KYC/AML GUIDE

Privacy Policy

KYC

Table Of Content.

Executive Summary

The idea of privacy by design was developed to counter the systemic implications of large-scale networked data systems and the systemic growth of information and communication technologies. The original ideas behind "Privacy by Design" were put forth in the 1970s, and the RL 95/46/EC data protection directive was created in the 1990s. The fundamental idea behind data protection legislative frameworks is privacy-by-design. An approach to data privacy places an emphasis on proactively incorporating privacy into the design requirements of information technology systems and processes. . The fundamental tenets of Privacy by Design call for user control, data reduction, security, and privacy as the default setting delivering clear privacy notifications and transparent data practices.

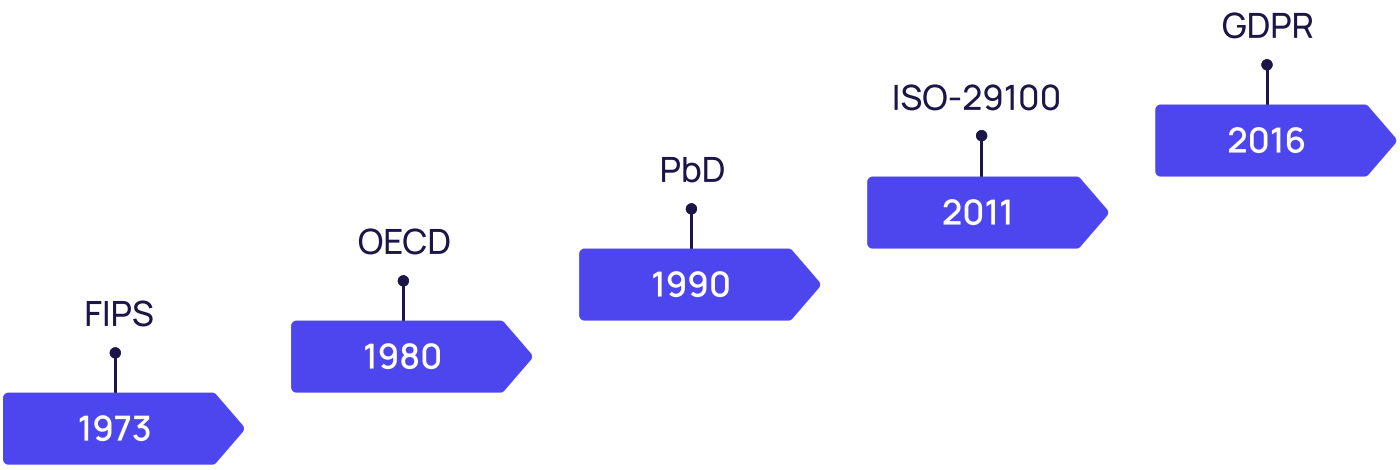
Introduction

Digital identification systems linked to civil registration can make a big difference in several development sectors, including financial inclusion, extending access to services and social safety nets, and effective humanitarian response. Personal data collection, analysis, and management exposes one set of vulnerabilities and creates substantial privacy challenges. At the same time, digital identity systems can create opportunities by making it easier to access and share personal data while preserving privacy. Other risks include:

1. Improper or erroneous data collecting that can result in identity theft or unfair treatment
2. Without the user's consent, using data gathered for one purpose for another;
3. Data transfers that are not permitted or are done in the wrong way between governments, government agencies, and even third non-governmental organizations

Privacy Policy and its Aspects

Initially, the approach to privacy issues was centered on the deployment of conventional security measures as well as policy, procedural, and legal considerations. The phrase "privacy-enhancing technologies" (PET) refers to all the IT tools that can be utilized to safeguard personal information. A discernible trend is the implementation and advancement of "Privacy by Design" and PET. The ISO 29100 Privacy Framework Principles, which were based on previously developed principles created by a number of governments and international organisations, were the first attempt at a more universal set of standards. The General Data Protection Regulation (GDPR) (EU) 2016/679, which was passed in 2016, then came as the first set of regulations with "teeth," namely Article 5.



Privacy by Design

Digital identification systems linked to civil registration can make a big difference in several development sectors, including financial inclusion, extending access to services and social safety nets, and effective humanitarian response. Personal data collection, analysis, and management exposes one set of vulnerabilities and creates substantial privacy challenges. At the same time, digital identity systems can create opportunities by making it easier to access and share personal data while preserving privacy. Other risks include:

Privacy by Default

The privacy-by-default strategy compels enterprises to implement the most stringent privacy-related settings accessible by default. To ensure compliance with privacy-by-default, organizations should also follow the data protection principle of 'purpose limitation,' which states that an organization should only collect and process data that is relevant, adequate, and limited to specified, explicit, and legitimate purposes, and should not engage in any processing activities that are incompatible with the aforementioned purposes.

Privacy Policy Aspects

Although the General Data Protection Regulation requires Privacy by Design, as well as other compliance requirements, it provides a massive answer to practically every issue that the new law introduces. Privacy by Design was practiced by a few people prior to the GDPR's implementation. It is a methodology that dates back to the 1990s but has only lately come to light.

The GDPR is not the only rule that requires privacy by design, but it is the most important in this context. Ann Cavoukian, a former Canadian Information and Privacy Commissioner, was responsible for shaping the principles which form the basis of this practice.

1. Fair Information Practice Principles
2. International Organization for Standardization
3. Information Systems Audit and Control Association
4. Organization for the Advancement of Structured Information Standards
5. National Institute for Standards & Technology.
6. United States Government

Privacy Policy Regulations

The goals of Privacy by Design are preserving privacy and establishing personal control over one's information, as well as gaining a lasting competitive advantage for enterprises. Foundations for implementing the seven Foundational Principles listed below can be met by implementing these principles in an organization's IT and physical infrastructure.

1.

Proactive not Reactive; Preventative not Remedial

Proactive rather than reactive measures characterize the Privacy by Design approach. It anticipates and prevents invasions of privacy before they occur. PbD does not wait for privacy hazards to manifest, nor does it provide remedies for resolving privacy violations after they have occurred; rather, it seeks to prevent them from arising. In short, Privacy by Design occurs before, not after, the fact.

2.

Privacy as the Default Setting

Privacy by Design aims to provide the highest level of privacy by guaranteeing that personal data is automatically secured in any given IT system or business activity. Individuals do not need to take any action to safeguard their privacy because it is integrated into the system by default. Even if an individual does nothing, their privacy is still protected.

3.

Privacy Embedded into Design

Privacy by Design is incorporated into the design and architecture of IT systems and business activities. It is not an afterthought. As a result, privacy has become an integral component of the basic functionality provided. Privacy is essential to the system without compromising functionality.

4.

Full Functionality Positive-Sum, not Zero-Sum

Privacy by Design strives to accommodate all legitimate interests and purposes in a positive-sum "win-win" manner, rather than an outmoded, zero-sum approach that involves unnecessary trade-offs. Privacy by Design overcomes erroneous dichotomies like privacy vs. security by proving that both can be had.

5.

End-to-End Security — Full Lifecycle Protection

Strong security measures are crucial to privacy, from start to finish. This ensures that all data is safely maintained and then securely erased in a timely manner at the end of the process. Privacy by Design ensures end-to-end information lifecycle management. It's designed to extend safely across the full lifecycle of the data involved.

6.

Visibility and Transparency — Keep it Open

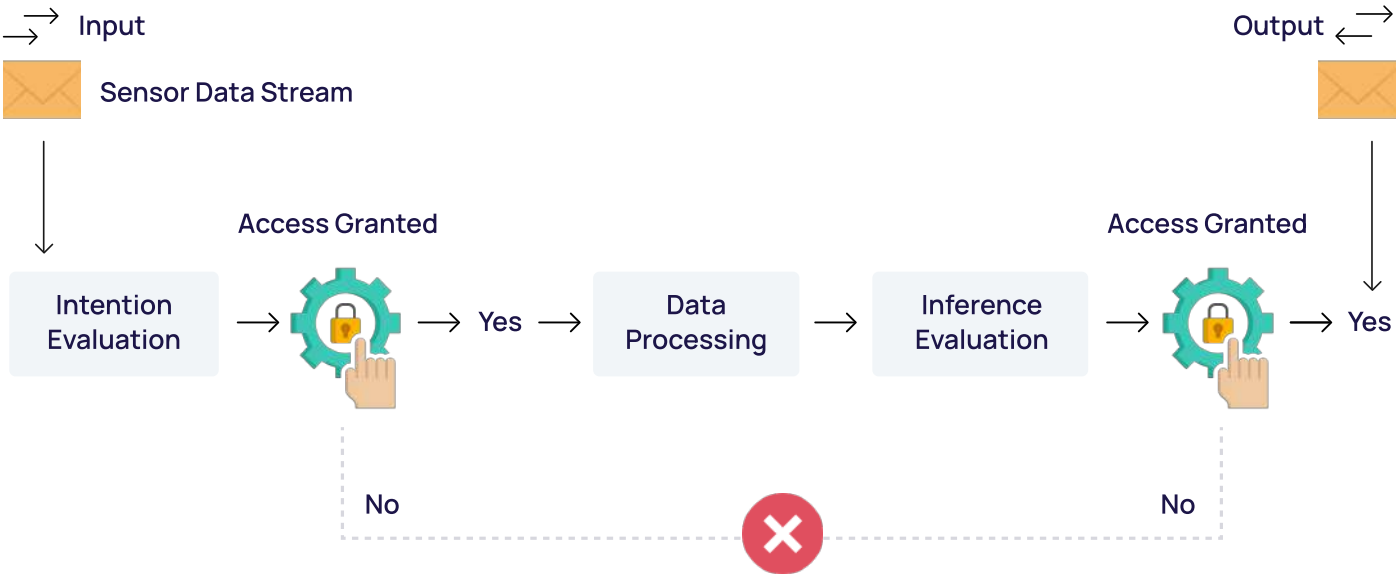
Privacy by Design strives to reassure all stakeholders that, regardless of the business practise or technology involved, it is, in fact, working in accordance with the stated promises and objectives, subject to independent verification. Users and suppliers alike can see and understand its component pieces and operations. Remember to believe but verify.

7.

Respect for User Privacy — Keep it User-Centric

Privacy by Design demands architects and operators to emphasize the individual's interests by including features such as strong privacy defaults, proper notification, and empowering user-friendly options. Keep the user in mind.

Privacy Policy by Design Mechanism



Privacy Policy by Design Implementation

Article 25 is infamously obscure, but thoroughness is still essential for protecting against threats as well as GDPR fines. Privacy by Design must take place:

- During the design phase
- Throughout its lifespan
- From beginning to end, engagement
- Following the engagement
- Following the demise of your website/app

One method for breaking down Privacy by Design implementation is to divide it into three parts: systems, processes, and risk management.

Checklist of System Requirements

To implement privacy into your systems, start with the following (at a minimum):

- Having an organizational commitment to data protection standards that is documented (including into corporate culture, business practices, and business services)
- If applicable, appointing a data protection officer (DPO) or utilizing a data protection advisor (non-GDPR cases)
- Creating a Data Security Framework (including encryption and anonymization)
- Developing and documenting a processing activity record-keeping system
- Choosing a Risk Management System (including compliance management)
- Updating privacy training for employees who work with personal information (both for customers and other employees)
- Using self-assessment to audit and monitor the application of the above-mentioned documented systems
- Putting in place security measures to prevent mishaps and breaches

Checklist of Processes

The processes area is where the majority of Privacy by Design and GDPR compliance work takes place, but it can't happen without first starting with the systems. The list includes:

- Assigning responsibility for gatekeeping (IT, legal, procurement, etc.)
- Identifying and mitigating privacy threats throughout your processes
- Data processing documentation (using the record keeping system designed in Systems Checklist)
- Before collecting data for use or storage, perform DPIAs, risk and compliance evaluations.
- Including privacy measures, such as a Privacy Center, that allow data subjects to access their personal information on their own terms.
- Implementing the measures from the preceding Systems checklist

Checklist for Risk Management

Risk management begins with the systems and continues through the workflow.

- Describe the processing's purpose
- Determine safeguards that prevent data from being processed for reasons other than those listed above.
- Monitor data reduction efforts and put necessary controls in place
- Determine the methods utilized to ensure data accuracy.
- Name and document the individuals and groups who have access to the data.
- Outline data access controls.
- Create and review Data Processing Agreements (DPAs) with each third-party processor.
- Keep an eye on the security practices that have been put in place.
- Determine the source of the information and notify data subjects about data processing.
- Outline the procedure to be followed in the event of a security or data breach
- Implement the measures from the aforementioned Systems and Processes checklists.

Challenges in Implementing Privacy by Design

With the increased usage (and abuse) of personal data, data privacy should be at the top of company's risk management agenda. It is an unavoidable challenge that must not be avoided.

GDPR and other standards, such as CCPA and HIPAA, carry significant fines for violations. Furthermore, reputational harm can pose an existential threat to your company and a career-limiting blemish on an IT manager's resumé

1. Concept

Privacy is a nebulous idea that is difficult to safeguard. We must decide what it is that we wish to safeguard. Furthermore, philosophically and methodologically, privacy and security are frequently confused. To know what to handle with what means, we must first separate security from privacy.

2. Methodology

There is no accepted approach that supports the systematic engineering of privacy into systems. The life cycle of a system rarely allows for privacy considerations.

3. Devices are proliferating

When you consider the Internet of Things (IOT), bring-your-own-device IT regulations, and the proliferation of internet-connected tablets, phones, and watches, data privacy becomes more difficult to manage. When more gadgets are introduced into the office, there is more data to handle.

4. Rising maintenance expenditures

Maintaining system security and preventing data privacy issues at the company level can be costly. However, the costs of a data breach are so high that you must bite the bullet and invest correctly.

5. A poor data culture

A miser's cache of data is becoming more of a liability than an asset. The days of storing as much data as technologically possible are long gone. Maintaining data for the sake of keeping data today broadens the attack surface for data theft and increases the danger of violating several data privacy regulations. Forward-thinking IT teams must weigh the benefits of collecting, storing, and analysing massive amounts of data against the pressing needs for privacy, security, and compliance.

6. Data on an ever-increasing scale

Businesses are increasingly swimming (or drowning) in data as cloud storage and computation costs fall. Indeed, as the volume of global data expands (today measured in tens of zettabytes), the difficulty of handling these oceans of data becomes enormous.

7. A lengthy set of regulations and documents

With so many requirements to obey, it can be difficult to keep track of the amount of data protection required for each dataset. You can reduce the complexity of multiple regulations by developing processes, modelling data, and automating as much as possible.

Conclusion

To resist the systemic consequences of large-scale networked data systems and the systemic proliferation of information and communication technologies, the concept of privacy by design was developed. Privacy-by-design is the essential concept underlying data protection regulatory frameworks. Privacy-by-design is an effective strategy for protecting personal information and data from misuse, unauthorized access, or disclosure. Privacy-by-design seeks to address the issue of data privacy and security by embedding data protection safeguards into the design and architecture of systems.