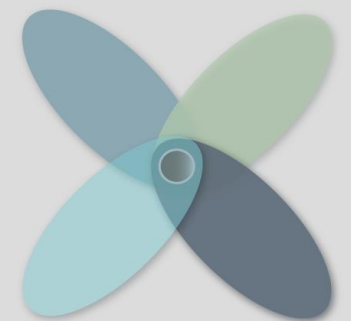


Preparing for GDPR

27th September, Reykjavik



insoft
services



ATIC 360

Introduction

Who I am?

- Solicitor from London
- Worked in digital industry for the last 7 years
- Specialized in Privacy for the last 7 years and did some consulting for many clients from startups to big multinational
- Member of IAPP for 6 years and CIPP/e and CIPP/US certified
- Speaking at conferences, writing blogs and whitepapers, sharing conferences

Who is Insoft?

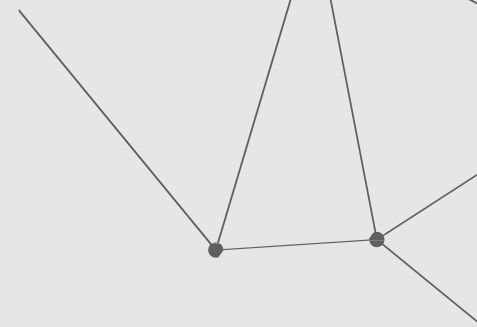
- Independent consultancy and authorized training company in GDPR
- Developed a complete solution "ATIC360" to help customers with GDPR compliance requirements.

Key facts on GDPR

- Privacy laws landscape
- Directive vs Regulation
- Data protection Directive 95/46/ec vs GDPR (different landscape and objectives)
- Reminder of coming into force: 28th May 2018 (8 months to go)
- Some rights of data subjects are strengthened by the GDPR (e.g., the right to object) and some new rights are created (e.g., the right to data portability)
- Increased compliance obligations for controllers

Main changes with GDPR

- Extended jurisdiction
- Consent
- Mandatory breach notification
- Right to access
- Right to be forgotten
- Data portability
- Privacy by design
- Data protection officers (DPO)



Does the GDPR apply to your Company?

Applicability is defined as:

- An organisation established in the EU is subject to the GDPR
- An organisation based outside the EU is subject to the GDPR if it either:

(a) offers goods or services to EU data subjects

or

(b) monitors the behaviour of EU data subjects

An organisation that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law is also subject to the GDPR.

This particularly affects organisations with internet-based business models, offering goods or services to consumers in the EU.

Steps to follow for GDPR compliance (1)




Think global first: what other laws (privacy or not apply to you)?

Does GDPR apply to you and why?

What is your current state?

What data are you gathering? (employee, customers (B2B and B2C), third party)



Steps to follow for GDPR compliance (2)

Look at each of the principle and establish what are your practices? e.g. are your activities with the personal data high, medium or low risk?

Are you planning any new data processing activity or reviewing an existing processing activity? e.g. creating a new HR database.

How important is Privacy for your organization? Who are your Sponsors?

What is your Privacy mission/vision?

What actions you will need to take to reach this desired state?

What does the GDPR requires? (1)

What does the GDPR require?	What to think of to comply?
<p>Is the processing "fair and lawful"?</p> <p>Rec.39; Art.5(1)(a)</p>	<p>"fair" (in particular, organisations must ensure that they give data subjects clear and transparent notice of the ways in which, and purposes for which, their personal data will be processed); and "lawful" (i.e., they comply with the GDPR and all other applicable laws)</p>
<p>Have the Data Protection Principles been satisfied?</p>	<p>Organisations must ensure that their processing activities comply with all of the Data Protection Principles (next slide)</p>
<p>Is there a lawful basis for processing "regular" personal data?</p>	<p>Satisfy at least one lawful basis for the processing of "regular" personal data in respect of each processing activity (e.g., consent; legitimate interests; contractual necessity; compliance with legal obligations; etc.).</p>

What does the GDPR require? (2)

What does the GDPR require?	What to think of to comply?
Is there a lawful basis for processing Sensitive Personal Data? (If applicable.)	Satisfy at least one lawful basis for the processing of Sensitive Personal Data in respect of each processing activity (e.g., explicit consent; compliance with employment law; necessity for the purposes of legal claims; etc.).
Is there a lawful data transfer mechanism in place?	To the extent that an organisation is planning to transfer personal data to a recipient outside the EEA, it must ensure that one of the appropriate vehicle for transfer is in place (e.g., statutory permission; Model Clauses; Binding Corporate Rules; the transfer is made to an Adequate Jurisdiction; etc.)
Is it necessary to consider any national data protection laws in addition to the GDPR?	Organisations should consider whether their processing activities are affected by issues that remain subject to national data protection laws(e.g., employment law; national security; freedom of expression; etc.).
Is it necessary to conduct an Impact Assessment?	If, in the process of answering any of the questions set out above, it is determined that a proposed processing activity is likely to pose material risks to the rights or freedoms of data subjects (e.g., because the planned activity that could be seen as invasive or because there are inherent security risks) the organisation should consider conducting an Impact Assessment

What are the main GDPR principles?

Principle	summary
purpose limitation Rec.50; Art.5(1)(b)	personal data collected for one purpose should not be used for a new, incompatible, purpose.
Data minimisation Rec.39; Art.5(1)(c)	subject to limited exceptions, an organisation should only process the personal data that it actually needs to process in order to achieve its processing purposes.
Accuracy Rec.39; Art.5(1)(d)	controllers are responsible for taking all reasonable steps to ensure that personal data are accurate.
Data retention periods Rec.39; Art.5(1)(e)	personal data should not be retained for longer than necessary in relation to the purposes for which they were collected, or for which they are further processed, is key to ensuring fair processing.
Data security Rec.29, 71, 156; Art.5(1)(f), 24(1), 25(1)-(2), 28, 39, 32	Controllers are responsible for ensuring that personal data are kept secure, both against external threats (e.g., malicious hackers) and internal threats (e.g., poorly trained employees).
Accountability Rec.85; Art.5(2)	seeks to guarantee the enforcement of the Data Protection Principles. This principle goes hand-in-hand with the growing powers of DPAs.



Questions?

Thank You.

