



Privacy by Design

Vital steps towards a clean audit

Your guide to the solutionist approach tread by
Privacy by Design

Overview

With the adoption of 'Data Protection by Design and Default' notion under Article 25 of the General Data Protection Regulation, implementation of the protection measures at the design level became the best practice for all the organizations. Consulting firms will always recommend to swallow the protection pill at the initial steps but they often miss out on effective

measures to embed such a crucial step in their practice to resonate across organizational functions. This whitepaper aims to hold hands with organizations in the process of implementation of Privacy by Design (PbD) and approach towards an unqualified audit. It discusses various issues faced by organization and tries to provide solutions to this ever-growing enigma.

Target Audience

This whitepaper aims to be useful for the senior and mid senior IT management, program managers and compliance leaders to understand what is privacy by design and how it can be used to tweak the IT practices to make the organization proactively compliant to data protection regulations.

It also aims at helping a wide array of secondary audiences like learners and scholars who want to understand how to implement the data protection measure of Privacy by Design at the organizational level. This whitepaper contains a wholesome strategy for implementation.



Introduction

The European Data Privacy Law, GDPR came into effect on May 25, 2018, it was dawn of global privacy laws that changed the face of the internet forever. It classified Personal Data as information capable of identifying an individual. Personal Data in its own self cannot essentially identify a person but when put together like a jigsaw puzzle, speaks otherwise. Personal

Data is a highly valued trillion-dollar industry & the fine for data breach is to the tunes of 20 million euros or 4% of the Annual Global Turnover. Though it is a European law but its presence bleeds through businesses worldwide. In turn, almost every business in the world has to comply with the law if their data processing is even remotely associated with the European region.

Problem Statement

Businesses & organizations have nothing to lose from ensuring privacy and security from the onset of the data lifecycle. The data collection exercise to its completion is mutually beneficial to them if they are able to maintain compliance, avoid litigation, and gain the confidence of their customers. But the main challenge that the organizations are facing is with the operationalization setup. The compliance obligations for the Controllers multiplied manifold with the introduction of the new law.

Structure

This whitepaper would be covering the following aspects:

- Privacy by Design and what it holds?
- Seven Principles of Privacy by Design under GDPR
- Technical & Organizational Measures under Recital 78
- Privacy by Design in Product Development
- Strategy to Implement Privacy by Design: The Tsaro Way
- Implementation challenges faced by organizations
- Advantages of Privacy by Design for organizations
- Conclusion: Privacy by Design - A silver bullet yet to be shot



PRIVACY BY DESIGN & WHAT IT HOLDS?

Although, the General Data Protection Regulation mandates Privacy by Design just like its other compliance measures but it poses a gigantic solution to almost every issue that the new law brings in. Until the enforcement of the GDPR, Privacy by Design was practiced by a few. It is a methodology that dates back to the 1990s but gained limelight recently.

In principle, it pushes organizations to proactively make privacy a priority. It is fair weather to the data privacy regulatory climate.

Privacy by design is essential refers to the practice of building new technologies, systems & business processes with the aim to achieve highest level of data protection.

Ann Cavoukian, a former Canadian Information and Privacy Commissioner was responsible for molding the foundational principles which forms the basis of this practice. The foundational principles ensure that privacy is embedded into every aspect of the organization's data processing activity.

Privacy by Design (PbD) requirement comes from numerous regulations other than the GDPR. In this context, the most important are:

1 Fair Information Practice Principles (FIPPs)

2 Organization for the Advancement of Structured Information Standards (OASIS)

3 International Organization for Standardization (ISO)

4 National Institute for Standards & Technology (NIST)

5 Information Systems Audit and Control Association (ISACA)

6 United States Government (HIPAA & FTC Act)



SEVEN PRINCIPLES OF PRIVACY BY DESIGN UNDER GDPR

1

Proactive not Reactive; Preventative not Remedial

This approach anticipates and prevents data privacy breach even before it happens. It aims to have more compliant products and services that best provide the privacy of personal data of the users. Work must be done during development phase and not at the completion end.

Privacy as the Default

2

This principle ensures that personal data are automatically protected in process, product & features by default and no extra effort is put into place for it. Privacy by default should be maintained foremost. If high privacy & security measures are present from the start then configurational changes can be made as per the user's requirements.

3

Privacy Embedded into Design

By embedding privacy into the design, rather than trying to add it on later, the system will run better. No process should commence if the best privacy & security shield is absent.

Full Functionality — Positive-Sum, not Zero-Sum

4

Trade-offs shouldn't be made to accommodate either privacy or functionality. It's easy to fall victim to false dichotomies. Such compromises should be kept aside. A usable as well as a secure product ticks off all the checkboxes.



5

End-to-End Security — Lifecycle Protection

Privacy by Design considers security from start to finish, in the entire data lifecycle. Data flows and it has no boundaries. Measures should be kept in place to secure data in all kind of states- collection, processing or at rest. The notion that the data is only living and not static should be done away with & appropriate steps should be taken to secure it.

By allowing users and other involved parties to see how information moves through your system, the system improves. This needs to be part of the design and build plan so that users have a comprehensive understanding of the technical and organizational measures implemented throughout to protect their personal information.

Granular visibility and Transparency

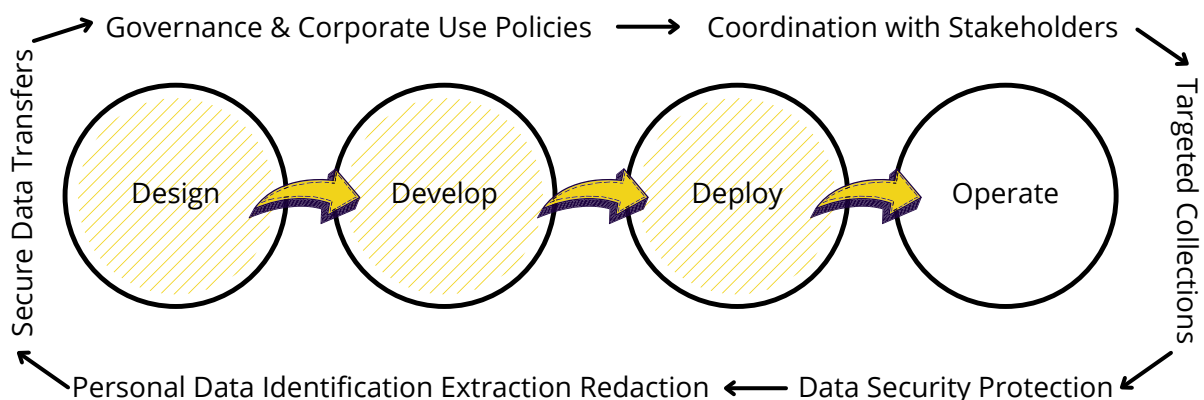
6

7

Respect for User Privacy

Organizations should make user privacy their number one concern. Prioritizing user privacy should resonate from top to the bottom of an organizational structure. Helps construct a healthy relationship with users, clients & customers. The design & built of the product should necessarily have user privacy as a vital string.

Privacy by Design: Intersection between Product Development & Legal Obligations



○ Product Development Stage



GDPR RECITAL 78

- Technical & Organizational Measures at the initial stages
- Adoption of policies & compliance measure by the Controller
- Minimization of processing of personal data
- Pseudonymization of personal data
- Transparency with functions of processing
- Development & Design of Product with data protection obligations
- Principles of data protection by design and by default with public tenders

PRIVACY BY DESIGN IN PRODUCT DEVELOPMENT

Privacy by Design essentially walks through the product design approach to management of individual control over personal data flow, ultimately putting it together into systems by default. To the bare eye this seems to be an 'engineering issue', while we strongly believe & suggest it to be strategy driven issue that needs to be implemented at the grass-root level even before initiating the product development.

It is a pathway of potholes for organizations both big and small, who have been into product development to implement the privacy & security principles in their product. Lots of information & knowledge on the part of the software developers is becoming a huge problem. When the development process is complete and data protection related issues pop-up, the developing team finds itself helpless.

The requirements for data protection & security have been mentioned in the data protection regulations as we have already discussed above. It is on the developers to glance through the law as per their product & its requirement. They should merge their aspirations from the end product & parts of the legislation relevant to their organization or enterprise.

Privacy by design is not hard to achieve if the skeleton of the product is drawn over good strategy & planning with effective controls shadowing.

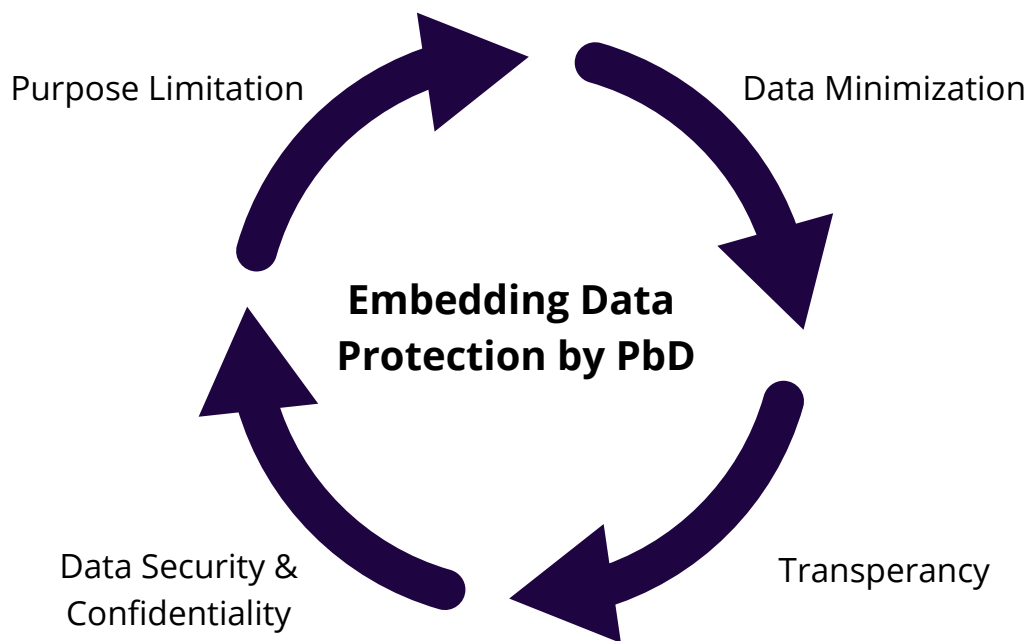


STRATEGY TO IMPLEMENT PRIVACY BY DESIGN: THE TSAARO WAY

1 Adhere to 7 Foundational Principles

At the initial stage of product development, the development team should focus on the long term strategy to stick to the 7 foundational principles in any circumstance. Half the job gets done when doing so. The stakeholders should come together to analyze the privacy requirements relevant to their product and the organization.

The foundational principles should then be integrated into the data management lifecycle to get rid of any privacy and security risks at any level whatsoever. From an early design stage to installation and operation, properly defined set of principles should be followed.



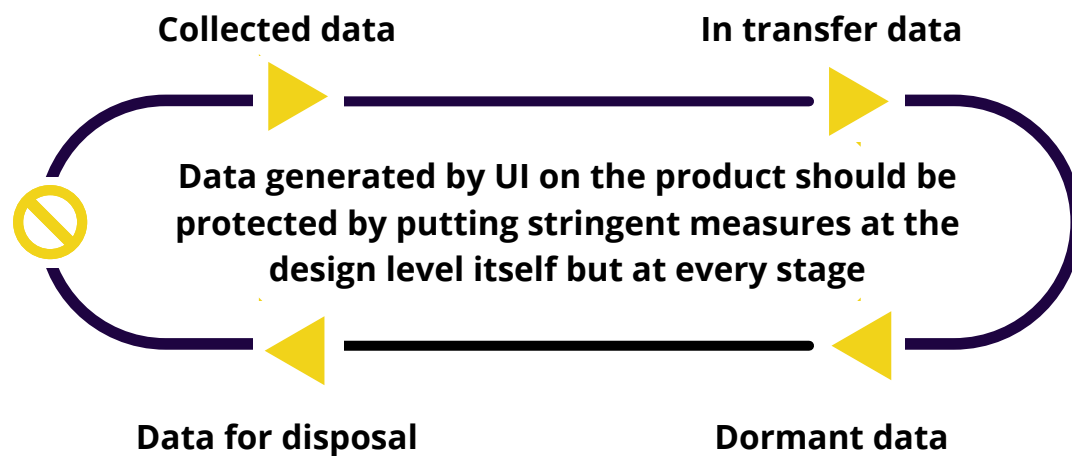
2 Data Protection across stages

For organizations, the job isn't done as soon as the product is out of development stage. They need to make sure the data is protected and secured at each stage of its lifecycle. This is a bit tricky and challenging. All the stakeholders need to come together and work in the process.

With Privacy by design, the developer can make this a possibility at the very nascent stage of development. Application of core privacy principles to the design of the product will make this happen.



STRATEGY TO IMPLEMENT PRIVACY BY DESIGN: THE TSAARO WAY



3 Monitor issues on the product

Any product or software might start to run for the purpose it wasn't made for due certain anomalies like virus threats. During these unforeseen circumstances, purpose limitation principle takes a toll. Purpose Limitation is one of the most important foundational principles of data protection. The purpose mentioned in the privacy notice & the real-time purpose of collection should not vary in any situation or circumstance.

To avoid this unwarranted situation due to issues related to the product, periodic monitoring and review should be put into place.

Checks and balances should be present to avoid the penalties for discrepancy in the purpose of collection. There might be situations where additional data sink occurs than actually asked for.

The developer should remedy the unauthorized data ingestion by regular updates on the product.

4 Actual control at the user-end

During the development stage of a product it should keep in mind that the actual control of the product & its functions lies with the user. This can be found to be true as the product works on user consent only. Every product necessarily has the consent checkbox for users to agree to the collection and processing of the data. In all the usage

of the product is decided by the user itself.

The developers should design the product in a manner that consent requirement should be fulfilled at the very initiation of the usage of the product.



STRATEGY TO IMPLEMENT PRIVACY BY DESIGN: THE TSAARO WAY

The UI should be made in such a manner that the consent requirement is unmissable by the user. It should be user-friendly and easy to understand by any person.

It is also extremely necessary to keep the privacy statement updated on the product. It should be in consonance with the privacy policy of the organization.

5 Identification of Data Leeches

The developers should monitor the presence of data leeches on the product with restrict access to data unless there is appropriate authorization.

It is known that encryption practices can help avoid this situation but one should not turn a blind eye towards it.

Periodic monitoring & review of the analytics that have been attached to the product should be strictly done. Mitigation of potential risks is also necessary.

DATA LIFECYCLE



STRATEGY TO IMPLEMENT PRIVACY BY DESIGN: THE TSAARO WAY

6 Due diligence with third parties

Organizations should be diligent while associating with third parties/ their products & technologies. It should be known that such instances may result in humongous data breach incidents. Periodic updates/ fix patches on the

product should always be available. Preventive measures like these should be developed from time to time and as per product & situation demand.

7 Minimal access across teams

Development & Operations teams work hand in hand to make vision of a product to reality. But should all the teams working on a product have a readily available access to the actual user data?

No matter how many teams have worked on the product from scratch, user data should only be available to the team responsible for processing and in the prescribed anonymized form.

The developers' and the admins' access should be kept away from each other. For bugs fixes and troubleshooting, the developing team should have minimal access to the data to avoid and data breach incidents. Hence anonymization techniques should be applied from the initiation of the product development.



IMPLEMENTATION CHALLENGES FACED BY ORGANIZATIONS

ETHICAL ASPECTS OF DEVELOPMENT

An organization should decide how transparent they would like to be about its data processing. Analysis of what minimal data is required should be passed on to the developer. This decision should not depend on the developer but rather be decided by the organization.

COMMUNICATION WITH USERS

Communication with users is very essential at the initial design stages and throughout the complete development process. But this becomes a problem as the developer has no point of communication with the users and hence overlooked in the design.

KNOWLEDGE ON PRIVACY

A successful systems implementation will happen when everyone involved in the development and implementation phases has knowledge and understanding of privacy. The lack of knowledge poses a problem in most organizations.

LEGACY APPLICATIONS & PRODUCTS

Organizations had been running on non-GDPR compliant apps for years and years and suddenly they have to deal with this new concept. It is a big deal for them to keep up with this obligation and be proficient with its nuances.

INNOVATION VS PROTECTION

Novel ideas are the selling point of any product but it could also be a problem for organizations. It is easy to come up with new ideas but hard to comply with regulations. This is an obstacle for organizations complying with privacy regulations at the application building stage itself.

USABILITY VS UTILITY


Usability is the ease to use privacy features. Utility refers to the functionality available for databases containing personal data with privacy protection. Both need to be considered through the design, implementation and operation. It is challenging for organizations to strike a balance.




ADVANTAGES OF PRIVACY BY DESIGN FOR ORGANIZATIONS



Helps with a **clean audit** as there are minimal or no material findings on non-compliance with key data protection legislations.




Efficient and reduces costs where embedding PbD is technologically challenging, expensive or even impossible at a later stage.




Ascertains compliance at the very initial stage and **minimizes the operational business tasks.**



Privacy compliance helps **balance the interest** of the stakeholders and have better corporate governance.



Incorporates strong security and privacy controls thereby **reducing** the likelihood of a **data breach or security incidents.**



Integrating PbD at the core of the big data analytics value chain will allow organizations to **make the most of big data analytics.**



CONCLUSION

Though Cavoukian's approach to privacy has been criticized as being vague, challenging to enforce its adoption, difficult to apply to certain disciplines, as well as prioritizing corporate interests over consumers' interests and placing insufficient emphasis on minimizing data collection but this in turn has resolved many issues which are yet to be realized.

It has also been pointed out that privacy by design is similar to voluntary compliance schemes in industries impacting the environment, and thus lacks the teeth necessary to be effective, and may differ from company to company.

But requisite heed hasn't been paid to the strict compliance rules that GDPR brings in with Privacy by Design, making it impossible to just be a voluntary measure.

Privacy by Design is a remedy to the Article 35 requirement, Privacy Impact Assessment which is a reactive method of privacy application. Instead, heads should turn to Article 25 GDPR which has found its basis in the preventive approach to privacy compliance. Privacy by Design is not used to its full potential as yet & it must be integrated into each stage and aspect of the design of a new product, as well as in the organizational structure.

BIBLIOGRAPHY

- Privacy by Design - General Data Protection Regulation (GDPR) (gdpr-info.eu)
- Art. 25 GDPR - Data protection by design and by default - GDPR.eu
- Privacy by Design - The 7 Foundational Principles (iapp.org)
- Engineering Privacy by Design Reloaded (iapp.org)
- A. Cavoukian, "Privacy by Design Curriculum 2.0", 2011. Available at <https://www.ipc.on.ca/>
- Privacy By Design Is Important For Every Area Of Your Business (forbes.com)
- Mikael_Viitaniemi-PbD-in-agile (tuni.fi)
- Privacy by Design in Product Development - dotmagazine.com
- Advantages of privacy by design in IoE (slideshare.net)
- How to operationalize privacy by design (iapp.org)
- Best Practices for the Implementation of the Privacy by Design Concept in Smart Devices - Infosec Resources (infosecinstitute.com)
- Privacy by design in big data — ENISA (europa.eu)





WHY TSAARO?

Tsaaro provides privacy and cybersecurity services to help organizations meet regulatory requirements while maintaining a robust security infrastructure.

Our industry-standard privacy services include Privacy compliance, DPO-as-a-service, Vulnerability Assessment & Penetration Testing, Cyber Strategy, DPIA to name a few, delivered by our expert privacy professionals recognized by IAPP.

Akarsh Singh **(CEO & Co-Founder, Tsaaro)**

Akarsh is a fellow in Information Privacy by IAPP, the highest certification in the field of privacy. His expertise lies in Data Privacy and Information Security Compliance.

Krishna Srivastava **(Co-Founder & Head of Cyber Security, Tsaaro)**

Krishna is a xKPMG data security consultant. He has vast experience in Information Security and Data Privacy Compliance.

Akanksha Sachan **(Data Privacy Consultant, Tsaaro)**

Akanksha is a privacy professional with a strong legal background. She is a certified Data Protection Officer.

CONTACT US

You can assess risk with respect to personal data and strengthen your data security by contacting Tsaaro.

Tsaaro Netherlands Office

Regus Schiphol Rijk
Beech Avenue 54-62,
Het Poortgebouw,
Amsterdam, 1119 PW,
Netherlands
P: +31-686053719

Tsaaro India Office

Manyata Embassy Business
Park, Ground Floor, E1 Block,
Beech Building, Outer
RingRoad,
Bangalore- 560045
India
P: +91-0522-3581

Email us

info@tsaaro.com