

(enter

vienna | brussels | berlin | hong kong | london | new york europäisches zentrum für e-commerce und internetrecht european center for e-commerce and internet law

partners:

a1 telekom austria | arthur d. little | asia-pacific council | computer ethics society | das | deloitte | erste bank hutchison | international lab for it & ip | kyberna | ky-center for social media law | mbo media | microsoft | novomatic orange | public interest | raiffeisen informatik | siemens | telering | t-mobile | tailored apps | updatemi | wolf theiss

ceo:

prof. dr. wolfgang zankl



The New European Data Protection Regulation

A Threat to China?



Introduction

- So far: European Data Protection Directive 1995
 - Directive: Differences in data privacy regulations of member states
 - Outdated
- From May 25th 2018: General Data Protection Regulation (GDPR)
 - Regulation: In all member states
 - Contemporary







- "The GDPR is a compromise between the EU member states, and is has therefore lead to a number of undetermined legal terms. I do hope that law enforcement authorities will not apply the GDPR in such a way that Europe will miss opportunities" (Angela Merkel).
- "World's toughest privacy law" (fortune.com)
- "One of the worst laws of the 21st century" (Thomas Hoeren)



Key Issues

- 1. Territorial Scope
- 2. Data scope
- 3. Controllers and Processors
- 4. Data Protection Principles
- 5. Accountability
- 6. Lawful Processing
- 7. International Transfers
- 8. Data Breach Notification
- 9. Rights of Individuals
- 10. Sanctions







- Companies established within the EU: processing personal data "in the context of the activities of an establishment of any organization within the EU, regardless of whether processing takes places in the Union or not" (Art. 3/1).
- Companies established outside the EU: processing personal data of EU data subjects ("who are in the Union") by "offering goods or services, irrespective of whether a payment of the data subject is required", or "monitoring of their behavior" (Art. 3/2).





- Personal Data: "any information relating to an identified or identifiable natural person" = "data subject"
- I dentifiable: e.g. by name, birthday, gender, IPaddress







- Data controllers: responsible for determining the purposes and means of processing personal data
- Data Processors: engaged by controllers to process personal data on their behalf
 - Processors only where <u>sufficient guarantees</u> to implement appropriate measures to meet GDPR requirements and protect data subjects rights
 - Requirements (e.g.): maintain written <u>record of processing</u> <u>activities</u> for each controller







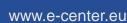
- Lawfulness, fairness and transparency: "processed lawfully, <u>fairly</u> and in a transparent manner"
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability: "controller shall be responsible for, and be able to demonstrate compliance" with these principles





- Companies (exemptions when less than 250 employees) need to be able to demonstrate compliance by
 - keeping <u>extensive records</u> of processing
 - performing impact assessment for <u>high risk processing</u>,
 e.g. sensitive data
 - designating data protection officer (when core activities in monitoring or in sensitive data)
 - notifying and keeping <u>comprehensive record</u> of data breach
 - implementing data privacy by design/default









- •Data subject has given freely, specific and informed consent (clearly distinguable from other matters; right to withdraw; related to sensitive data only with <u>explicit</u> consent, data made public by data subject and other exemptions, Art. 9)
- •Processing necessary for (e.g.)
 - performance of a contract
 - compliance with legal obligation
 - purpose of <u>legitimate interests</u> of controller (except where overridden by data subject interests)









Only allowed where

- •Adequacy decision (by EU-Commission)
- Appropriate safeguards by controller/processor, e.g. binding corporate rules
- •Explicit consent after having been informed of the possible risks





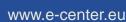
- To supervisory authority: "without undue delay, and where feasible, not later than 72 hours", including categorie and approx. number of individuals concerned, likely consequences and measure taken to mitigate harm (Art. 33)
- To data subject: "when likely to result in a high risk to rights and freedoms of individuals without undue delay" (Art. 34), describing nature and measures. No notification when (e.g.) "it would involve disproportionate effort" (public information instead)
- Unless "unlikely to result in a (to data subject: high)
 risk to rights and freedoms of natural persons": no
 other exemptions (Uber conceiling data breach by
 paying hackers in order to destroy stolen data)
- Processors: notify controller





- Transparency (Art. 13): Where personal data are collected from the data subject (from third parties see Art. 14) information must be provided (like all other information in a "concise, transparent, intelligible and easily accessible form, using clear and plain language, Art. 12), e.g.
 - identity and contact of controller
 - purpose
 - recipients of data
 - rights of the data subject (e.g. access, rectification, erasure, portability)

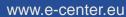






- Confirmation of whether or not data are being processed and access to such data within a month and free of charge (Art. 15), including information about (e.g.) purpose, categories
- Rectification (Art. 16)
- Erasure (Art. 17): "right to be forgotten" without undue delay where e.g. the following applies: data no longer necessary, withdraw of consent, unlawfully processed, except when e.g. exercising right of freedom of expression and information
- Data Portability (Art. 20): right to receive or have transmitted to another controller personal data in a structured, <u>commonly used</u> and machine-readable format







- Fines: Failure in complying with GDPR results in fines up to 20 Million Euro or (whichever is higher) up to 4% of total worldwide turnover of preceding year (Art. 83)
 - Fines imposed on "undertakings" (rather than controllers); should be understood in accordance with Art. 101/102 EU-Treaty (Recital 150): Group companies treated as one?
 Questionable in regard to Art. 4/19: "group of undertakings means a controlling undertaking and its controlled undertakings" vs. only "undertaking" in Art 83
 - Fines "shall in each individual case be <u>effective</u>, <u>proportionate and dissuasive</u>" (Art. 83/1)







- Compensation and liability: "Any person who has suffered material or non-material damages as result of infringement of this Regulation shall have the right to receive compensation from the controller or processor" (Art. 82)
 - "Any person" vs. "data subject"
 - Exemption of liability: controller/processor proves that <u>in</u> no way responsible for the event given rise to damage







Thank you for your attention

zankl@e-center.eu