Microsoft

EU legislation and standard frameworks for:
- personal data protection,
- cybersecurity
- and for data in the cloud

Dr. Severin Löffler
Asst. General Counsel, Legal & Corporate Affairs, CEE Region

Microsoft

Personal Data Protection

EU Data Protection draft Regulation

1995 Directive vs Proposed EU Draft regulation : main principles

Directive	Draft Regulation EP	Draft Regulation council
Notice and consent: key principles but no set of operational tools	Accountability + risks' assessment Transparency and fair use. Key issue on profiling and further use of data	Concrete implementation of innovative tools ?

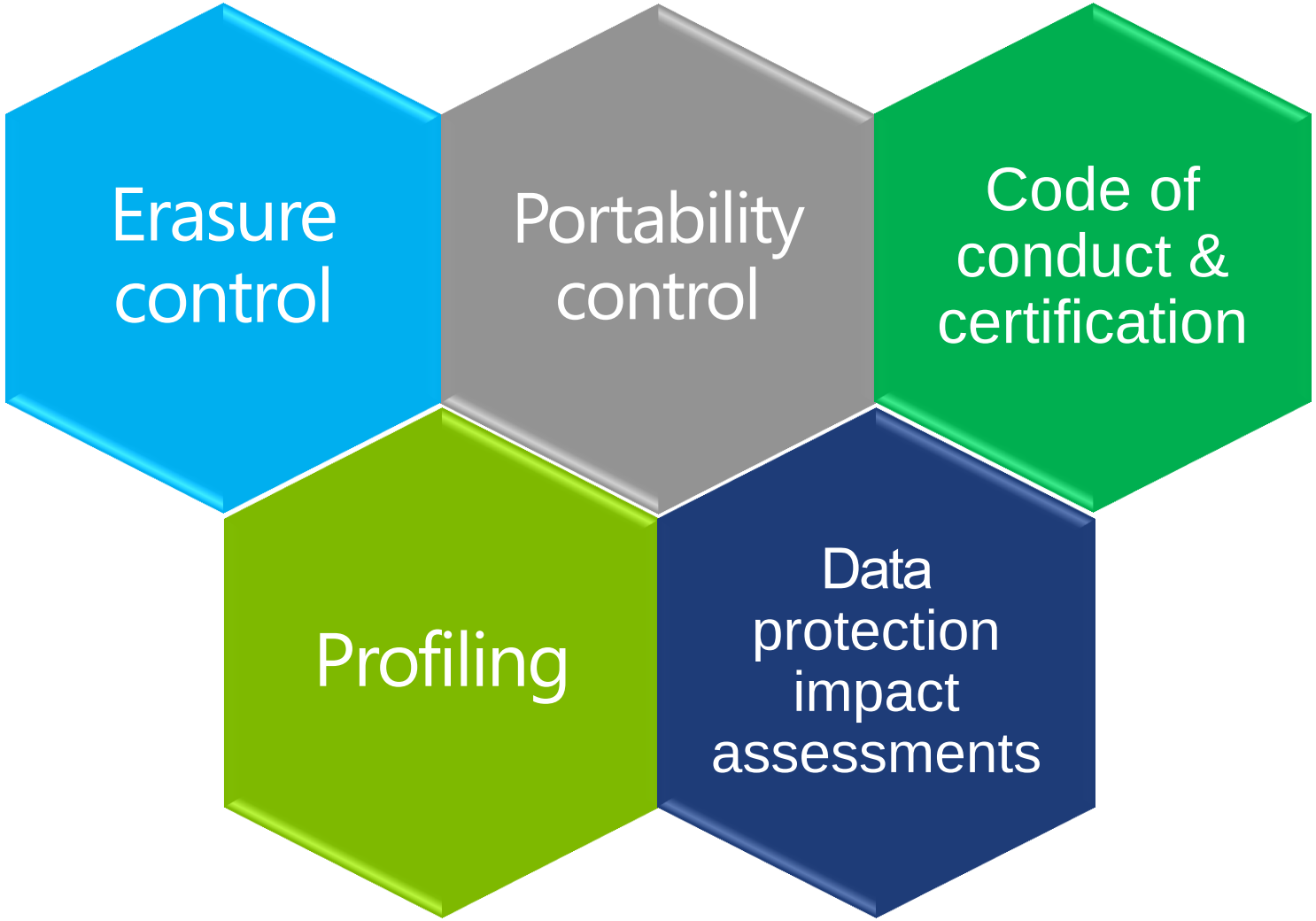
Why a new regulation ?

A “notice and consent” principle not really fitting digital world’s data protection challenges

Diverging national transpositions do no longer suit a basic need to frame online activities

The need for a more comprehensive and flexible assessment of privacy risks

New concepts proposed in the EU Draft regulation



Microsoft

Cybersecurity

EU draft NIS Directive

Network and Information Security Directive

Critical Years for European Cybersecurity to Come.

Portuguese Cybersecurity Law

German Cybersecurity Law

Safe harbor review

Microsoft believes regulation plays a critical role in the realm of cybersecurity & welcomes the Commission initiative.

Cyber Security Strategy

European Cloud Strategy

eID regulation

Latvian Cybersecurity Law

Open discussion with industry

Focus on risk management

Dutch Cybersecurity Law

French Cybersecurity Law

NIS Directive

Focus on critical infrastructure (reduction of scope)

Polish Cybersecurity Law

Introduction of single point of contact

Danish Cybersecurity Law

Removal of Delegated Acts

Czech Cybersecurity Law

Telecom package

Croat Cybersecurity Law

Focus on risk management & prioritization central to the success of the Directive.

Lithuanian Cybersecurity Law

Estonian Cybersecurity Law

Data Protection Package Review

Questions remained:

- Are public administrations included?
- How will Member States cooperate?
- How to preserve voluntary exchange of information?
- How to best make use of international standards?
- How to ensure maximum harmonization across the EU, globally and with other legislative proposals?

Potential Challenges with Current Direction

Microsoft

Making the perfect be the enemy of the good

Broad regulatory scope + minimum harmonization = uneven cybersecurity patchwork for Europe

Broad regulatory scope + limited security resources = less security.

Broad regulatory scope + incident reporting = data protection concerns

What does it mean for European cybersecurity

Harmonization will be critical

Opportunity Lost: Lowest Common Denominator

Rising Baselines: stronger risk management, analysis, readiness, response, and cross-border collaboration

Common Operational Understanding: Building on baselines to include sharing of strategic assessments and enhanced public-private cooperation.

Optimum scenario: EU cybersecurity shield

Microsoft

Cloud Standards

ISO 27018

ISO 27018

The first international standard for privacy in the cloud

ISO 27018 is a new international standard for the protection of personal data in cloud, based on EU data protection laws. It has been published on July 30 2014. Contributors from 14 countries and 5 international organisations.

An efficient alternative to customer audits

ISO 27018 compliance can be assessed and certified by independent 3rd parties through an audit. This can facilitate the verification of compliance with applicable laws and regulations for the protection of personal data by customers in a few seconds.

ISO 27018 compliant cloud services are easy to assess and compare

ISO 27018 requires the cloud service provider to establish several transparency measures regarding its policies for the protection of personal data, such as the data retention period once contract has terminated. This transparency information is then readily available for customers.

ISO 27018 can facilitate compliance of customer with obligations under EC/95/46

ISO 27018 provides appropriate technical and organizational measures to protect personal data, in implementation of article 17.1 of the directive EC/95/46.

A cloud service provider complying with ISO 27018 can be presumed to have provided sufficient guarantees in respect of the protection of personal data, as required by article 17.2 .

ISO 27018 – Born in the Cloud

Key Principles - Cloud providers must:

- Not use data for advertising or marketing unless express **consent** is obtained
- Be **transparent** about data location and how data is handled
- Provide customers with **control** over how their data is used
- Be **accountable** to determine if customer data was impacted by a breach of information security
- **Communicate** to customers and regulators in the event of a breach
- Have services **independently audited** for compliance with this standard