e., being notified once the task is performed).

The potential of PbD

Combined, PbD requirements should form a baseline response that covers most privacy regulations. Why? PbD reflects data governance best practice globally, and its requirements therefore apply more broadly than any other approach. Let's examine how PbD maps to specific privacy regulations.

DPbD requirements for GDPR

We can start with the **EU General Data Protection Regulation** (GDPR),[6] which is directly applicable in the EU since May 2018. GDPR imposes an obligation to perform data protection by design (DPbD) for organizations processing personal data. DPbD is a variant of PbD, and is spelled out in Article 25 of the GDPR.

DPbD requirements, in fact, mirror PbD requirements.

Under Article 25, for example, DPbD means

> "... implement[ing] appropriate technical and organisational measures, such as pseudonymisation, which are designed to (1) implement data protection principles, such as data minimisation, in an effective manner and to (2) integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

Article 25 refers to the list of data protection principles included in Article 5. DPbD requirements, as set forth in GDPR, are summed up in Table 5.

[6] Regulation 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, available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679.

DPbD requirements

DPbD REQUIREMENTS
Lawfulness, fairness and transparency (Articles 5, 6, 7, 12)
Purpose limitation (Articles 5, 6)
Data minimization (Article 5)
Accuracy (Article 5)
Storage limitation (Article 5)
Security (Articles 5, 32–34)
Accountability (Articles 5, 26, 28, 30, 35, 37–39)
Intervenability (Articles 12–22)

Table 5. DPbD requirements

According to PbD requirements, tasks as well as controls are all relevant for pursuing compliance with GDPR Article 25. What is more, because of its reference to Article 5 and Articles 12–22, Article 25 acts as the backbone of GDPR itself. Compliance with Article 25 is the safest route to reach full GDPR compliance, making PbD central to any serious attempt to meet the GDPR's requirements.

GDPL PbD requirements

What is true for the GDPR is also true for the Brazilian General Data Protection Law (GDPL), which is directly inspired by the GDPR.[7] The similarities between the two legal regimes are much greater than their differences – despite, for example, the fact that the list of legal bases in the GDPL is slightly different than the GDPR's, or that the principle of fairness is expressed in terms of a differeent principle of non-discrimination.

Indeed, the eighth principle of prevention listed in Article 6 of the GDPL provides for the adoption of "measures to prevent the occurrence of harm due to the processing of personal data." Implementing PbD controls as early as possible is perfectly aligned with this principle.

While the GDPL will not be enforced until February 2020, global efforts to ensure compliance with the law are already well under way.

[7] Text of the GDPL is available at http://dataprivacy.com.br/protecao_de_dados_pessoais.docx.

CCPA PbD requirements

PbD requirements are also fully compatible with other privacy regulations, such as the California Consumer Privacy Act of 2018 (CCPA), which does not as closely follow the GDPR as Brazil's GDPL.[8] While it is true that CCPA is less comprehensive than GDPR, and does not include an express by–design obligation or a principle of prevention of harm, pursuing a PbD strategy easily facilitates compliance with CCPA.

To begin with, many PbD requirements are explicitly addressed by CCPA. This holds true, for example, for the requirements for purpose specification, purpose limitation, security, transparency, intervenability, and accountability.

Purpose specification and limitation requirements can, for example, be derived from the obligation under the CCPA to inform consumers of "the purposes for which the categories of personal information shall be used"[9] and from the prohibition to "collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice."[10]

While data minimization and accuracy cannot be related to express provisions within CCPA, they still make sense as the most effective way to reduce the number of consumer requests.. Reducing the volume of data an organization retains, while also ensuring that data's accuracy, will in practice translate to a lower number of access, opt–out, and deletion requests. Table 6 sums up the CCPA PbD requirements.

CCPA PbD REQUIREMENTS
Purpose specification (sections 1798.100; 1798.110; 1798.115)
Data minimization (implicit)
Accuracy (implicit)
Lawfulness and fairness (section 1798.120)
Purpose limitation (sections 1798.100; 1798.140(w))
Security (sections 1798.150)
Transparency (sections 1798.100; 1798.130; 1798.135)
Intervenability (sections 1798.100; 1798.105; 1798.110; 1798.120; 1798.125; 1798.130)
Accountability (sections 1798.135; 1798.100)

Table 6. CCPA PbD requirements

[8] Text of the CCPA is available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[9] Section 1798.100.

[10] Section 1798.100.

HIPAA PbD requirements

Notably, PbD requirements are consistent with older privacy regulations as well. Take the US[11] Health Insurance Portability and Accountability Act of 1996,[12] also known as HIPAA, which protects individually identifiable health information (i.e., protected health information).[13] The HIPAA Privacy Rule governs situations in which individuals protected health information may be used or disclosed by covered entities. Permitted purposes are exhaustively listed within the Privacy Rule. Further, the amount of data processed must be tailored to each purpose in order to guarantee that only the minimum amount of protected health information is used or disclosed. Table 7 sums up HIPAA PbD requirements.

HIPAA PbD REQUIREMENTS
Purpose specification (sections 164.502(a), (c); 164.506; 164.508; 164.510(b)(1); 164.512; 164.514)
Data minimization (sections 164.502 (b); 164.514(d))
Accuracy (section 164.526)
Lawfulness and fairness (sections 164.506(b); 164.510)
Purpose limitation (sections 164.502(a), (c); 164.506; 164.508; 164.510(b)(1), 164.512; 164.514)
Security (sections 164.306; 1164.308;1164.310; 164.312; 1164.404-410; 164.502(h); 164.522(b); 164.514(a)(2))
Transparency (sections 164.512(c)(2); 164.520)
Intervenability (sections 164.510; 164.522; 164.524; 164.526; 164.528)
Accountability (sections 164.314; 164.504; 164.508(a)(6); 164.514(b)(1)(ii); 164.514(d); 164.520 (e); 164.530)

Table 7. HIPAA PbD requirements

[11] Text of the regulation is available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf?language=es.

[12] Text of the regulation is available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf?language=es.

[13] See 45 C.F.R. § 160.103.

Scaling privacy law compliance with PbD

Any serious effort to comply with multiple privacy laws – both existing and future – should start with designing a PbD strategy and selecting controls to embed PbD requirements into processes, products, and services as early as possible. PbD requirements, when viewed correctly, form a common denominator for converging privacy regulations at the global level.

Once PbD requirements are met, differences between different regulatory regimes become easier to handle – such as, for example, the differing grounds of justifying the processing of personal data (i.e., legal bases), or in the conditions for exercising data subject or consumer rights.

Perhaps most importantly, when pursuing a PbD strategy, privacy law compliance can become a competitive differentiator when engaging with potential customers, and a sign of high-level of organizational maturity. Ultimately, good governance will translate to better performance in the market, for all these reasons and more – as studies have shown.[14]

This whitepaper aimed to outline a framework to operationalize PbD, and we welcome suggestions or comments to improve this framework. Please reach out to **governance@ immuta.com** with feedback.

[14] See, for example, Stijn Claessens, "Corporate Governance and Development," The World Bank Research Observer, Vol. 21, No. 1 (Spring, 2006), pp. 91-122 avilable at https://www.jstor.org/stable/40282344?seq=1#page_scan_tab_contents.

IMMUTA

7878 Diamondback Dr, Suite C, College Park, MD 20740 | immuta.com | (800) 655-0982