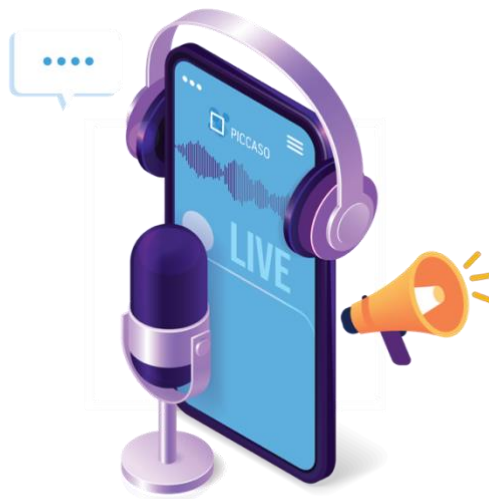




Privacy & Security Insights with **PICCASO**



Privacy by Design and Default

Safeguarding Personal Data in a Global Company

Dr Philipp Raether

Group Chief Privacy Officer



Sponsored by

PrivacyCulture

Privacy by Design and Default

Safeguarding Personal Data in a Global Company

Introduction

In today's digital age, privacy has become a crucial concern for individuals and organisations alike. With the increasing volume of personal data being collected, processed, and shared, and the use of Artificial Intelligence (AI), it is essential to incorporate privacy safeguards into the very foundation of systems, products, services, and projects. This article explores the concept of Privacy by Design and Default and its significance in a global company's operations.

What is now Privacy by Design?

The [UK Information Commissioner](#) defines it as "an approach that ensures you consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle."

When is it done?

It is very important that Privacy by Design comes in as early as possible so that privacy is part of the DNA of any new system, product, service, or project. If it is only considered at the last minute of a corporate approval process, it is doomed to fail. There comes the second aspect into play: that it should also be Privacy by Default. This means that privacy considerations shall be mandatory in these approval process and not only be optional. Therefore, it is key that processes like Privacy Impact Assessment (PIAs) are in integral part of these approval processes. Practically, it is still a challenge for Privacy Professionals to get in involved in system, product, and service developments at early stages.

How is it done?

[GDPR](#) is suggesting that Privacy by Design and Default shall be achieved by implementing technical and organisational measures. These can be the following:

Technical Measures:

- Pseudonymisation: Switch the original data set (for example, email or a name) with an alias or pseudonym. It is a reversible process that de-identifies data but allows the re-identification later if necessary.
- Anonymisation: Same as pseudonymisation but going a step further not to allow a re-identification of the concerned individuals.
- Data Minimisation: Adopt data minimisation techniques to collect and process only the necessary personal data.
- Encryption: Implement robust encryption mechanisms to safeguard data both at rest and in transit, minimising the risk of unauthorised access.
- Access Controls: Establish stringent access controls to limit data access to authorised personnel only.

Organisational Measures:

- Designated DPO: Appoint a Data Protection Officer (DPO) responsible for overseeing privacy compliance and offering expert advice (2nd line function).
- Privacy Champions: Designate privacy champions within the business to promote Privacy by Design and Default (1st line).
- [Privacy Policies](#): Develop and communicate transparent privacy policies, detailing data processing practices and individual rights.
- Privacy Training: Train employees regularly to stay updated on privacy best practices and regulations.

- Privacy Culture: Foster a privacy-aware culture within the organisation by educating employees and stakeholders about the importance of privacy.

Conclusion:

Privacy by Design and Default is not only a legal obligation but also a fundamental ethical responsibility in today's data-driven world. By integrating privacy into the design and development of systems and processes, organisations can establish a solid foundation of trust with their users. Through mandatory project approvals and Privacy Impact Assessments (PIAs) that prioritise privacy, global companies can ensure compliance with regulations such as the GDPR, UK GDPR and many other privacy laws while safeguarding personal data and respecting individual privacy rights. Embracing privacy-centric practices benefits both organisations and individuals, fostering a privacy-conscious environment that prioritises data protection.



Listen now on:



About us:

We are a UK based non-for-profit privacy special interest group, led by seasoned volunteers who are senior leaders in privacy and data protection.

The primary aim of PICCASO is to create a community of professionals that share the value of exchanging 'know how', insights, clarity and explanation on specific privacy and data protection topics designed to distinguish between legal requirements, operational implementation, and strategic objectives, with the aim of greater understanding in how to achieve optimal outcomes based on good practice and thought leadership.

The PICCASO community is drawn from across the UK, Europe, and beyond, and from all industry sectors.

Contact us:

www.piccaso.org
Bouverie House | 154-160 Fleet St | London | EC4A 2DQ
T. +44 (0) 207 112 9360 | hello@PICCASO.org
<https://www.linkedin.com/company/piccaso/>