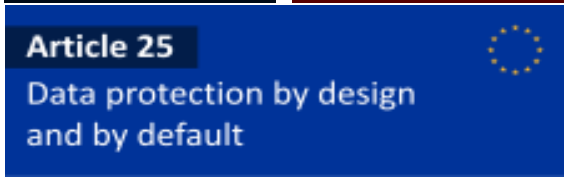
besecure
Managed E-Business Security

GDPR and Privacy by Design: How to gain competitive advantage

Andreas Lalos, Professional Services Director

Data protection by design



"1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures.."

(EU) 2016/679 Article 25

..and by default

Article 25
Data protection by design and by default

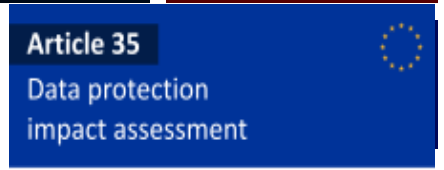
" 2. The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

.. such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. "

(EU) 2016/679 Article 25

besecure
Managed E-Business Security

DPIAs help designing more efficient processes for data processing



The DPIAs assess the:

- necessity and proportionality of the personal data processing
- risks to the rights and freedoms of data subjects
- measures that will address the risks to the rights and freedoms of data subjects and other persons concerned, including:
  - security measures
  - safeguards for cross-border transfers.

Protection by design is State of the Art

- ✓ Regulation does not specify how much security you should apply nor the specific measure you have to take.
- ✓ …but provides a caveat that with due regard to the **state of the art**, to make sure that controllers and processors are able to fulfill their data protection obligations.
- ✓ Proving to supervising authorities that data protection taken in account from beginning of design very likely will save your organization from big fines.

Also by default

- ✓Organization ensures that systems and processes include privacy controls and that systems adopt privacy as a ‘default’ setting, for example by automatically opting data subjects out of processing unless they choose to opt in.

Cost of Taking the Reactive Approach to Privacy Breaches

Class-Action Lawsuits

Damage to One's Brand

Proactive

Reactive

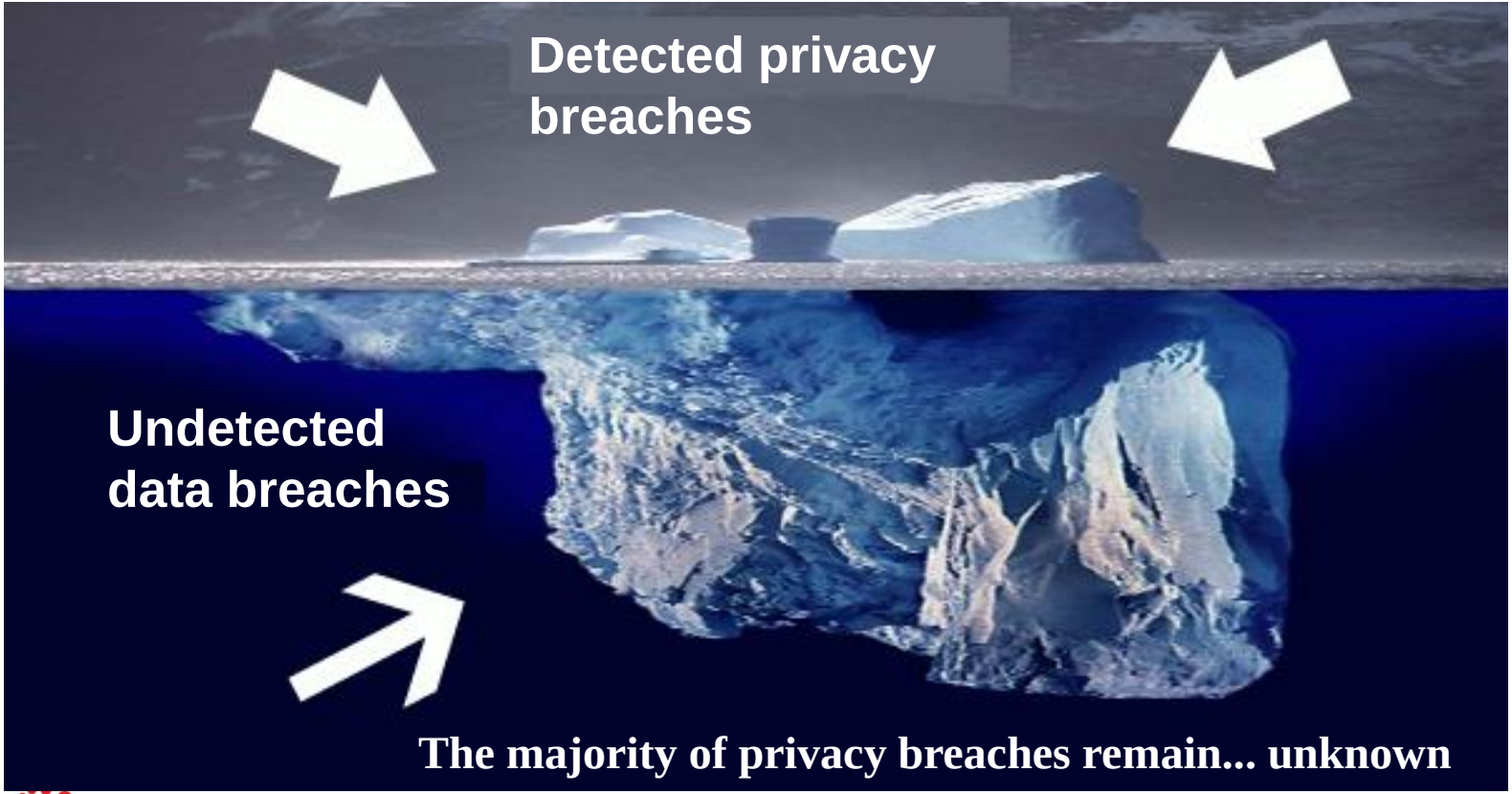
Loss of Consumer Confidence and Trust

Integrating privacy considerations into project and risk management

Privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. For example when:

- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

Why We Need Privacy by Design



The 7 Foundational Principles of privacy by design

1. **Proa**ctive not **Rea**ctive; Preventative not Remedial
2. Privacy as the **Default** Setting
3. Privacy **Embedded** into Design
4. **Full** Functionality - Positive-Sum, not Zero-Sum
5. End-to-End **Security** – **Full** Lifecycle Protection
6. Visibility **and** Transparency – Keep it **Open**
7. Respect for the User – Keep it **User-Centric**

Proactive not Reactive; Preventative not Remedial

- *The Privacy by Design approach is characterized by proactive rather than reactive measures.*
- *Anticipates and prevents privacy invasive events before they happen.*
- *Does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred*
- *Aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.*

Privacy as the Default Setting

We can all be certain of one thing – the default rules!

- Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice.
- If an individual does nothing, their privacy still remains intact.
- No action is required on the part of the individual to protect their privacy – it is built into the system, by default

Privacy Embedded into Design

- Privacy by Design is embedded into the design and architecture of IT systems and business practices.
- It is not bolted on as an add-on, after the fact.
- Privacy becomes an essential component of the core functionality being delivered.
- Privacy is integral to the system, without diminishing functionality.

Full Functionality – Positive-Sum, not Zero-Sum

- Accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made.
- Avoid the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

End-to-End Security – Full Lifecycle Protection

- Embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved
- Strong security measures are essential to privacy, from start to finish.
- Ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion.
- Ensures cradle to grave, secure lifecycle management of information, end-to-end.

Visibility and Transparency – Keep it Open

- Assures all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification.
- Its component parts and operations remain visible and transparent, to users and providers alike.
- Remember, trust but verify !

Respect for User Privacy – Keep it User-Centric

- Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.
- Keep it user-centric.

Benefits of taking a ‘privacy by design’ approach

- ✓Potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- ✓Increased awareness of privacy and data protection across an organization.
- ✓Organizations are more likely to meet their legal obligations and less likely to breach the Data Protection Act.

Benefits of Privacy by Design

Integrating Privacy by Design within organization's integral processes and infrastructure offers many benefits:

- ✓ Gain customers trust: *"If you can trust me more than you can trust a competitor, perhaps you'll do business with me more often"*
- ✓ Integrating security and privacy mitigates customer fears and offers comfort to clients
- ✓ Competitive advantages by developing and maintaining accountable business practices.

besecure
Managed E-Business Security

Thank you

Andreas Lalos,
Professional Services Director
a.lalos@besecuregroup.com