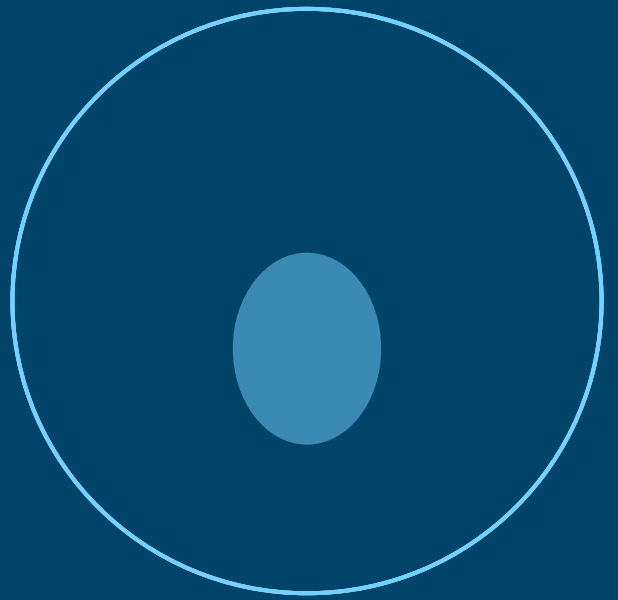
DATA PROTECTION

BY DESIGN &
BY DEFAULT



Presenter:

Omar Gutale

“Where there is data SMOKE, There is business FIRE”

—Thomas Redman

INTRODUCTION

The GDPR provides for two crucial concepts for future project planning:

Data Protection by *Design*.

&

Data Protection by Default

These two principles are enshrined in law under the GDPR (Article 25).

What is the Difference between Data Protection by Design and by Default?

1 - BY DESIGN

Emphasizes embedding measures into the design and architecture of systems, products, and processes from their inception. It advocates for a proactive approach to privacy rather than a reactive one.

2 - BY DEFAULT

Complements the principles of Data Protection by Design by ensuring that privacy features are automatically enabled, with the highest level of privacy protection being the default setting.

1

DATA PROTECTION BY DESIGN

This approach involves collaboration between various stakeholders, including developers, designers, privacy professionals, and legal experts. It requires a thorough *assessment of potential* privacy impacts and the implementation of appropriate measures to address them.

THERE ARE TWO TECHNIQUES THAT CAN BE USED TO IMPLEMENT:

BY DESIGN

1

Pseudonymization

2

Encryption

BENEFITS BY DESIGN

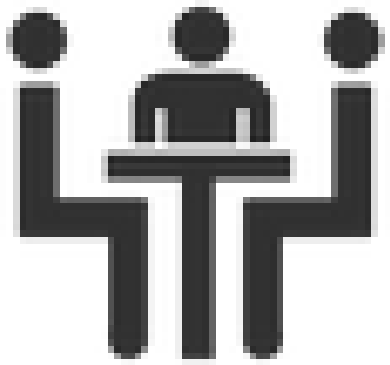
By adopting Data Protection by Design, organizations can achieve THREE benefits.

1

Enhanced Privacy

By proactively addressing privacy concerns, organizations can minimize the risk of data breaches and unauthorized access, thereby enhancing individuals' privacy rights.

2
Compliance Readiness



Integrating privacy into the design phase helps organizations align with regulatory requirements such as the GDPR, ensuring that privacy considerations are not an afterthought but a core element of their operations.

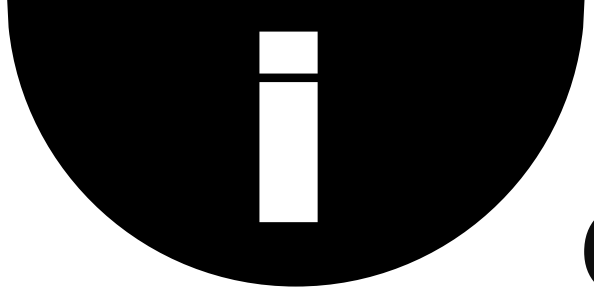
3
Risk Reduction

Identifying and mitigating privacy risks early in the development process can prevent costly data breaches and regulatory penalties, ultimately safeguarding the organization's reputation and financial stability.

2

DATA PROTECTION BY DEFAULT

This principle recognizes that individuals may not always have the knowledge or ability to adjust privacy settings themselves and therefore places the onus on organizations to prioritize privacy by default.



Organizations can achieve the following objectives:

1) IMPOWERING USERS

2) REDUCING PRIVACY RISKS

2) PROMOTING TRANSPARENCY

CONCLUSION

Data Protection by Design and by Default represent fundamental principles for building privacy-conscious systems and fostering a culture of privacy within organizations

THAT IS ALL!

THANK YOU