Baker McKenzie.

European and International Privacy Law

Dr. Lukas Feiler, SSCP, CIPP/E
Baker & McKenzie
LL.M. European and
International Business Law

Topics

1	Regulatory approaches in the EU and the U.S.
2	Highlights & Basic Concepts
3	Principles of processing personal data

1 Regulatory approaches in the EU and the U.S.

Data Protection as a Fundamental Right in the EU (1/2)

- European Convention on Human Rights
  - Article 8(1): *Everyone has the right to respect for his private and family life, his home and his correspondence*.
  - Article 8(2): *There shall be no interference by a public authority with the exercise of this right except such as*
    - *is in accordance with the law and*
    - *is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*.

© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

Data Protection as a Fundamental Right in the EU (2/2)

- EU Charter of Fundamental Rights
  - specifically provides the right to data protection (article 8)
- Austria: Data Protection Act § 1
- Germany: Fundamental right of informational self-determination

© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

Data Privacy under U.S. Law (1/2)

- Constitutional Law
  - 1st Amendment: Freedom of association covers confidentiality of membership list (NAACP v. Alabama, 357 U.S. 449 (1958)
  - 4th Amendment: Protection against unreasonable searches & seizures; however only if there is a “reasonable expectation of privacy” (Katz v. United States, 389 U.S. 347 (1967))
    - secrecy paradigm

© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

Data Privacy under U.S. Law (2/2)

- Federal law
  - only sector-specific and in reaction to specific incidents, e.g.:
    - Health Insurance Portability and Accountability Act: health care providers
    - Gramm-Leach-Bliley Act: financial institutions
    - Fair Credit Reporting Act: credit reporting agencies
    - Video Privacy Protection Act: video tape service providers
  - largely: self-regulation
- Common law / privacy torts
  - intrusion upon seclusion secrecy paradigm
  - public disclosure of private facts secrecy paradigm

© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

The Legal Framework of Data Protection in the EU

The old regime

- Data Protection Directive (Directive 95/46/EC)
  - ECJ Joined Cases C-468/10 and C-469/10:
    - Not only minimum but full harmonization
    - Directly applicable if unconditional and sufficiently precise
- ePrivacy Directive (2002/58/EC) – generally only applies to the telecommunications sector

The new regime as of 25 May 2018

- General Data Protection Regulation – GDPR (2016/679/EU)
- Directive for the processing of data by law enforcement authorities (2016/680/EU)
- ePrivacy Regulation (expected for 2019)

© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

2 GDPR – Highlights & Basic Concepts

GDPR - Highlights

- Uniform law … but
  - 69 opening clauses for Member State law
- Enforcement by national DPAs
  - European Commission is not granted any enforcement authority
  - European Data Protection Board
    - Will replace Article 29 Working Party
    - Will only settle disputes between DPAs
- No general notification requirement
  - But prior consultation/authorization requirements for high risk processing
- High fines

© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

GDPR Background

- EC Data Protection Directive of 1995:
  - Not directly applicable but 28 different national laws and interpretations of data protection and associated administrative burdens cost business an estimated €2.3bn per year
  - Data protection filings in almost all EU Member States cost business an estimated €130 million per year
- EU Data Protection Regulation:
  - One uniform and directly applicable piece of data protection legislation doing away with the most burdensome administrative requirements
  - Looking at the background facts
  - Implementation should be a no-brainer?

© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

Legislative Process of the GDPR

- Legislative process proves long and winding
  - almost 4000 amendments tabled by members of the EP
  - Vote of EP postponed twice
- Timeline
  - Jan 2012: Commission introduces first proposal
  - Jan 2013: Rapporteur of LIBE releases initial report
  - Since Nov 2013: trialogue talks (EP/Council/Europ. Comm.)
  - March 2014: EP approves draft by plenary vote (1st reading)
  - June 2014: Council adopts common position on some aspects
  - December 15, 2016: Political agreement in trialogue
  - May 4, 2016: Publication in Official Journal (Regultion 2016/679)
  - May 25, 2018: Start of application

© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

Scope of the GDPR (1/2)

- General rule
  - GDPR applies (Art 2(1))
    - to the processing of personal data wholly or partly by automatic means, and
    - to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system
      - "Filing system": any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis

© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

Scope of the GDPR (2/2)

- Exceptions
  - DPD does not apply to the processing of personal data (Art 2(2) GDPR)
    - by a natural person in the course of a purely personal or household activity
    - in the course of an activity which falls outside the scope of Union law
      - public security, defence,
      - State security
    - processing by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security
      - Directive 2016/680/EU

© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

What is “Personal Data”? (1/2)

- Data Protection Directive
  - any information relating to an identified or identifiable natural person
  - an identifiable person is one who can be identified, directly or indirectly
  - True anonymization is tricky:
    - e.g., Netflix movie ratings, AOL searches, location data
    - Mostly pseudonymization

© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

What is “Personal Data”? (2/2)

- Is Personal Data a relative or absolute term?
  - relative: personal data only if company processing the data can determine identity of data subjects
  - absolute: personal data if *anyone* can determine identity
  - ECJ Case C-582/14, 19 October 2016:
    - Is an IP address which a website provider stores when his website is accessed personal data for the website provider if a third party (an access provider) has the additional knowledge required in order to identify the data subject?
    - IP address “constitutes personal data […] in relation to that provider, where the latter has the legal means which enable it to identify the data subject”

© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

Actors in the Data Protection Landscape (1/3)

- Data subject
  - a natural person to whom the information relates
- Controller
  - Natural or legal person which determines the purposes and means of the processing of personal data

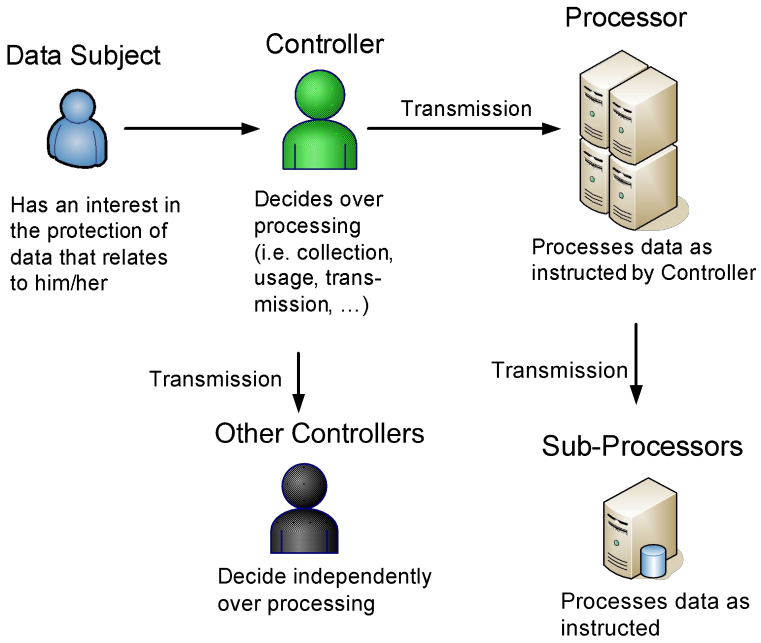
© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

Actors in the Data Protection Landscape (2/3)

- Processor
  - Natural or legal person which processes personal data on behalf of a controller
  - Processing: *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction* (Article 4(2) GDPR)

© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

Actors in the Data Protection Landscape (3/3)



© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

Regulatory Authorities

- National Supervisory Authorities / DPAs
  - EU data protection law is exclusively enforced by these national authorities
- European Data Protection Supervisor (EDPS)
  - monitors the compliance of processing operations carried out by an EU institution (European Commission, European Parliament, Council, …).
  - Advises EU institutions in legislative affairs
- European Data Protection Board (successor of “Art 29 Working Party”)
  - Consists of representatives from the DPAs
  - Settles disputes between DPAs
  - Issues interpretive guidance

© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

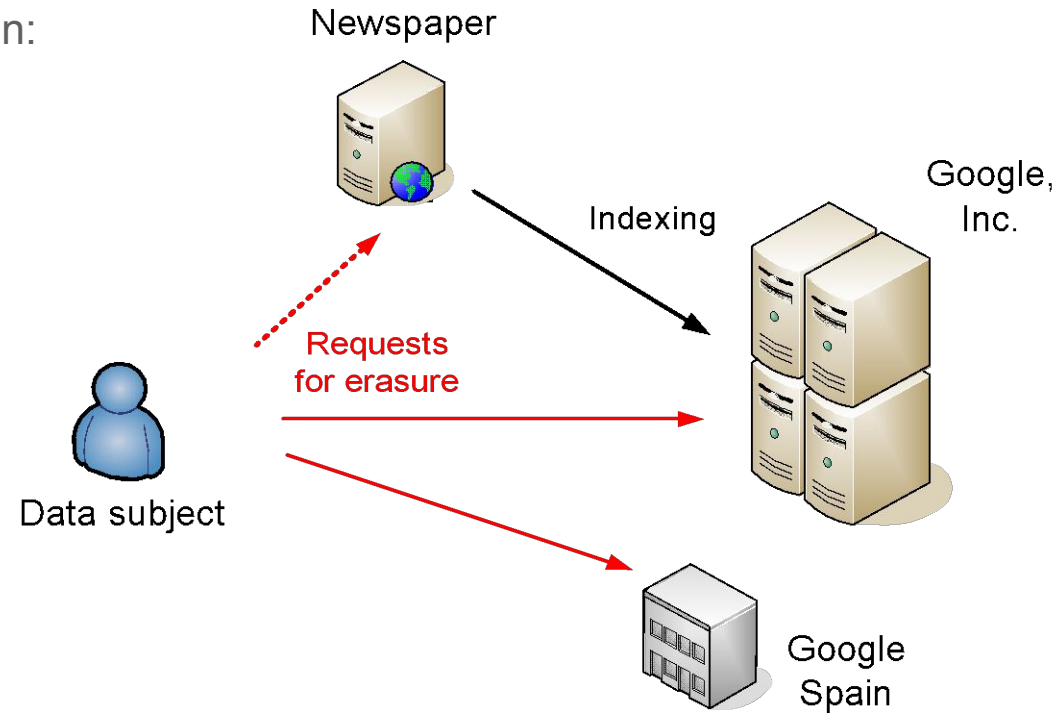
GDPR – Geographic scope of application (Art 3 GDPR)

- If controller/processor has an establishment in the EU
  - and processing is performed in the context of the activities of the EU establishment
  - Establishment "*implies the effective and real exercise of activity through stable arrangements*"; "*whether through a branch or a subsidiary with a legal personality, is not the determining factor*" (Recital 22)
- If controller/processor is not established in the EU
  - but EU residents' data is processed and processing of relates to
    - the offering of goods or services to EU residents, irrespective of whether a payment by the data subject is required
      - covers all non-EU e-commerce companies offering their services in the EU
    - the monitoring of their behavior within the EU
      - covers all online tracking companies (ad networks)

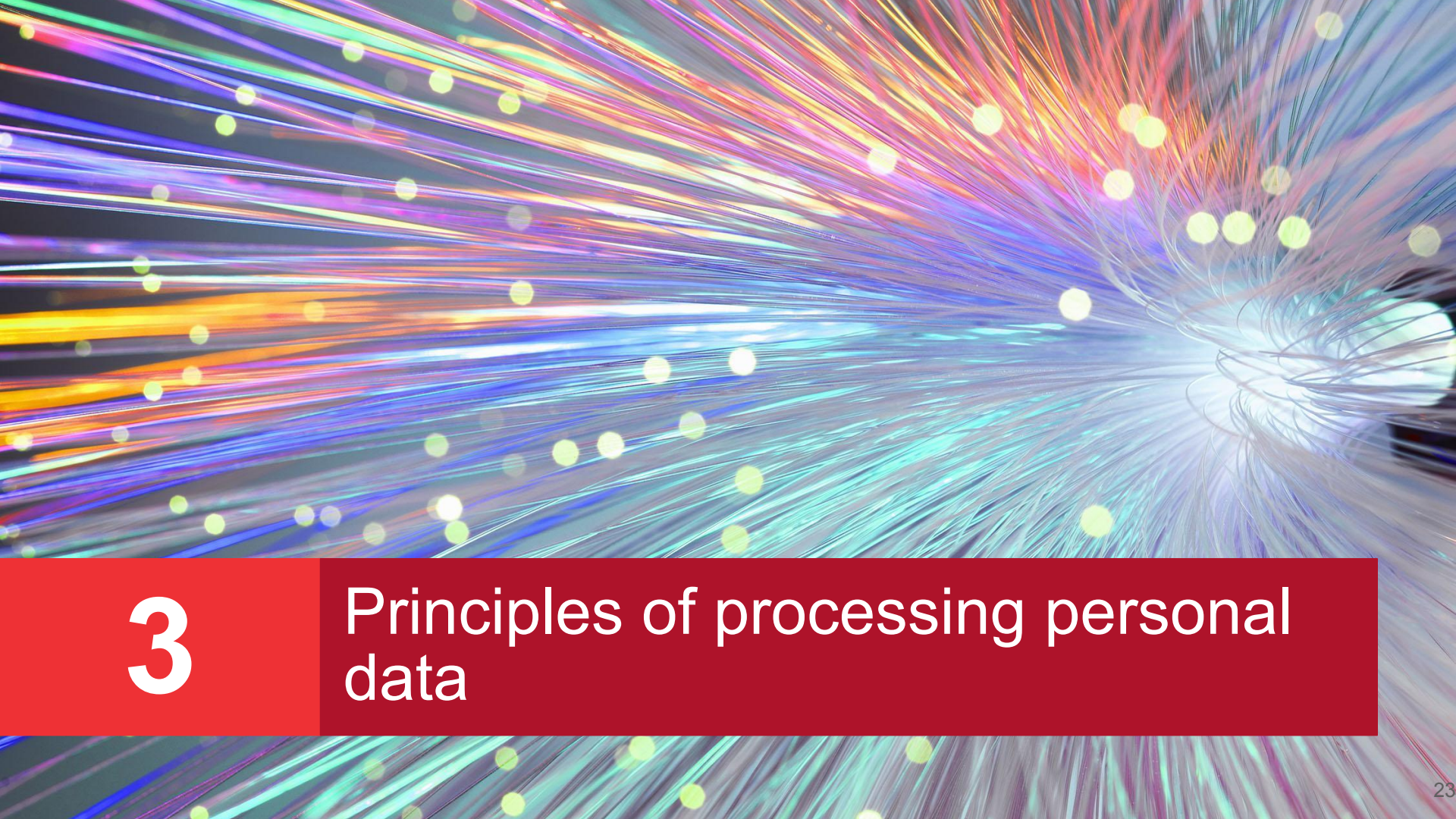
© 2018 Diwok Hermann Petsche Rechtsanwälte LLP

ECJ Case C-131/12, Google v. AEDP

Initial situation:



© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG



3 Principles of processing personal data

Principles of data processing

General principles

- Lawfulness
- Fairness
- Transparency

Purpose-oriented principles

- Purpuse specification & purpose limitation
- Data minimization & storage limitation
- Accuracy

Compliance-oriented principles

- Technical and organizational measures
- Accountability

© 2017 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

General principles of data processing

- Lawfulness (Art 5(1)(a) GDPR)
  - Any processing operation requires a legal basis pursuant to Art 6, 9 or 10
- Fairness (Art 5(1)(a) GDPR)
  - General principle of proportionality – don‘t use a sledge-hammer to crack a nut
- Transparency (Art 5(1)(a) GDPR)
  - processing to be performed in a transparent manner in relation to the data subject
  - specified by
    - obligation to provide data protection notices (Art 13 et seq.)
    - obligation to perform data breach notification (Art 34)

© 2017 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

Purpose-oriented principles – 1 of 3

- Purpose specification (Art 5(1)(b) GDPR)
  - personal data may only be collected for specified, explicit and legitimate purposes
  - specified purposes: no data collection based on „let‘s see what we can do with it“
  - explicit purposes: not „company purposes“
    - practical tip: short description of the business process for which the data is used
  - legitimate purposes
    - compliance with all other legal/regulatory requirements, e.g. employment law

© 2017 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

Purpose-oriented principles – 2 of 3

- Purpose limitation (Art 5(1)(b) GDPR): personal data may only be processed
  - for the originally defined purposes
  - for compatible purposes compatibility assessment (Art 6(4) GDPR):
    - link between old and new purposes
    - context of data collection / relationship between data subject and controller
    - nature of the personal data, in particular whether sensitive data (Art 9) or crime-related data (Art 10)
    - possible consequences of processing for new purposes
    - appropriate safeguards such es encryption or anonymization
  - Exception from purpose limitation: data subject consent
- Data minimization (Art 5(1)(c) GDPR)
  - personal data may only be collected/process to the extent necessary for the processing purposes

© 2017 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

Purpose-oriented principles – 3 of 3

- Accuracy (Art 5(1)(d) GDPR)
  - personal data has to be accurate and, where necessary, kept up to date
  - „reasonable step“ have to be taken depends on processing purposes
- Storage limitation (Art 5(1)(e) GDPR)
  - personal data may only be kept in a form which permits identification of data subjects for as long as necessary for the processing purposes
  - obligation to erase or anonymize

© 2017 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

Compliance-oriented principles

- Technical and organizational measures (Art 5(1)(f) GDPR)
  - Technical and organizational measurs („TOMs“) are required to ensure
    - security and
    - lawfulness of processing
  - Specified by Art 24 (TOMs for lawfulness) and Art 32 (TOMs for security)
- Accountability (Art 5(2) GDPR)
  - Obligation to implement measures that ensure compliance with other principles
  - Obligation to demonstrate compliance with other principles

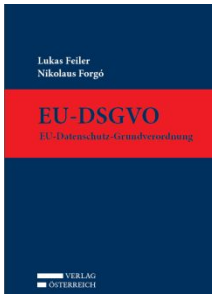
© 2017 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG

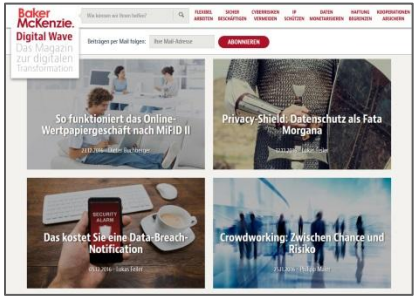
Baker McKenzie.

Dr. Lukas Feiler, SSCP CIPP/E
Senior Associate
Head of IP/IT in Vienna

Schottenring 25
1010 Vienna

T: +43 1 24 250
lukas.feiler@bakermckenzie.com





Lukas Feiler is co-autor of the first Austrian commentary on the GDPR and of the first Austrian book on the practical implementation of the GDPR. He also advises companies on the digital transformation under www.digitalwave.at.

www.bakermckenzie.com

Diwok Hermann Petsche Rechtsanwälte LLP & Co KG is a member firm of Baker & McKenzie International, a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as “Attorney Advertising” requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.
© 2018 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG