The GDPR – A modern data protection framework

Safeguarding Privacy and Exchanging Data in a Connected World

CSG West, 17 July 2019
Rainer Wessely, EU Delegation to the US
10 things you need to know about the GDPR

1. GDPR nothing new
2. Personal scope
3. Material scope
4. Data protection principles
5. Rights
6. Obligations / Responsibilities
7. Enforcement
8. The role of the EDPB
9. International transfers
10. One year of GDPR
1) The GDPR is nothing "new"

- **Existing data protection law** (Data Protection Directive from 1995), **but**...

- **Technological developments and globalisation**: Addressing the challenges and seizing the opportunities of the digital economy

- **Fragmentation of legislative framework** (different transposition of the current Directive into national laws)
2) Personal scope

- **Business operators**

- **Public authorities** (except criminal law enforcement (LED); national security and defence)

- Processing carried out for purely personal/household activities is **excluded**
3) Material scope

Processing of personal data
= information relating to living natural person who:

• is **identified** directly by that information;

• can be **(in-)directly identified** from that information, incl. **in combination with** other information

  => all means reasonably likely to be used (e.g. costs, time, technology) by controller or other person

Includes “**pseudonymised data**”, but not “**anonymous information**”
4) Data protection principles

- Transparency
- Lawfulness (legal basis for processing)
- Purpose limitation
- Data minimisation
- Data accuracy
- Limited retention
- **Data security** - Special protection of sensitive data
5) Key rights

- Right to **information** (transparency)
- Right to **access, rectification and erasure**
- Right to **data portability**
- Right to **object** to processing
- Right **not to be subject to decisions based solely on automated processing** and producing legal/significant effects
- Right to **redress**
6) Key obligations / responsibilities

- **Risk-based approach** = No "one-size-fits-all", but different obligations according to the risk of processing
- **Accountability, responsibility** to demonstrate compliance, cooperation with authorities, **Record-keeping** of processing
- **Data protection by default and by design** (Pseudonymisation)
- **Data security**
- **Data breach notification**
- **Data protection impact assessment**
- **Data protection officer (DPO)**
7) Independent enforcement

More than 28 independent Data Protection authorities (DPAs)

- Responsible for monitoring and enforcing compliance with data protection law
- Contribute to the consistent interpretation and application of data protection law throughout the EU
- Cooperate with other DPAs and enforcers in third countries (cross-border enforcement of increasing importance)
8) European Data Protection Board (EDPB)

Nature and composition

- **Independent EU body** with legal personality.
- Represented by its **Chair**, who is elected for a renewable term of five years (currently the Head of Austrian DPA).
- Composed of the **Head of one supervisory authority per Member State** and of the European Data Protection Supervisor.
- **European Commission** has the right to participate in activities and meetings of the Board without voting right.
9) International transfers

- General principle = **Protection should travel with the data/not be undermined**

- Broad “**toolbox**”

- **Convergence** as a **trade facilitator**: facilitating data flows while ensuring a high level of protection (e.g. adequacy decision for Japan)

- Proposal for **data flows provisions in free trade agreements** (FTAs): prohibition of data localisation, regulatory autonomy when it comes to data protection standards
10) 1 year of GDPR implementation

- **Individuals are making use of their rights**: increased number complaints, queries, information requests, etc.
- **Guidance on all novel aspects has been issued**: the EDPB has adopted a series of guidelines on the GDPR following broad public consultations
- **Companies are putting their data house in order**: taking a closer look at what data they are collecting, what they use it for, how they keep and share it etc.
- **Compliance is a dynamic process**: DPAs engage with stakeholders to find best ways to implement obligations
- **Enforcement** (British Airways, Google etc)
Thank you very much for your attention!