CEST Centro de Estudos Sociedade e Tecnologia
USP Universidade de São Paulo
Bulletin - Volume 6, Number 06, August/2021

Privacy by Design and Privacy by Default

Marcel Simonette

With several data protection regulations around the world, understanding the concepts is essential to build a good foundation for how companies deal with data protection and privacy without overloading compliance. At the same time, the protection and use of personal data are not solely about compliance; it is about building customer trust. And trust is the key to all businesses, especially those who operate online.

The European General Data Protection Regulation (GDPR) is the set of norms and regulations for data use practices created by the European Parliament and the Council of the European Union. This regulation incorporates some concepts such as Privacy by Design and Privacy by Default, dealing with data diversity, whether it's a browser cookie, for example, or your name and address. Data protection involves two fundamental concepts: transparency and responsibility.

Privacy by Design states that companies need to have data protection and privacy in mind at every step that involves processing personal data

Privacy by Design

Privacy by Design, also known as PbD, is a set of principles developed in the 90s by the Information and Privacy Commissioner of Ontario, Canada, Dr Ann Cavoukian. An interview with Dr Ann Cavoukian is available on CEST's YouTube channel. Privacy by Design states that companies need to have data protection and privacy in mind at every step that involves processing personal data. In practice, companies' initiatives must ensure that privacy and data protection are considered since the idealization, whether it is an initiative of the IT department or any other department. Internal projects, product development, software development, and IT systems are some examples of companies' initiatives.

Despite being created in the 1990s, Privacy by Design is directly related to the GDPR. Privacy by Design principles reduce privacy risks and build trust, as they are proactive rather than reactive measures. They don't offer remedies for resolving privacy infractions once they have occurred; they aim to prevent infractions from occurring. In short, Privacy by Design comes before the fact, not after.

To put the ideas of Privacy by Design into practice, we need to understand the pillars that support it, as the principles will change how companies idealize their projects.

Privacy by Design has seven foundational principles:

- Be proactive rather than reactive, choose to prevent rather than cure;
- The privacy and protection of the user must be guaranteed at all times, without the need for configurations by the user (privacy is a default setting);
- Incorporate privacy into the project, not just being seen as an addition, but as part of what will be developed (privacy embedded into the design);
- All possible functionalities must be complete and protected, generating a mutual benefit, for the user and the company (positive-sum, not zero-sum);
- Security must be present from the capture to the destruction or sharing of the data, that is, end-to-end (full lifecycle protection);
- Maintain transparency with the data subject, informing the user or consumer about the reason for collecting the information and who has access to it (visibility and transparency);
- User privacy must be respected at all times.

The focus of all company actions must be precisely the customer. It must be guaranteed by the company that the customer data is protected and fully secure.

Privacy by Default

Privacy by Default means that companies need to design their systems, services, products, and business practices to automatically protect personal data. The users or consumers don't have to take any steps to protect their data – their privacy remains intact, and they don't need to do anything. And, if the product or service demands user data to enable optimal use, these data will only be kept for the amount of time necessary to provide the product or service. If more personal data than is required to provide the service is requested, "privacy by default" has been violated.

Most users are just looking for convenience and don't bother figuring out how to change the privacy settings. In this scenario, Privacy by Default is a differential for companies that value transparency. The companies clarify the necessary data and how users can change the default configuration and its consequences, strengthening their trust in the relationship with their users. The users are protected, and they are informed of what data he is providing and for what purposes.

Privacy by Default is a consequence of Privacy by Design

The most restrictive privacy setting possible is established from moment zero. Only the essential data to provide the service or deliver the product are collected.

Privacy by Design and Privacy by Default

Privacy by Design is about how a project should be developed through the principles mentioned above. Since the beginning of any project involving customer data, it is necessary to consider data security and privacy, anticipating problems and reducing the risk of data theft and leaks.

The projects generated through this concept are proactive. They offer control for the user or consumer to change the system's default settings, choosing to provide the data or not.

When we talk about Privacy by Default, it is necessary to understand that "by Default" means that the most secure settings are applied by default as soon as the product or service is released to the public. In other words, the user doesn't need to choose the privacy and protection settings, as these settings are pre-configured considering privacy. All personal information provided by the user is collected only for the delivery of the service or product. However, even with Privacy by Design and Privacy by Default, all the necessary data must be informed to the user, as well as the purpose of each one of them.

When talking about data storage time, it is worth pointing out that they are kept only for the period in which the project or system will use them.

It is possible to understand that Privacy by Default is a consequence of Privacy by Design. Both are strategies that, when performed correctly, guarantee privacy, which is a fundamental point today.

Relationship with LGPD

Despite the inclusion of Privacy by Design and Privacy by Default in the GDPR, the Brazilian legislation LGPD (Lei Geral de Proteção de Dados, in Portuguese) doesn't have these principles explicitly. However, the Brazilian legislation has similar concepts linked to data protection, dictating how companies must guarantee security.

It is worth pointing out that, although LGPD does not require that companies use Privacy by Design and Privacy by Default, there is nothing to prevent from being applied. At last, Privacy by Design and Privacy by Default help companies to offer more security and privacy to user data. Moreover, the users become the main moderator of their data. The users gain control over which data will be provided and which will not, knowing which data are mandatory for the purpose explicitly stated by the company.

Marcel Simonette *is researcher at CEST-USP and Professor of the MBA-USP Data Science and Analytics at PECE – USP*

Academic Coordinator: Edison Spina

This article is a result of the author's ascertainment and analysis, without compulsorily reflecting CEST's opinion.