**Introduction**

The role of technology, with its capabilities and limitations, is becoming increasingly vital in our personal lives and throughout our societies. How well people can exercise their basic rights is influenced not just by laws and societal standards but by the technological tools available to them. Lately, revelations about the misuse of personal information have elevated the discussion on data privacy to new heights. The development and application of technology must prioritize protecting individual rights over the narrow financial motives of a select group of companies.

In early 2018, discussions centering around handling of personal data via sophisticated ICT (Information and Communication Technology) surged to unparalleled heights. Committees within the European Parliament[[1]](#footnote-1), the U.S. Congress[[2]](#footnote-2), and national legislatures of EU countries, including Germany[[3]](#footnote-3), and France[[4]](#footnote-4), started conducting or contemplating probes. Lawmakers alongside the broader public, were eager to comprehend the methodologies behind the tracking of individual online activities and the subsequent usage of amassed personal data. A key aspect of these inquiries involved the testimonies from executives at major technology corporations.

As concern over privacy issues heightens today, a growing number of consumers are becoming hesitant to share their personal data with companies. In 2019, data from the Pew Research Center[[5]](#footnote-5) indicated that 81% of American consumers were apprehensive about businesses gathering their personal information (*see below)*. Many Americans believe they have barely any control over the data collected and used by companies the government and its agencies.

Collecting customer data is typically critical for the smooth functioning of businesses. Thus, building and maintaining customer trust becomes essential through a commitment to their privacy. This commitment can be demonstrated by adopting a strategy centered on privacy by design. Privacy by Design is a proactive strategy to guarantee data security and privacy from the very beginning of any system, service, or product development. Integrating privacy into the architecture and design of IT systems and business procedures is the fundamental component of this concept.

**Privacy by design**

Privacy-by-design represents an engineering philosophy in which privacy considerations are embedded into the product design process from the earliest stages, rather than treating data protection and consumer privacy as secondary considerations to be addressed after a product’s development or at the culmination of its lifecycle. This methodology ensures that privacy safeguards are foundational, and not retrofitted post development.

Article 25[[6]](#footnote-6) of the GDPR, titled "Data Protection by Design and by Default,"[[7]](#footnote-7)mandates that controllers must apply suitable technical and organizational measures from both the design and operational phases of data processing. These measures, decided based on current technological capabilities, cost, and the processing's nature, aim to embed data protection safeguards in compliance with the Regulation and ensure the protection of data subjects' fundamental rights. It highlights that only the personal data necessary for each specific processing purpose should be handled by default. Additionally, it mentions that obtaining approved certification can help demonstrate adherence to these requirements[[8]](#footnote-8).

Moreover, the origin of these principles is rooted in the Data Protection Directive 95/46/EC[[9]](#footnote-9), which GDPR subsequently succeeded. Recital 46 of the Directive emphasizes the importance of incorporating technical and organizational measures to protect individual's rights and freedoms in relation to data processing, starting from the system's design phase and continuing through all processing operations.

As deployment frequency continues to increase, treating security and privacy as secondary concerns will lead to a manually intensive, protracted, and expensive process unlikely to keep pace, perpetually lagging. Furthermore, the loss of a customers' data could seriously damage an organization's brand and financial standing due to significant costs. The principal insights presented are derived from examining research data compiled by the Ponemon Institute, as analyzed by IBM Security, provided below

**Engineering privacy and data protection**

EU data protection legislation along with other privacy standards, like the Fair Information Practice Principles[[10]](#footnote-10) or the OECD guidelines[[11]](#footnote-11), set forth goals to be achieved but often don't provide specific instructions on how to achieve them in practical terms. Employing the concept of privacy by design can address this problem by offering concrete guidance on how to implement the following objectives;

1. Devise a strategy to blend privacy and data protection requisites into initiatives for creating and operating any process, procedure, or system that processes personal data.
2. Identify and enforce appropriate technical and organizational strategies within these processes, procedures, and systems to defend both individuals and their data. Utilize technological advancements as aids for these measures.
3. Incorporate privacy support into the organizational management and governance framework, specifying tasks, and delineating and assigning resources and responsibilities effectively.

Several current methodologies in privacy engineering operate by establishing data protection objectives, which are either derived directly from data protection principles or through defining operational intermediary goals that facilitate the achievement of the primary objectives. Alternatively, some methodologies adopt a more explicit risk management strategy by identifying and addressing the risks associated with failing to uphold the data protection principles, or by evaluating the potential negative effects on individuals directly.

In addition to the above, the 7 principles of privacy by design can help in the implementation process:

GDPR treats its principles as objectives to attain, employing them as intermediaries to safeguard individuals' basic rights and freedoms, regardless of the risk level. Simultaneously, it takes a "precautionary" stance, defining certain safeguards that must be implemented under specific conditions (such as security protocols and notifications of personal data breaches). What remains to ensure the desired level of protection for individuals and to secure their established data protection rights, given various factors like context, data nature, and processing type, is addressed through a risk management strategy. This strategy permits organizations to pinpoint new safeguards and aids in refining and incorporating obligatory measures based on individual risk levels. The approach to adopting a catalog of specific design patterns to craft solutions for recognized privacy issues is inspired by software development methodologies.

**Addressing the entire lifecycle of services and products, organizational governance and management**

Some methodologies in privacy engineering predominantly emphasize either the initial requirements phase or the implementation strategies. However, it's essential for privacy engineering to encompass the entire lifecycle of a product or service, starting from its conception to its final decommissioning. To facilitate this holistic approach, it is crucial for an organization to establish proper governance and management frameworks. An example of a methodology that considers the full project lifecycle is the one developed by the PREPARE research project[[12]](#footnote-12). It outlines detailed privacy-focused activities and outcomes across eight distinct phases of a project, ranging from evaluating the organizational environment and infrastructure to the process of system decommissioning. Other useful guidance can be found in a web publication of the Norwegian data protection authority[[13]](#footnote-13).

In essence, ensuring privacy by design and default means that safeguarding individuals' fundamental rights becomes a task for the organization, which should be reflected in its organizational governance and management structure. This includes properly assigning privacy tasks and responsibilities in an accountable manner. While the primary responsibility for meeting privacy requirements lies with management, the task of implementing these requirements can be delegated to departments tasked with designing and managing relevant systems. IT and technology departments provide support to business owners, guided by their directives and best practices for privacy by design.

The involvement of privacy and data protection officers is key in the privacy by design approach, playing a central role. It is essential for them to be involved from the beginning stages of planning systems for personal data processing. This allows them to support managers, business owners, and IT and technology departments, aligning with the required skill set.

The European Data Protection Supervisor (EDPS)[[14]](#footnote-14) has released guidance on IT management and governance. The guidance aims to assist EU institutions in integrating privacy and data protection standards into the creation and functioning of IT systems. Additionally, the guidance outlines how an organization's IT governance can be structured to align with the principle of accountability. While these guidelines are specifically designed for the EDPS's direct stakeholders, the principles they are based on have universal applicability.

**Standardization efforts**

Initiatives to include privacy considerations in system design through standardization efforts[[15]](#footnote-15) are progressing across various organizations and groups. These initiatives often build on established IT security risk management methods, adapting and expanding them to address privacy concerns. The ISO has developed standards for privacy, including a privacy framework (ISO/IEC 29100) and a privacy architecture (ISO IEC 29101) that focus on personally identifiable information (PII) in the context of information and communication technology. This involves broadening the scope of existing standards for information security management, specifically ISO/IEC 27001 and 27002, to encompass privacy management. Additionally, the IETF has published RFC 6973[[16]](#footnote-16), which discusses "Privacy considerations for Internet Protocols", aiming to integrate privacy considerations into the development of internet protocols.

The expectation is for privacy standardization to increase, particularly considering how certifications might serve to show adherence to GDPR requirements. In detail, certification methods can be employed to show adherence to the principles of data protection by design and by default[[17]](#footnote-17). In 2015 the EU Commission requested[[18]](#footnote-18) the European Standardization Organizations (ESOs)[[19]](#footnote-19), which have a cooperation agreement with the Commission, to work on a “privacy and personal data protection by design approach” and “privacy and data protection management framework” for the security industry.

In 2017, following the introduction of the GDPR, the ESOs contemplated the chance for an expanded and more complex work agenda combining privacy, data protection, and cybersecurity. This plan encompasses: a standard for “Data protection and privacy by design and by default” that offers “requirements for manufacturers and/or service providers” for executing the principle ‘relevant across all business sectors, including the security industry’, as well as technical reports on precise applications of the principle[[20]](#footnote-20), initiatives on cybersecurity and privacy and data protection to support recent and ongoing relevant EU level policy making[[21]](#footnote-21). This standardization activity may provide a baseline for the industry and all stakeholders for establishing the state of the art in privacy by design. For this reason, ensuring that the outcome aligns with pertinent legal requirements is essential for it to truly facilitate the enforcement of data protection principles from the design phase.[[22]](#footnote-22)

**Privacy Design Strategies**

**Software design patterns, strategies, and technologies**

Software architecture is about making critical decisions on a software system's[[23]](#footnote-23) organization, involving selecting structural elements, defining their interfaces, and specifying their interactions to form a cohesive subsystem. It also entails adopting an architectural style for this organization. Software development follows methodologies like the waterfall model, which is a six-phase process: concept development, analysis, design, implementation, testing, and evaluation. Since systems evolve through several iterations, software development is cyclical, with updates and evaluations leading to further modifications. Privacy considerations are integrated at every stage, with privacy design strategies applied in early phases, design patterns in the design stage, and privacy-enhancing technologies during implementation.

**Design Patterns**

Design patterns play a crucial role in structuring software systems. They offer a framework for refining components and their interactions within a system, addressing common design issues in specific contexts. Such patterns facilitate breaking down complex problems into smaller, manageable ones, guiding designers away from intricate implementation details. They also highlight the potential outcomes of using these patterns, helping designers assess their effectiveness towards achieving the system’s goals. For instance, the Model-View-Controller[[24]](#footnote-24) pattern is known for separating data representation from user interface and interaction mechanisms. Although explicit examples of privacy-focused design patterns are few, with notable work by Hafiz, Pearson, van Rest, and initiatives by UC Berkeley[[25]](#footnote-25), numerous implicit patterns exist, yet to be formally recognized.

**Design Strategies**

Design patterns often target specific problems and aren't always directly usable in the early stages of concept development. In contrast, architecture patterns offer a higher-level structural framework for software systems, defining subsystems, their roles, and the organization of their relationships[[26]](#footnote-26). An example of such an architecture pattern is the Model-View-Controller (MVC). The line between architecture and design patterns can blur, highlighting the value of examining system design from various levels of abstraction. Since design patterns can sometimes be too narrow for certain applications, broader design strategies are proposed. These strategies outline general approaches for achieving specific design goals, preferring certain structures while not being prescriptive. This flexibility makes them useful even in the concept development and analysis stages of the design cycle. A privacy design strategy is one that seeks to protect privacy as its primary objective, demonstrating how strategies can focus on overarching goals without dictating the exact structure of the system.

**Privacy Enhancing Technologies**

In discussions around designing for privacy, Privacy-Enhancing Technologies (PETs) have gained significant attention and undergone extensive research over many years. (A summary of this extensive research is provided later in this document.) A notable definition, subsequently almost verbatim embraced by the European Commission, was proposed by Borking and Blarkom among others. They defined Privacy-Enhancing Technologies as a collection of measures within ICT that safeguard informational privacy by reducing or eliminating personal data. This, in turn, deters unnecessary or undesired processing of personal data, all while maintaining the information system's functionality. Essentially, PETs are applied to execute specific privacy design patterns using tangible technology. For instance, ‘Idemix’ and ‘U-Prove’ serve as examples of privacy-enhancing technologies that embody the anonymous credentials design pattern, although implicitly. Additionally, numerous other examples exist, such as ‘cut-and-choose’ strategies, and ‘onion routing’ , just to highlight a couple.

**Privacy Techniques**

**Authentication**

For optimal privacy against active adversaries, it's essential to sometimes shield the identities of both the initiator and responder. This level of protection is achieved through secret handshake protocols, where both participants keep their identities hidden until certain identity aspects are mutually verified. Such protocols enable users to authenticate each other's group membership through a shared key without revealing any personal or group identity details. There are also developments that support private authentication within groups.

Emerging authentication paradigms include:

1. Client-server authentication, which verifies a user's identity through an identifier (e.g., username) to a server or third party. This model is common in federated chat protocols like XMPP, where users authenticate with an XMPP server to confirm their identity.
2. End-to-end authentication allows users to directly verify each other's identities without needing a trusted third party. This can involve running an authentication protocol to check a user's identity claims and secure communications cryptographically. Methods might include sharing a secret or verifying public keys. This approach, highlighted for its privacy and data protection potential, enables secure, direct communication channels that bypass potential third-party compromises (see Section 4.3.2 on channel security).
3. End-to-end models are recommended for their direct, secure communication and protection against third-party breaches, aligning with privacy and data protection principles.[[27]](#footnote-27)

**Attribute-based Credentials**

Attribute-based credentials[[28]](#footnote-28) present a fundamentally different approach for managing identity when compared to the traditional methods of federated identity management detailed in section 4.1.3. Unlike in federated (or network-based) identity management, where a user's identity information is always retrieved via an online identity provider (IdP) when accessing a service, attribute-based credentials center the user in all identity-related transactions. In federated identity management, the process involves directing the user to an identity provider whenever they attempt to access a service. Only after successfully logging into this identity provider does the IdP send the required user information back to the service provider. This situates the IdP at the heart of all identity-related transactions, thereby raising numerous concerns regarding security, privacy, and usability. For instance, the identity provider has the capability to track all the service providers with whom the user interacts, while service providers might gain access to more personal information about the user than what is strictly necessary to provide their services. If the service provider requests information critical for accessing valuable resources (like health records or financial details), the identity provider essentially holds the keys to this information, enabling access without the user’s consent or knowledge. In contrast, attribute-based credentials (ABC) ensure that the user remains the focal point of any transaction concerning their identity[[29]](#footnote-29).

**Secured private communication**

Physical network connections generally offer inadequate assurances of confidentiality and privacy. Local networks are increasingly reliant on wireless technology, and securing wide area networks physically against widespread surveillance is not feasible. Hence, any data exchanged between a user and a service or among users should ideally be encrypted using advanced cryptographic methods to ensure that it remains incomprehensible to unauthorized listeners. This applies to all forms of user communications: personal or sensitive information should be encrypted to maintain its confidentiality (and security), but even public resource requests should be encrypted to prevent any potential eavesdroppers from deducing users' browsing behaviours, profiling, usage of services or gathering identifiers for subsequent tracking.

**Communications anonymity and pseudonymity**

Using end-to-end encryption safeguards the content of conversations, yet it doesn't shield metadata from external parties. Metadata refers to data that provides context about the communications, such as the identities of the communicators, when and how much they communicate, the length of their conversations or calls, and the locations or potentially the identities of the network connection points. The leakage of metadata can severely infringe upon one's privacy. For instance, revealing that a journalist has been in contact with a source inside a corporation or government body could jeopardize their role as a confidential informant, even if the actual content of their exchanges remains secure. Similarly, if someone is consistently searching for information regarding a certain type of cancer, it might suggest a personal health issue or condition. Metadata can also reveal lifestyle choices or relationships that might not be directly communicated. For instance, consistently finding two cell phones in the same location outside of work hours and during weekends could suggest a personal relationship. Analysis of metadata through mobile phone tracking or WiFi/IP address logs can expose such relationships, even without any direct message exchanges.[[30]](#footnote-30)

**Conclusion**

As can be seen from previous sections, several policy documents refer to privacy/data protection by design and by default either as principles or as practical implementation concepts. While these terms are not clearly defined in all these reviewed documents, they have a common focus, namely, to incorporate all privacy/data protection principles through all the design and use stages of data processing and this to be the norm by default.

As nations worldwide keep enacting new privacy regulations and compliance standards, it's crucial for companies to integrate privacy safeguards at the heart of their development phases and throughout their operational lifespan. This approach not only guarantees adherence to legal requirements but also fosters trust among consumers.

1. 1EP President Tajani invites Facebook CEO: <http://www.europarl.europa.eu/news/en/agenda/briefing/2018-0416/1/facebook-meps-to-discuss-misuse-of-eu-citizens-personal-data>. [↑](#footnote-ref-1)
2. US Senate Committee hearing of Facebook CEO: <https://www.judiciary.senate.gov/imo/media/doc/04-1018%20Zuckerberg%20Testimony.pdf>. [↑](#footnote-ref-2)
3. German Federal Parliament, Digital Agenda Committee, report <https://www.bundestag.de/presse/hib/2018_03//548624>. Resolution French Parliament, <http://www.assemblee-nationale.fr/15/pdf/propositions/pion0858.pdf>. [↑](#footnote-ref-3)
4. German Federal Parliament, Digital Agenda Committee, report https://www.bundestag.de/presse/hib/2018\_03//548624. 5Resolution French Parliament, <http://www.assemblee-nationale.fr/15/pdf/propositions/pion0858.pdf>. [↑](#footnote-ref-4)
5. Pew Research Centre: Americans and Privacy

   <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/> [↑](#footnote-ref-5)
6. Giovanni Buttarelli on CNN, 5 April 2018: http://transcripts.cnn.com/TRANSCRIPTS/1804/05/qmb.91.html. [↑](#footnote-ref-6)
7. Data controllers must implement technical and organizational measures, like pseudonymisation, to adhere to data protection rules, ensuring only necessary personal data are processed. This includes managing the data's collection, processing, storage, and access. An approved certification under Article 42 can evidence compliance with these obligations. [↑](#footnote-ref-7)
8. These certification mechanisms must be approved based on Article 42. An interpretation of this Article has been adopted by the European Data Protection Board (see Article 70 of the GDPR). [↑](#footnote-ref-8)
9. European Parliament and the Council, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281, 23.11.1995. [↑](#footnote-ref-9)
10. Remarks of Commissioner Edith Ramirez, Privacy by Design Conference, Hong Kong, June 13, 2012: https://www.ftc.gov/sites/default/files/documents/public\_statements/privacy-design-and-new-privacyframework-u.s.federal-trade-commission/120613privacydesign.pdf. The Fair Information Practice Principles (FIPPs), were adopted by US government for federal agencies when processing PII. They could be basically summarised in: transparency, use limitation, access and correction, data quality, and security. Many consider the FIPPs as the original building blocks for worldwide privacy laws and charters, Companies can implement privacy-by-default systems, using techniques like data minimization and encryption, to easily maintain privacy and reduce data misuse risk. [↑](#footnote-ref-10)
11. See: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.h tm. [↑](#footnote-ref-11)
12. PRIPARE Handbook - Privacy and Security by Design Methodology: <http://pripareproject.eu/wpcontent/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf>. [↑](#footnote-ref-12)
13. Datatilsynet, “Software development with Data Protection by Design and by Default”: https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/. [↑](#footnote-ref-13)
14. EDPS “Guidelines on the protection of personal data in IT governance and IT management of EU institutions”, March 2018: <https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf> [↑](#footnote-ref-14)
15. See a list (non-exhaustive) of privacy related standardisation initiatives in IPEN wiki: <https://ipen.trialog.com/wiki/Wiki_for_Privacy_Standards#Privacy_Standards>. [↑](#footnote-ref-15)
16. See: https://tools.ietf.org/html/rfc6973. [↑](#footnote-ref-16)
17. These certification mechanisms must be approved based on Article 42. An interpretation of this Article has been adopted by the European Data Protection Board (see Article 70 of the GDPR). [↑](#footnote-ref-17)
18. European Commission (2015) M/530 Commission Implementing Decision C(2015) 102 final of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 27 | P a g e 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy: http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548. [↑](#footnote-ref-18)
19. See: <https://ec.europa.eu/growth/single-market/european-standards/key-players_en>. [↑](#footnote-ref-19)
20. Presentation at CEN/CENELEC Cybersecurity Conference, 12 March 2018, A. Guarino, K. Rannenberg: ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity\_ENISA\_CEN\_CL\_ETSI\_Presentations/GUARIN O\_RANNENBERG\_CEN-CLC\_JTC8.pdf. [↑](#footnote-ref-20)
21. See: ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity\_ENISA\_CEN\_CL\_ETSI\_Presentations/WalterFUMY\_Chair\_CEN-CLC\_JTC13.pdf. [↑](#footnote-ref-21)
22. See also Kamara, I., "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'", in European Journal of Law and Technology, Vol 8, No 1, 2017: <http://ejlt.org/article/view/545/723#_edn20>. [↑](#footnote-ref-22)
23. Based on an original definition by Mary Shaw, expanded in 1995 by Grady Booch, Kurt Bittner, Philippe Kruchten and Rich Reitman [↑](#footnote-ref-23)
24. Originally formulated in the late 1970s by Trygve Reenskaug at Xerox PARC, as part of the Smalltalk system [↑](#footnote-ref-24)
25. <https://privacypatterns.org/> [↑](#footnote-ref-25)
26. See http://best-practice-software-engineering.ifs.tuwien.ac.at/patterns.html, and The Open Group Architecture Framework (TOGAF) http://pubs.opengroup.org/architecture/togaf8-doc/arch/chap28.html [↑](#footnote-ref-26)
27. See <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design> [↑](#footnote-ref-27)
28. http://net.educause.edu/ir/library/pdf/eqm0442.pdf 37 [↑](#footnote-ref-28)
29. See note 28 [↑](#footnote-ref-29)
30. *ibid* [↑](#footnote-ref-30)