Developments in Data Protection from a Technical Perspective

Julia Stoll
Referatsleiterin Informatik
Der Hessische Datenschutzbeauftragte
Gustav-Stresemann-Ring 1, 65189 Wiesbaden
Telefon +49 (0)611 / 14 08 - 150
E-Mail: j.stoll@datenschutz.hessen.de

Outline

- Introduction to the role of the EU-Regulation 2016/679 (“General Data Protection Regulation”, GDPR)
- Some basic terms and data protection principles
- Different technical perspectives (data, operations and procedures)
- Data protection impact assessment (DPIA)
- Upcoming ideas and possible solutions

Some information ...

- The General Data Protection Regulation 2016/679 (GDPR) will apply from 25 May 2018
  - Period of implementation and transformation
- 98 article and 173 recitals (role of recitals)
- Legal basis: European Charta of Human Rights, especially Art. 8
- 27/28 Member States + 3 (Island, Norway and Switzerland, where these counties are part of the "Digital Market")
- 24 official languages (like Maltese or Gaelic)
- 3 languages „in use" (English, French and German)
- Art. 29 Working Party (WP29) to the European Data Protection Board (EDPB)

Some more information ... (Ch I: General provisions)

Art. 1 (1) Subject-matter and objectives

This Regulation lays down rules relating to the **protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.**

Recital 1: The protection in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

Recital 2: Convergence of the economics within the internal market (resp. “Digital Market”)

Recital 2: The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, **to strengthening and the convergence of the economics within the internal market, and to the well-being of natural persons.**

Some basic terms in brief

Personal Data	Information on identified or identifiable natural person; „data subject“ (Art. 4 (1))
Processing	Handling of personal data (Art. 4(2))
Controllers in the EU	Any person who operates from an establishment within the Union (recital 14)
Data processing controller	Natural person or legal person, public authority, agency or other body which either alone or with others decides on the purpose and means of the prcoessing Art 4 (7), Art. 26
Processor	Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Art. 4 (8))

Principles („Data processing“)

Art. 5	Principles relating to processing of personal data
„Data minimization“ (Art. 5 (1) lit. c): Personal data shall be: adequate, relevant and limited to what is necessary in relation to the purposes for which the are processed	
Art. 6	Lawful of processing
Art. 7	Conditions for consent
Art. 9	Processing of special categories of personal data
Art. 9 (1): Processing of personal data regarding revealing racial or ethic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic, biometric, for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.	

RIGHTS OF THE DATA SUBJECT – PROCESSING DATA

Articles related to operations on data (Ch. III: Rights of the data subject)

Art. 12	Transport information, communication and modalities for the exercise of the rights of the data subject (**"overview, what has to be done for operating personal data"**)
Art. 13	Information to be provided where personal data are ***collected for the data subject***
Art. 14	Information to be provided where personal data have ***not been obtained from the data subject***
Art. 15	Right of the access by the data subject

Articles related to operations on data (Ch. III: Rights of the data subject, con'd)

Art. 16	Right to rectification
Art. 17	Right to erasure ('**right to be forgotten**')
Art. 18	Right to restriction of processing ("new" **– it does not mean "disable"**)
Art. 19	Notification obligation regarding rectification or erasure of personal data or restriction of processing
Art. 20	Right of data portability ("new" – using a **standard format**)

Articles related to operations on data (Ch. III: Rights of the data subject, con'd)

Art. 21	Right to object
Art. 22	**Automated individual decision-making**, including profiling
Art. 23	Restrictions

PRINCIPLES OF DATA PROTECTION – FOCUS ON PROCESSES

Principles of Data Protection

- Availability
- Integrity
- Confidentiality
- **Unlinkability**
- **Transparency**
- **Intervenability**

Availability

The protection goal of **availability** is the requirement that personal data must be available and can be used properly in the intended process.

Integrity

The protection goal of **integrity** refers to, on the one hand, to the requirement that information technology processes and systems continuously comply with the specifications that have been determined for the execution of their functions. On the other hand integrity means that the data to be processed remain intact, complete, and up-to-date.

Confidentiality

The protection goal of **confidentiality** refers to the requirement that no person is allowed to access personal data without authorization.

Unlinkability

The protection goal of **unlinkability** refers to the requirement that data shall be processed and analyzed only for the purpose for which they were collected.

Transparency

The protection goal of transparency refers to the requirement that the **data subject** as well as the **system operators** and the **competent supervisory authority** must be able to understand, to a varying extent, which **data are collected and processed for a particular purpose**, which **systems and processes are used** for this purpose, where the **data flow** for which purpose, and **who is legally responsible for data and systems in the various phases** of data processing.

Intervenability

The protection goal intervenability refers to the requirement that **data subjects are effectively granted their rights** to notification, information, rectification, blocking and erasure at any time, and that the controller is obligated to implement the appropriate measures.

Data protection principles in the GPDR

	Data Minimisation	**Availiability**	**Integrity**	**Confidentialty**
Articles	Art. 5. Abs. 1 lit. c and lit. e; Art. 25, Art. 32	Art. 5. Abs. lit. e, Art. 13, Art. 15, Art. 20, Art. 25, Art. 32	Art. 5 Abs. 1 lit. f , Art. 25, Art. 32, Art. 33	Art. 5 Abs. 1 lit. f, Art. 25, Art. 28 Abs. 3 lit. b, Art. 29, Art. 32
Recitals	28, 29, 30, 39, 78, 156	49, 78, 83	39, 49, 78, 83	39, 49, 78, 83

Data protection principles in the GPDR

	Unlinkability	**Transparency**	**Intervenability**
Articles	Art. 5. Abs. 1 lit. c dnd lit. e; Art. 17, Art. 22, Art. 25, Art. 40 Abs. 2 lit. d	Art. 5. Abs. lit. a, Art. 13, Art. 14, Art. 15, Art. 19, Art. 25, Art. 30, Art. 32, Art. 33, Art. 40, Art. 42	Art. 5 Abs. 1 lit. and lit. f , Art. 13 Abs. 2 lit. c, Art. 15 Abs. 1 lit. e, Art. 16, Art. 17, Art. 18, Art. 20, Art. 21, Art. 25, Art. 32
Recitals	31, 32, 33, 39, 50, 53, 71, 78	32, 39, 42, 58, 60, 61, 63, 74, 78, 84, 85, 86, 87, 90, 91, 100	39, 59, 65, 66, 67, 68, 69, 70, 78

Articles related to processes (design, processing operations, processing acticities and (re-)use)

Art. 25	Data protection by design and by default **(data protection principles)**
Art. 30	Records of processing activities
Art. 32	Security of processing **(data protection principles)**
Art. 35	Data protection impact assessment (DPIA) **(critieria, which should be checked in advance to reduce a „high risk“)**
Art. 36	Prior consultation (to proceed a DPIA)

PROCEDURES FROM A TECHNICAL PERSPECTIVE
IMPLEMENTING NEW TECHNOLOGIES

Data protection impact assessement (DPIA)

- Goals of a data protection impact assessment
  - To manage risks to the data protection rights and freedoms of natural persons
  - To determine the measure to address them
  - To comply with the requirements of the GDPR
  - To demonstrate the appropriate measure have been taken to ensure compliance with this Regulation
  - To guarantee accountability and traceability
- DPIA is a process for building and demonstrate compliance
- No DPIA can result in an administrative fine up to 10M€, or up to 2% or the total worldwide annual takeover of the preceding financial year, whichever is higher

What does a DPIA address?

- A DPIA may concern a single data processing operation; see e.g. application of Art. 12-15
- A single DPIA could be used to assess multiple processing operation that are similar.
- A DPIA can be also useful for assessing the processing impact of a new technology.

Some formal criteria apply to proceed a DPIA

Art. 35 (1):

Where a type of processing in particular using **new technologies**, and taking into account the **nature, scope and context and purposes of the processing**, is ***likely to result in a high risk* to the rights and freedoms of natural persons**, the controller shall, *prior to the processing*, carry out an assessment of impact of the envisaged processing operation on the protection of personal data. [...]

Criteria in practice (work in process) for a DPIA – „positive list“ (Art. 35 (10))

- Evaluation and scoring
  - ePrivacy Regulation (work in process)
- Automated-decision making with legal or similar significant effect
- Systematic monitoring
- Processing of sensitive data (Art. 9 and recital 91)
- Data processing on a large scale

Criteria in practice (work in process) for a DPIA (con‘d)

- Data sets that have been matched of combinded
  - ePrivacy Regulation (on tracking, profiling or scoring in respect to identification)
- When the processing itself „prevents data subjects for exercising a right or using a service or a contract“
  - Art. 22 and recital 91
- A processing operation, where a service which entails a processing of personal data is used by natural persons in the course of a purely personal or household activity
- A processing operation that transfers data outside the EU

ORGANIZATIONAL MATTERS

Newer organisational structure

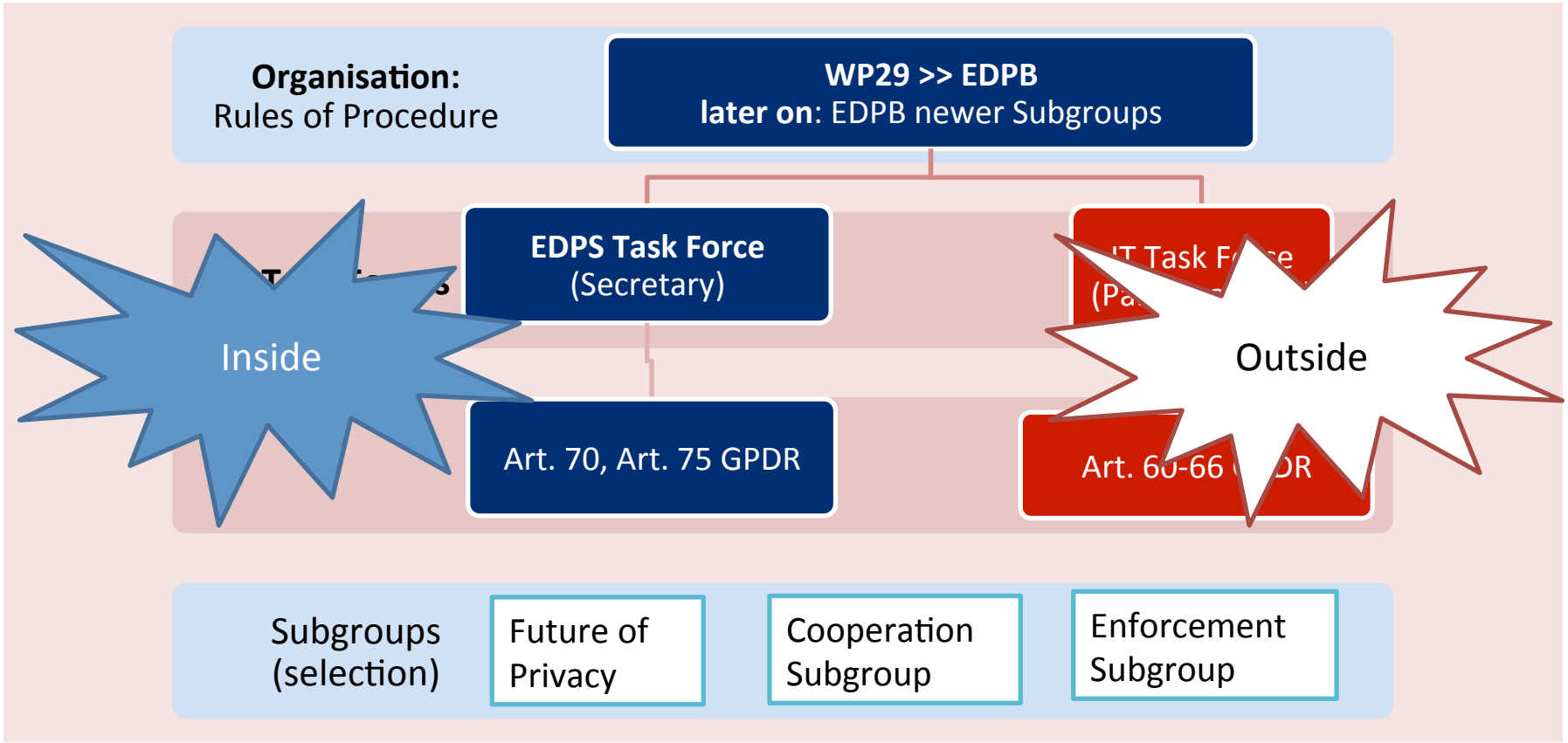
- European Data Protection Board ([former] Article 29 Working Party]
- Cooperation
  - Art. 60 Cooperation between the lead supervisory authority and the other supervisory authorities (often called: data protection authorities – DPAs)
  - Art. 61 Mutual assistance
  - Art. 62 Joint operations of supervisory authorities

  >> Urgency procedure (Art. 66 GDPR)
- Art. 63 to Art. 64: Consistency mechanism

  >> Urgency procedure (Art. 66 GDPR)

Newer organisational structure

EDPB Task Force << Art 29 Working Party



SOME DIFFERENCES

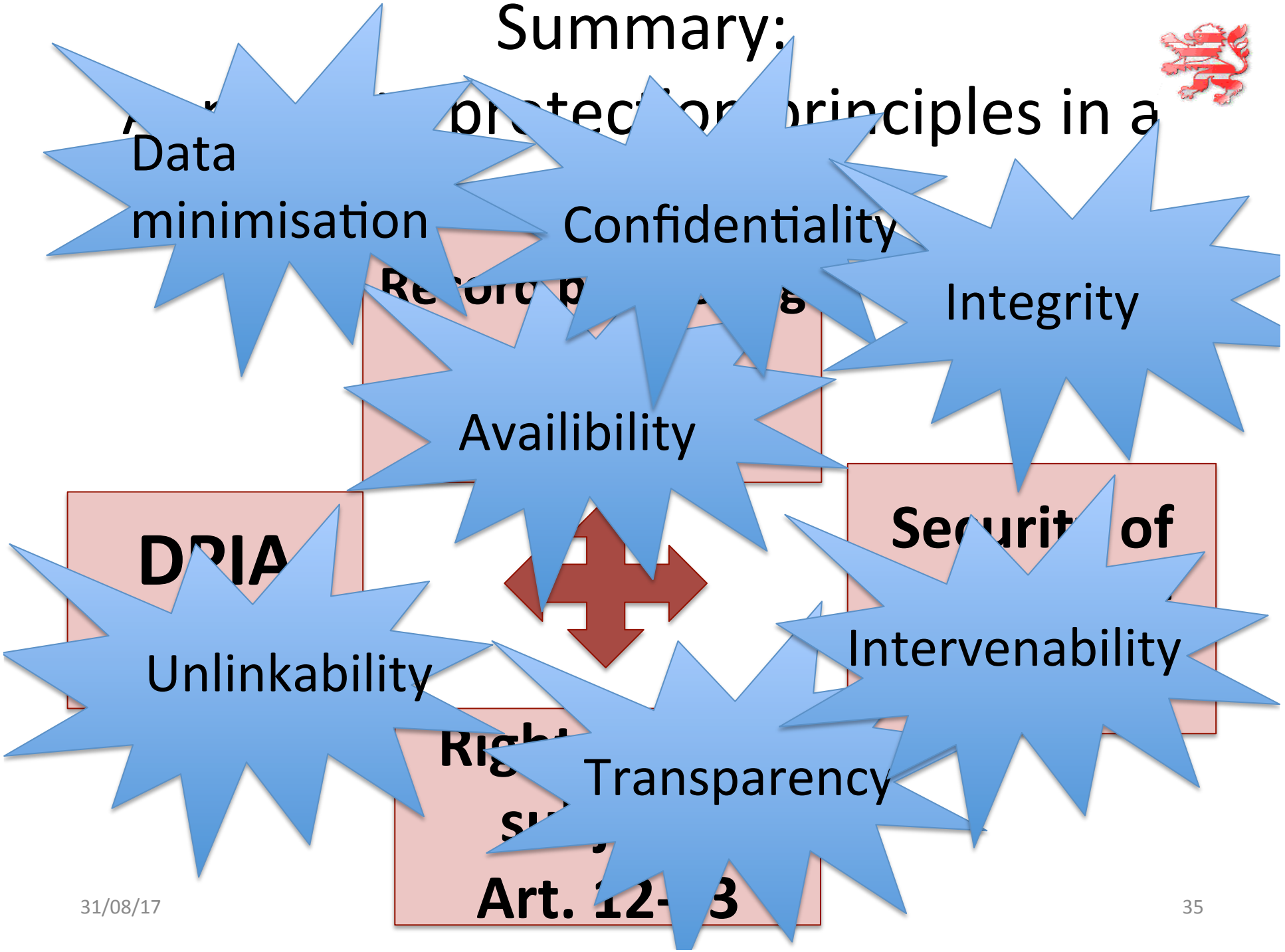
Terms and pitfalls

English	German
Procedure	Verfahren, insb. in der öffentlichen Verwaltung als Fachverfahren
Rules of procedure	Geschäftsordnung
Process	Prozess (als IT-gestütztes Verfahren)
Processing actities („Neu-Englisch“)	Verarbeitungstätigkeiten (Art. 30 GDPR)
Record of processing actities	(Gesamt)-)Verzeichnis von Verarbeitungsvorgängen [unterschiedlich!]
Processing operations („Neu-Englisch“)	Verarbeitungsvorgänge (Art. 35 GDPR)
Data protection impact assessment	Vorabkontrolle (lieferte (Gesamt-)Verfahrensverzeichnis) [unterschiedlich]

Terms and pitfalls (con‘d)

English	German
Operations	Operationen auf personenbezogenen Daten (erheben, beauskunften, informieren, Verarbeitung einschränken, löschen und portieren [an andere Anbieter übermitteln]
Unlinkability	Zweckgebundenheit / Nicht-Verkettbarkeit
Data subject	Betroffene (vorher: betroffene Personen, ggf. mit Trennung zwischen natürlichen und juristischen Personen)
Processor(s)	Verantwortliche
Controller(s)	Auftragsverarbeiter (Auftragsverarbeitung über einen Vertrag)
Consent	Nicht (!) alles geht über eine Einwilligung

Summary:


Data minimisation
Confidentiality
Integrity
Availibility
Unlinkability
Transparency
Intervenability

Some references (selection)

Bundesamt für Sicherheit in der Informationstechnik -Schutzbedarfskategorien: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Schutzbedarfsfeststellung/Schutzbedarfskategorien/Definitionen/definitionen_node.html (letzter Aufruf: 06.05.2013) - Take care standard will change, e.g.. BSI 200-2 (Juli 2017)

Der Hessische Datenschutzbeauftragte: Der behördliche und betriebliche Datenschutzbeauftragte nach neuem Recht (Stand Juni 2017) (Web-Site)

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK): Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele (V.1.0 – Erprobungsfassung) 9. und 10. November 2016

Das Standard-Datenschutzmodell: Entwurf Maßnahmenkatalog (in private communication)

EU - Veröffentlichung der **EU-DSVGO im Web (dt. Fassung)**:
http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=EN

Forum Privatheit und selbstbestimmtes Leben in der digitalen Gesellschaft: Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz (White Paper) unter: https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf, veröffentlicht 17.03.2016 (letzter Aufruf: 21.03.2017)

WP 248 (in process, working title): Guidelines on Data Protection Impact Assessement (DPIA) and determining whether processing is „likely to result in a high risk“ for the purposes of Regulation 2016/679