WHITE PAPER

How organisations can practise "Privacy By Design"

Coforge

Overview

Privacy by Design is based upon the fundamentals of implementing proactive measures rather than reactive. There is no remedial approach to an infringement apart from putting on some guardrails, which would cater to this aspect. However, Privacy by Design has its own challenges. Ambiguity of how it can be achieved is definitely one of them.

An organisation could attempt to document its commitment, appoint DPO(Data Protection Officer) who ensures a framework is in place, but these are not enough. One needs multiple systems to synergise such as risk management, record keeping, audits and trainings.

This article describes points of view on some of the privacy controls to achieve the same.

Definition

The term "Privacy by Design" means "approaching data protection through technology design" especially in data processing procedures. This is not a remedial specification or ways to resolve privacy infractions once they have occurred, but a proactive technical and organisational measure designed to implement data-protection principles. E.g. The European GDPR regulation incorporates privacy by design.

This article shows how an organisation can implement 'privacy by design'.

It is important to note that since this is a wholesome approach, it spans technologies, application ecosystems, organisational boundaries with varied practices, design methodologies or physical/network boundaries of information ecosystems.

Privacy by design is based on seven "foundational principles"

1. Proactive not reactive; preventive not remedial

Fair practices are defined as:

- To be clear, consistent, explicit and be vocal about 'privacy'.
  - This is achievable through publishing it over various channels viz. intranet, notice board, seminars, webinars etc.
- Include the user as well as all stakeholders in a commitment.
  - This is achievable through a signed clause which comes as a part of organisational value to uphold.
- Since, perfection never comes in a day and is not everlasting, one needs to learn continuously from its context.
  - This is achievable through regular audit and feedback mechanisms to outdate and rectify or establish new practices if need be.

2. Privacy as the default setting

Fair practices are defined as:

- **Purpose Specification**
  - The purpose(s) must be specific and pertinent to the stated needs, and the data subjects must be informed of them at the time of, or prior to, any data collection, retention, or usage.
- **Collection Limitation**
  - Data must only be collected in a fair, legal, and purpose-specific manner.
- **Data Minimisation**
  - The least amount of data should be collected, and technologies should have non-identifiable, non-observable users as a default.
- **Use, Retention, and Disclosure**
  - Use, retention, and disclosure of data must be limited and only for what has been consented to, with exceptions by law. Information should only be retained for the stated amount time needed and then securely erased.

These are achievable through tagging, access management based on tags, audit reporting, data life cycle based on tags viz.

A data-set collected for medical purpose goes through consent and once collated should be

- tagged as 'medical' under the category 'Restricted', encrypted with storage
- isolated and accessed only by a specific role,
- reported every time its accessed, shared or printed and
- destroyed on expiry date set.

3. Privacy embedded into design

Fair practices are defined as:

- Following accepted standards and frameworks, open to external audits & applied with equal rigour, at every step in the design and operation.
- Detailed privacy impact and risk assessments done and published along with its mitigation.

Organisation wide governance bodies can ensure that there is a standardisation by defining templates which cover all grounds. It also ensures that these act as checkpoints to the usual flow of programmes/projects/engagements.

The report is made available for remediation and is shared with all stakeholders for publicising the practice, growing awareness. A public statement of compliance also goes a long way in boosting the confidence of the stakeholders in the process.

4. Full functionality – positive-sum, not zero-sum

Fair practices are defined as:

- makes this as an added feature which is not inclusive to the core product feature.
- This is more like a non-intrusive, non-functional feature added to the product.

Given the potential difficulty of clearing up the ambiguity, it is essential to explicitly define objectives. These could be identification, processing, masking, tagging etc. Scopes are marked for functionalities/features on the data which is under the purview of privacy. This is agreed on and usage of specific metrics viz. access, modification etc. are captured and reported. An important consideration is to reject requested trade-offs and rather favour coming up with a solution which brings out enablement.

5. End-to-end security – full lifecycle protection

Fair practices are defined as:

- Entities must assume responsibility for the security of personal information
- The confidentiality, integrity, and availability of personal data must be ensured by applied security standards throughout the life of the data.

This is achievable using strong security measures to privacy from start to finish. Privacy by Design extends safely across the full lifecycle of the data involved since it is built into the system before the first element of information is acquired. This guarantees that all data are safely stored and promptly erased after the operation is complete.

6. Visibility and transparency – keep it open

Fair practices are defined as:

- **Accountability:** There is a responsibility to take reasonable precautions to protect personal information when it is collected. It is required to provide comparable privacy protection through contractual or other measures when disclosing personal information to other parties.
- **Openness:** Transparency and openness are essential for accountability. Individuals must have easy access to information regarding the policies and procedures governing the management of personal information.
- **Compliance:** It is important to develop complaint and redress channels and teach people about them, including how to proceed to the next level of appeal. It is important to take the necessary measures to monitor, assess, and confirm adherence to privacy policies and procedures.

These are some of the governance practice and organisation wide practices and could be tailored to each verticals or business units. The culture talks about being transparent in definition and propagating the process and accountability. E.g. Awareness among the people handling data on accountability and escalation matrix ensures that issues are resolved proactively.

7. Respect for user privacy – keep it user-centric

Fair practices are defined as:

- **Consent** – owner of the data must allow collection, use or disclosure of personal information, except where otherwise permitted by law.
  - This also makes the user a stakeholder. The choice govern the data handling piece. It is important to consider a feature in the system to withdrawn consent at a later date. All the choices are also captured as a feedback to the business process.
- **Accuracy** – this is correctness, completeness, and up-to-date as is necessary.
  - An incorrect data is a more dangerous entity than not having data in the first place.
  - Also an outdated data is incorrect data.
  - Data must be shown with last possible updated timestamp and source if possible.
  - The system should design to raise flags to correct the data and mark it unusable for the duration.
- **Access** – Just like an owner, one has access and can restrict its specific usage or distribution. One can also challenge correctness or staleness and amend the same.
  - This helps to achieve accuracy and engage owner to make choices necessary for privacy adherence.
- **Compliance** – establishing a complaint and redressal mechanisms, an FAQ, a customer service line and an escalation channel for redressal.
  - Owner of data may have limited information on the process and his rights, these should be transparent and explained in a simpler language to the owner.

Summary

The list above is just one example of the various ways "privacy by design" can be put into practice. Depending on the type of organisation, the type of business, the area, or any other pertinent circumstance, we as an organisation tailor the solution. We bring in checklists, templates and customise them as needed.

- Less intuitive UI for end users
- Lack of configurability of the product features, parameters elongate the development and deployment time of new products
- Manual task assignment/underwriting referrals is time consuming

About Coforge

Coforge is a global digital services and solutions provider, that enables its clients to transform at the intersect of domain expertise and emerging technologies to achieve real-world business impact. A focus on very select industries, a detailed understanding of the underlying processes of those industries and partnerships with leading platforms provides us a distinct perspective. Coforge leads with its product engineering approach and leverages Cloud, Data, Integration and Automation technologies to transform client businesses into intelligent, high growth enterprises. Coforge's proprietary platforms power critical business processes across its core verticals. The firm has a presence in 21 countries with 25 delivery centers across nine countries.

Learn more: www.coforge.com

For more information, contact information@coforge.com

Coforge