Excerpt of «Designing for Privacy and its Legal Framework»

Aurelia Tamò-Larrieux *

Technical and economic advances have led to the digitalization of our environment. Whether collected from smartphones, smart household devices, or wearable health trackers, data is automatically processed and used to provide us with multiple services throughout the day. While the benefits of such technologies for individual users — as well as society at large — are undisputed, the resulting transformed environment triggers concerns vis-à-vis informational privacy and the loss thereof. These privacy and data protection challenges must be addressed. As privacy protects different and evolving interests, research in this field is a complex undertaking. To do justice to the complex and interdisciplinary nature of privacy and data protection, the topic at hand has to be approached from multiple perspectives. The book «Designing for Privacy and Its Legal Framework» focuses on how the law and technical tools, acting together, can enhance the protection of privacy and data in an Internet of Things environment. In doing so, we provide concrete insights into how to implement the concept of privacy by design.

Citation: Aurelia Tamò-Larrieux, Excerpt of «Designing for Privacy and its Legal Framework», in: *sui-generis* 2019, S. 12

URL: sui-generis.ch/89

DOI: https://doi.org/10.21257/sg.89

* Dr. Aurelia Tamò-Larrieux (aurelia.tamo-larrieux@uzh.ch), Postdoctoral Researcher at the Information Technology, Society, and Law Center (ITSL), University of Zurich.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

1 The following sections provide insight into some core research contained in the book Designing for Privacy and Its Legal Framework, published within the Law and Governance Series of Springer (DOI: 10.1007/978-3-319-98624-1).

I. The Evolution towards Privacy by Design

2 To understand the concept of privacy by design, one should first take a step back and describe the normative and technical tools used to design for privacy. On one hand, privacy and data protection legislation, industry standards on data security, and guiding ethical norms on how to process data build the «normative rationality» of how legal scholars approach the topic of privacy and data protection. We call such approaches legal tools to design for privacy. While these legal tools can vary depending on who issues them (e.g., policymakers, industry agreements, etc.) and how they are enforced, they all build upon a moral imperative. Figuratively speaking, these tools stipulate rules such as «you are not allowed to enter my house». On the other hand, engineers and developers approach the topic of designing for privacy by employing technical tools aimed at protecting the security of communications, the autonomy of transactions, the anonymity of connections, and enhancing the transparency of data processing operations. This more hands-on approach to privacy and data protection is akin to «locking the door of the house».[1]

3 While numerous technical tools that incorporate technical mechanisms (typically referred to as privacy-enhancing technologies) exist, their focus often remains on single goals, addressing specific data protection needs (e.g., the anonymity of email communication). Thus, the argument for a more holistic approach to privacy and data protection emerged and took shape in the concept of privacy by design. Ann Cavoukian pioneered the vision of designing for privacy in 1990 when she argued for a systematic approach to creating technology that embeds privacy into its underlying architecture.[2] Her vision was designed to overcome the juxtaposition of the legal and technical rationality: Legal principles being reactive to past harms (law as a passive observer), while technical tools are proactive measures, enacted to prevent infringements (technology as an active preventer). Privacy by design is an attempt to embrace a holistic approach to privacy protection, from both a preventative and sanctioning standpoint. In this sense, privacy by design is neither strictly a legal nor a technical tool. It combines a principle-based rationality with the aim of finding technical mechanisms and organizational procedures to protect informational privacy preemptively. As privacy by design – or data protection by design and default as Article 25 of the General Data Protection Regulation (GDPR)[3] calls it – has now been encoded into the European data protection framework, it has gained even more significance, with data controllers subject to the GDPR being compelled to implement this new principle.

4 Implementing privacy by design in practice, though, is not a straightforward process and requires legal (i.e., what the normative

---

1 Tamò-Larrieux, Designing for Privacy and its Legal Framework – Data Protection by Design and Default for the Internet of Things, Springer 2018, p. 21.

2 See Cavoukian, Privacy by Design in Law, Policy, and Practice. A White Paper for Regulators, Decision-makers and Policy-makers, 2011, pp. 3 et seqq.

3 The General Data Protection Regulation (GDPR) of the European Parliament and council, Regulation (EU) 2016/679.

principle calls for) and technical (i.e., how to design systems in a way that are compliant with the law) knowhow. Realizing that there is often a gap between the theoretical conception of data protection by design and its practical implementation, «Designing for Privacy and its Legal Framework» unveils the scope of legal principles and technical tools used for privacy and data protection in order to address the question of how to implement Article 25 of the GDPR. We present an analysis of how current regulations in the European Union delegate the implementation of technical privacy and data protection measures to data controllers and show how policymaking must evolve to implement privacy by design in its fullest ideal.

II. The Codification of Data Protection by Design and Default within the GDPR

5 Before the implementation of the GDPR, the Directive 95/46/EC[4] obliged data controllers to «implement appropriate technical and organizational measures to protect personal data» (Article 17). Today, Article 25 of the GDPR goes beyond this statement and introduces a three-paragraph-long article on the subject. Unlike the Directive 95/46/EC, this new article specifies the principle of technical data protection and defines it with respect to time, its scope, and the subject matter.[5] Firstly, Article 25 mandates that technical tools for the protection of personal data are applied beyond the initial design phase, throughout the life cycle of data. Secondly, the scope of data protection by design is broadened to focus not only on data security but also on all prerequisites established in the GDPR. Thirdly, rather than leaving the implementation of privacy by design to the discretion of data controllers, the GDPR stipulates that data subjects have a right to request such technical data protection measures. Finally, the concept of data protection by default is stressed within Article 25, illustrating the evolution towards a more preventive and proactive regime of data protection. A similar evolution is seen within Article 10 of the modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data[6] (Convention 108+), which now includes an obligation to enact privacy by design norms and stipulates the need to foster privacy-friendly configurations by default.

6 In and of itself, Article 25 of the GDPR is a «hollow» norm,[7] as its notion of privacy by design relies on the other legal principles that specify the data processing requirements. The article literally refers to meeting the «requirements of this Regulation» through technical and organizational measures. Thus, to translate Article 25 into practice, we need to take three steps:

(1) Understand what the requirements of the GDPR are. This task requires that we deconstruct the legal principles of the GDPR in order to understand the essence of its protection aim.

(2) Analyze and classify technical and organizational measures that can realis-

4 Directive 95/46/EC of the European Parliament and Council of 24th October 1995.

5 Brinhack/Toch/Hadar, Privacy Mindset, Technological Mindset. Jurimetris: Journal of Law, Science & Technology, 55, 2014, 55–114, pp. 55 et seqq.

6 Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018.

7 Tamò-Larrieux, (Fn. 1), p. 209.

tically be implemented by data controllers to encode the goals of legal principles.

(3) Analyze how the law provides guidelines on how the technical tools identified in step (2) should be applied to be compliant with Article 25 of the GDPR. This task requires referring back to the text of Article 25 of the GDPR to understand how potentially conflicting interests should be balanced in the eyes of the law.

7 Given this basis and because privacy by design is inherently dependent upon context, we then look at a concrete scenario and discuss how in a specific case privacy by design can be implemented.

1. Meeting the Legal Requirements of the GDPR

8 Article 25 of the GDPR states that data controllers must «implement appropriate technical and organizational measures (...) in order to meet the requirements of this Regulation and protect the rights of data subjects». Thereby, the data protection by design clause refers to all principles within the GDPR and requires technical or organizational approaches to encode them.

9 In light of this provision, we classify the aforementioned legal principles into four main groups, those concerning the legality of data processing, the design of data processing systems, the rights of data subjects, and the compliance and enforcement of the GDPR. While other classifications of legal principles are possible, we chose this one as we found it to be the most accessible to non-legal scholars such as engineers and developers.[8]

10 Principles concerning the legality of processing include that of lawful, fair, and transparent processing and informed consent or other means for lawful processing (in particular legitimate interests for processing personal data). Such principles are core components of the GDPR as they build the foundation for legitimizing data processing.[9] However, these principles do not stand alone; instead they are merely the first hurdle data controllers must overcome in order to process personal data of EU citizens.

11 One could argue that adhering to the principles concerning the design of the data processing system presents an even greater challenge for data controllers. These principles contain specific design requirements such as the mandate that data controllers build data processing systems that minimize the collection of data; to only process said data to the minimum extent necessary to achieve the goal for which it was gathered; to build secure data processing systems with explicit use, disclosure, and storage limitations; and to apply anonymization or pseudonymization techniques. These requirements define the boundaries within which developers and engineers are free to innovate and create new data processing services and products.[10]

8 Tamò-Larrieux, (Fn. 1), pp. 87 et seqq.
9 Bygrave, Data Protection Law–Approaching Its Rationale, Logic and Limits, Kluwer International 2002, p. 58 et seq.
10 Tamò-Larrieux, (Fn. 1), pp. 91 et seqq.

12 Aside from the aforementioned principles, which focus more on the duties of data controllers, these concerning the rights of individuals provide data subjects with specific information, access, objection, and erasure rights. It remains the duty of data controllers to ensure that data subjects can make use of those rights. However, these rights are – in contrast to the ones mentioned above – «pull rights», meaning that data subjects have to actively request access to their personal data or object to data processing and demand erasure of said data.[11]

13 Finally, the principles concerning compliance and enforcement ensure that all the principles of the GDPR are implemented. The GDPR not only sanctions the lack of conformity with the core principles of the GDPR but also enables government authorities to supervise and monitor the activities of data controllers. Additionally, increased accountability and liability for outsourced data processing encourages data controllers to consider the consequences of failure to adhere to data protection rules.

2. Taxonomy of Technical and Organizational Tools

14 In computer science literature, the quest to preserve privacy has often been linked to the confidentiality of data.[12] Even if the linkage of security and privacy has driven research in computer science, security tools are not the only available technical data protection measures that are proposed in the literature. In «Designing for Privacy and its Legal Framework» we, therefore, take a broader approach and classify the technical and organizational measures that data controllers can realistically implement to encode the legal principles described above. Such measures are divided into four categories, namely, security, anonymity, autonomy, and transparency tools.[13]

15 Security traditionally contains three main sub-elements, namely, the preservation of confidentiality, integrity, and availability.[14] Confidentiality requires that the data is not disclosed to unauthorized parties while in storage, in transit, or during processing. Integrity means that information remains accurate, complete, unmodified, and consistent; in other words, data cannot be altered without authorization. Finally, availability stipulates that information is accessible and usable by authorized parties. Other sub-elements, such as the preservation of authenticity, authorization, accountability, non-repudiation, and reliability, further add to a complete picture of a palette of security goals.[15] Technical mechanisms such as cryptographic tools, overall secure communication architectures that protect the confidentiality of data in transit or storage, digital signatures that ensure the integrity of a message and authenticate users, and digital certificates infrastructures ensuring that cryptographic keys can be exchanged, all working towards implementing the goal of security.[16]

11 Tamò-Larrieux, (Fn. 1), pp. 93 et seqq.

12 See Gürses, Multilateral Privacy Requirements Analysis in Online Social Network Services. Dissertation, Department of Computer Science, Katholieke Universiteit Leuven, 2010, pp. 36 et seqq.

13 Tamò-Larrieux, (Fn. 1), pp. 101 et seqq.

14 See, e.g., ISO/IEC 27000: 2016 standard on information technology (overview and vocabulary).

15 See for further references Tamò-Larrieux, (Fn. 1), pp. 105-106.

16 Tamò-Larrieux, (Fn. 1), pp. 109-123.

16 Another core goal of technical tools is anonymity. While ISO guidelines seem to approach the topic of anonymity in a binary fashion (one is either anonymous or identifiable),[17] it is also possible to quantify anonymity as the inability to «sufficiently identify the subject within a set of subjects, the anonymity set».[18] Likewise, pseudonymity is contained within the latter definition of anonymity; a pseudonym allows the creation of a separate identity that can – depending whether pseudonymous identities can be linked to the actual identity – be anonymous. In contrast to anonymity, pseudonymity tools enable the establishment of reputation.[19] Elements inherent to anonymity tools are unlinkability, unobservability, and deniability. To implement these features, several anonymity tools exist. Included in this set are mechanisms to render data in datasets anonymous (generalization, randomization), the creation of multiple identities and digital identity management service providers, as well as techniques to obfuscate the data individuals leave online (e.g., by using proxy servers which hide IP addresses of senders and receivers).[20]

17 Technical measures that fulfill the ideal of privacy in computer science are autonomy tools.[21] These tools allow an individual to exercise control over data processing operations. From a technical perspective, we define autonomy to encompass three significant points of control. The first covers mechanisms that regulate who has access to the data. However, unlike confidentiality tools, the focus of these autonomy tools is not only to block unauthorized access to data but also to prevent third parties which have authorized access to use the data for purposes to which the individual did not consent to (e.g., by employing data tags or using data stores). Furthermore, disposal control mechanisms such as personal data stores or personal information management systems exist, that provide the individual with control over when and with whom he or she shares personal data. Lastly, deletion control mechanisms ensure that data is not only unlinked from a database, but also entirely erased from the user-level layer to the physical layer.[22]

18 Lastly, we look at transparency tools which aim to provide users with information on the collection, analysis, use, and erasure of data. Doing so helps to redress information asymmetries between data controllers and data subjects. We rely on a broad definition of transparency tools which must provide the data subject, or a proxy acting on his or her behalf, with at least one of the following options: (1) information about the intended collection, analysis, implementation, or storage of data, (2) information on how to access the data and on the logic of the processing operations, or (3) information on how the personal data is matched to group profiles.[23] Transparency tools, in particular, are often not only technical tools but also include design features (e.g., visualizations such as privacy icons) and organizational procedures (e.g., privacy impact assessments and notice procedures).[24]

---

17 ISO/IEC 29000: 2011 and ISO/IEC 15408-2: 2008.

18 Pfitzmann/Hansen, A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, Version v.0.34, 2010, p. 10.

19 Pfitzmann/Hansen, (Fn. 18), p. 33.

20 Tamò-Larrieux, (Fn. 1), pp. 123-131.

21 See Pfleeger/Pfleeger, Security in Computing, 4th edition, 2007, p. 604.

22 Tamò-Larrieux, (Fn. 1), pp. 131-137.

23 Tamò-Larrieux, (Fn. 1), pp. 108-109.

24 Tamò-Larrieux, (Fn. 1), pp. 137-141.

3. GDPR on how to Implement Tools for Data Protection

19 While past research has primarily been mono-disciplinary, with legal principles on one side and technical tools on the other, the book «Designing for Privacy and its Legal Framework» considers how the law refers to the technical tools. By doing so, we provide further guidance to developers and engineers on how to implement technical and organizational measures.[25]

20 To be substantiated, guidance for implementing technical tools should be based on existing legal rules and regulations. Current regulation will, therefore, be the foundation of the evaluation of the application of privacy by design. Consequently, we describe how regulations invoke technical objectives, namely, security, anonymity, autonomy, and transparency. When data controllers seek guidance on how to implement privacy by design, they will rely on existing rules which specify the need to build secure, anonymous, and transparent systems that provide individuals with control over their data.

a) Data Protection through Security

21 The GDPR provides guidance to developers on which security tools to implement by mentioning specific security measures in Article 32 such as «(a) the pseudonymization and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data; (c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing». Whether such security measures are appropriate depends on the risks presented by each individual case. The GDPR specifies certain risks, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.[26] Thereby, the GDPR relies on common terms from computer science, such as confidentiality, integrity, and availability, with which developers are more familiar. Similarly, industry standards specify which security tools to implement and how to do so, thereby providing further guidance to developers and engineers designing secure systems.

b) Data Protection through Anonymity

22 In contrast to security tools, the GDPR provides little guidance on how to implement anonymity tools. It does not elaborate upon the means to render personal data anonymous, but rather only states that «objective factors, such as the cost and the amount of time required for identification» as well as «the available technology at the time of the processing and technological developments» should be taken into account when assessing whether anonymization measures yield irreversible unlinkability.[27] The GDPR has focused more on the concept of pseudonymous data, which it mentions in various recitals and articles. It defines pseudonymization as «the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional

25 Tamò-Larrieux, (Fn. 1), pp. 167 et seqq.

26 Art. 32(2) of the GDPR.

27 Recital 26 of the GDPR.

information», and explicitly states that technical and organizational measures shall ensure that this «additional information» is stored separately from the identifiable information.[28] This language is the most specific example of the GDPR describing guidelines intended to ensure the objectives of a user's of anonymity, unlinkability, and pseudonymity. It does not elaborate on more specific (technical or organizational) pseudonymization measures that data controllers should take into consideration.

c) Data Protection through Autonomy

23 Within the GDPR, autonomy tools, in particular access and permission control tools, are primarily implemented through consent. The GDPR provides guidance on how to design consent forms, such as requiring that they be presented in a clear format and be separated from other text or information.[29] Furthermore, there must be an option to withdraw one's consent at any time.[30]

24 The GDPR mentions the term «control» several times (unlike the Directive 95/46/EC), putting more emphasis on employing autonomy tools.[31] Recital 68 of the GDPR (which by itself is not binding, but provides guidance on how to legally understand control or autonomy) for example states that in order to strengthen the control over personal data, data subjects must be able to receive said data «in a structured, commonly-used, machine-readable and interoperable format». Two points are key: First, the GDPR acknowledges the possibility of employing machine-readable formats as a tool to foster autonomy. In this sense, it refers to an existing concept in computer science which can, in theory, be adopted into the design of services and products. Second, Recital 68 introduces the concept of interoperability and the ability of a user to more easily change service providers (data portability). This concept brings technical features into the foreground and has far-reaching implications for developers and engineers.

d) Data Protection through Transparency

25 As with autonomy tools, the GDPR does not provide extensive guidance on which transparency tools to implement; however, it does acknowledge the importance of visualization efforts in order to maintain a sense of transparency.[32] In particular, it elaborates on data protection impact assessments and the use of privacy certificates in order to facilitate recognition of privacy-friendly products and services.

26 The goal of data protection impact assessments is to ensure compliance with all legal requirements, and thus it can be considered a preliminary step of any privacy by design process.[33] Privacy impact assessments take

28 Art. 4(5) of the GDPR. Cf. also Recital 29 of the GDPR: «In order to create incentives to apply pseudonymization when processing personal data, measures of pseudonymization should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organizational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is *kept separately*. The controller processing the personal data should indicate the authorized persons within the same controller.» (emphasis added).

29 Art. 7(2) of the GDPR.

30 Art. 7(3) of the GDPR.

31 Cf. i.a. Recital 7, 68, 75, 85 of the GDPR.

32 See Recital 58 of the GDPR.

33 Plath/von dem Bussche, in Plath (ed.), Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2nd edition, 2016, Art. 35, marginal No. 1.

a process-oriented approach to privacy protection. While data protection impact assessments generate transparency within the company collecting and processing data, their publication is not required by the GDPR, thus the results of such assessments remain behind closed doors. Further transparency could be provided to data subjects by publishing a summary of each assessment or the steps taken to minimize identified privacy threats.[34]

27 Additionally, compliance with the principle of data protection by design and default may be demonstrated by an «approved certification mechanism pursuant to Article 42» of the GDPR.[35] Privacy certificates or seals attest to compliance with specific privacy requirements, thus providing additional legal security to data controllers. Recital 100 of the GDPR states that these mechanisms should be further fostered, as they provide clear knowledge regarding a companies' data protection policies (i.e., applied transparency), and signal to consumers that the company has implemented all necessary privacy regulations.

e) Balancing of Interests

28 The implementation of technical and organizational measures is never an absolute obligation. The need for privacy protection in general, and particularly through technical tools, requires a balancing of interests. When determining the appropriate level technical and organizational tools to be implemented, Article 25(1) of the GDPR mandates that the data controllers take into account the state-of-the-art of technical measures, material cost of implementation, nature, scope, context, and purposes of the data processing techniques, and the likelihood and severity of the risks to the rights and freedoms of individuals.

29 While the state-of-the-art requirement is more objective and straightforward than the others, requiring developers and engineers to apply technical measures that are status quo in a given industry or context, and requiring to take cost and effectiveness into consideration, necessitate that a balance be struck between privacy-friendly design and economic feasibility for a given data controller. The costs include all incurred expenses from the planning and implementation of specific technical tools.[36] Likely included in these expenses are the costs of development of customized technical and organizational measures, secure hardware, and implementation of a secure password administration system. Other indirect costs, however, such as the revenue loss due to the implementation of such technical measures, are not covered by Article 25(1) of the GDPR.[37] In fact, economic obstacles to the implementation of technical tools exist, as high-performance hardware equipment becomes necessary when technical tools become computationally heavy.

30 Additionally, balancing the costs necessitates taking into consideration whether a measure is appropriate with respect to its protective purpose. This balance takes the likelihood of a privacy infringement and the

34 Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev. 01, (17/EN), 4 October 2017, p. 18.

35 Art. 25(3) of the GDPR.

36 See Paal/Pauly/Martini, in Paal & Pauly (eds.), Datenschutz-Grundverordnung, 2017, Art. 25, marginal No. 41-42.

37 Paal/Pauly/Martini, Art. 25, marginal No. 41 relying on the wording of Art. 25(1) of the GDPR which refers only to "the cost of implementation".

damage of such an infringement into consideration. As a general rule, the higher the risks of an infringement and the higher its damage, the more extensive (and costly) the protection measures must be.[38] This requirement stipulates the undertaking of a risk analysis and evaluation; such a risk assessment is codified in Article 25 of the GDPR. This risk assessment aligns with Article 35 of the GDPR, which lays out the requirements for data protection impact assessments. Unlike the privacy by design and default provision, the provision on data protection impact assessments provides data controllers with a non-exclusive list of scenarios which require an assessment prior to processing. Such scenarios include operations which systematically and automatically evaluate an extensive amount of personal data (included here are profiling operations) and processing operations based on a large scale of sensitive data. This assessment should be documented and updated whenever changes to the processing operations are foreseen.

III. Putting Data Protection by Design into Context

31 In order to illustrate how Article 25 of the GDPR works in practice, we describe a product developed by a fictional startup: A smart wearable wristband (the MySleep bracelet), measuring a user's (Alice's) sleep cycle. We follow the data processing steps and, in each phase of the life cycle of data, analyze the technical and organizational measures the startup must implement to comply with Article 25 of the GDPR.[39]

1. Collecting and Transmitting Alice's Data

32 We start with the collection and transmission of data via MySleep's website, bracelet, and through third parties. This early phase determines who collects what data from Alice. It also illustrates how the data is transmitted between devices. In our case study, Alice purchases a MySleep bracelet on the MySleep website. In order to do so, she enters her name, shipping address, and credit card information into a standardized form and agrees to MySleep's Terms of Service and Privacy Policy. Once her bracelet arrives, Alice downloads the smartphone application and registers with her full name and email address. Once logged into her account, Alice can provide MySleep with further physiological information (e.g., age, height, weight) and physical status (e.g., body aches, meals before bedtime, overall exposure to blue light). Alice wears the bracelet at night, thereby collecting sensor data such as her pulse, heart rate, body temperature, and duration of sleep. Every morning, Alice connects her bracelet via Bluetooth to her smartphone, which immediately transmits the data to a cloud server. Both the bracelet and her smartphone only store data as long as needed to complete the transmission to the cloud.

33 In order to comply with Article 25 of the GDPR, the MySleep startup has different technical and organizational tools it must apply during this early phase of the life cycle of data. First of all, Alice should not be required to provide her full name to register for the service, since such data is not necessary for MySleep's performance of the service. The default setting should require only a username, encouraging users to set pseudonymous identities. Additionally,

38 Paal/Pauly/Martini, Art. 25, marginal No. 37.

39 For more details on this fictional case see Tamò-Larrieux, (Fn. 1), pp. 203 et seqq. (Chapter 9 – Privacy by Design for the Internet of Things: A Startup Scenario).

the application should encourage Alice to enter approximate physiological data (such as only the month and year instead of her exact birthdate). Additionally, MySleep must provide Alice with transparent terms regarding the processing of her personal data. The GDPR elaborates in greater details than its predecessor (the Directive 95/46/EC) on the design of privacy policies. Transparent terms under the GDPR must include, among other requirements, who processes the data, what data is being collected and for what purposes, to whom the data is being disclosed, what safeguards are in place if data is disclosed aboard, and a list of her participation rights.[40]

34 In addition to the use of anonymity and transparency tools, security tools also are essential in this first phase of the life cycle of data. Secure end-to-end communication channels (e.g., Transport Layer Security [TLS]) must be implemented to ensure that even if the data is intercepted, it remains encrypted. MySleep logs the transmission of data and requests that Alice's smartphone authenticates itself (via an authentication token) before allowing the upload of health data; these measures help to identify improper transmissions. Likewise, the personal data stored on the server should be encrypted. From a privacy by design perspective, it is reasonable to differentiate among encryption schemes depending on the risks associated with the different types of data (see above, III.3.e Balancing of Interests). In this case study, two different databases are set up, each containing different types of data: The *identity database* requires a higher level of data security measures, as it stores directly identifiable data; the *health database,* in comparison, stores pseudonymized data. In the case of a breach, only the identity database poses a high risk to Alice's privacy. The health database, while containing more sensitive information, presents a lesser risk, as the data is pseudonymized, and Alice can only be identified in combination with the identity database. Therefore, MySleep must be reasonably allowed under Article 25 of the GDPR to differentiate between the measures taken to adhere to the principle of data security.

2. Analyzing Alice's Data on External Servers

35 The analysis phase looks at how and where Alice's data is stored and analyzed, as well as who, besides MySleep, has access to her data, and thus, the security of the infrastructure used to analyze the data is paramount in this phase. Typically, a startup will rely on external and scalable cloud computing services. In our case, MySleep safeguards Alice's data in two separate databases (the identity and health database), both of which are stored on Amazon Web Service (AWS) servers. These databases are not publicly accessible through the Internet, in fact, they may only be accessed through the MySleep network by a set of permitted MySleep administrators.

36 Before relying on an external service provider for any processing, MySleep must ensure that these external providers or processors provide sufficient guarantees to implement appropriate technical and organizational measures.[41] These guarantees are either provided by a contract between the data controller and the external

[40] See Art. 13 and 14 of the GDPR.

[41] Art. 28(1) of the GDPR.

service provider (e.g., AWS) or by EU legislation that binds the service provider. At the minimum the contract or law must define: (1) the subject-matter and duration of the commissioned processing, (2) the nature and purpose of the commissioned processing, (3) the type of personal data being processed, (4) the categories of users included, and (5) the obligations and rights of MySleep. Therefore, in order to ensure compliance with the GDPR, MySleep must first evaluate the physical controls that AWS employs and certifications of the company. In a second step, the security level necessary for each database must be determined. The authorization level to access either one or both of the two databases must be strictly defined, and automatic restriction of access when a system receives an incorrect identification must be technically implemented. Additionally, access to logical systems should be automatically blocked after periods of inactivity in order to prevent potential disclosure of data. These measures not only require technical implementation, but must also be contained in organizational rules that are known by employees. Depending on the database, the encryption of data at rest and in transit may vary. While health data must be analyzed and visualized for Alice, and since this task requires complex computation, such data can realistically not be analyzed in an encrypted format (even if homomorphic encryption enables that). This balancing of cost is necessitated by Article 25 of the GDPR, which requires that data controllers consider the various risks associated with databases as well as the nature, context, and purpose of processing.

3. Providing Alice with the Service

37 Every morning, Alice uses her wearable to obtain information about her sleep. To do so, the sensors' data is uploaded to the servers, processed, and communicated or visualized back to her. The visualization of her data allows Alice to screen for obvious mistakes (e.g., if the sleep logs are clearly too long or short). She can access additional information on her sleep quality as well as explanations of the values of her recordings. Visualizations enable Alice to grasp the overall processed sensor data. Results of analyses that combine her sensor data as well as physiological and physical data are less obvious to Alice (i.e., how a result was yielded is typically not shown to Alice). In light of Article 25 and Article 22 of the GDPR (the scope of the latter being much debated), some information expanding upon the logic involved behind the computations could be helpful.

38 In order to ensure that different categories of Alice's data are used for the purpose she agreed to, technical separation controls must be implemented in order to ensure that data collected for each individual purpose are processed separately. Separation is already achieved through the splitting of databases, as well as by imposing handling restrictions vis-a-vis who within MySleep is able to process various data types. Other technical tools that exist to ensure compliance with the purpose and disclosure limitation include privacy obligations and tags. Additionally, access rights on a «need-to-know» basis ensure that employees at MySleep are not able to access both databases and, in turn, reidentify Alice. Lastly, internal guidelines that explain how employees should cope with data breaches as well as protocols in case of such a breach must

be in place. Compliance training should be used to raise awareness on such topics.

4. Deleting Alice's Data

39 In the event that Alice decides to delete her account, MySleep must ensure that her data in the identity database (which is not anonymized or pseudonymized) is immediately erased from the server. Slowly, her data will then be erased from the company's backup systems. Likewise, if Alice stops using her bracelet and the application, MySleep does not need the data any longer for the purpose of providing Alice with a service and should, therefore, have a policy in place to automatically delete a users account after a long inactive period. How long the inactivity must last before MySleep needs to erase Alice's data is not explicitly defined within the GDPR, and best practices within the industry should be consulted in this respect. Additionally, MySleep needs to have a system in place, which notifies third-party providers (e.g., if Alice allowed optional cookies for improved targeting functions by third parties) that may have access to Alice's data, that she requested her personal data to be erased. Thus, deletion of Alice's data requires not only technical but also organizational measures, such as guidelines directed to employees in order that they know how to respond to erasure requests and completion of secure deletion (i.e., deleting the content of the data layer-by-layer). Overall, the deletion process must be logged, and not all MySleep employes should be able to actually trigger such a process.

IV. Outlook

40 In «Designing for Privacy and Its Legal Framework» we aim to enhance both developers' and policymakers' understanding of what the principle of privacy by design entails in practice. Policymakers should consider how they want legal principles to regulate behavior and be implemented by data controllers.[42] The more precise guidance each principle prevails to data controllers and the more clearly each principle aligns with technical objectives, the easier it will be for developers and engineers to adhere to. In turn, the more abstract and unaligned with the technical objectives, the more of a discrepancy will exist between the law and the implementation of technical tools. Self-regulatory standards can help to bridge this gap from the abstract legal sphere to the concrete technical sphere; yet, developers will require more guidance on how to comply «technically» with legal principles. Concrete scenarios and case studies help to break the legal principles down into more concrete implementation schemes.

41 More clarity regarding which tools are appropriate to use can be provided by development of privacy engineering guidelines. Such guidelines aim to define the technical measures that should be implemented to minimize identified privacy risks. Additionally, the education of engineers and users must play a vital role in every regulatory strategy to achieve better privacy and data protection. Likewise, privacy professionals, such as Chief

[42] See for a comprehensive overview of the functions of legislation: Gasser, Perspectives on the Future of Digital Privacy. Rechtsfragen im digitalen Zeitalter. Schweizerischer Juristentag 2015, ZSR Band 134 II, 337–448, pp. 368 et seqq.

Privacy Officers, will help to ensure compliance with data protection legislation within a company. Such measures and positions are also crucial in light of the rapidly changing technological and social environment that includes ever more digitalization and dependence on it. New regulatory solutions will be required in the coming time, but can only be brought about through regulatory and perspective shifts toward alignment with the principle of privacy by design and default.