GDPR – Data Protection and Privacy for EU Projects

Dipl.-Jur. Univ.
Gernot Kirchner
Data Protection Officer of the CUT

Privacy protects no data, but the dignity and personality of each individually affected person.

Data protection is human protection!

Structure

1. Presentation of the data protection officer
2. Legal framework in data protection
3. Data processing principles
4. Data protection for E-Learning
5. Rights of the data subject, Art. 12 et seqq. GDPR
6. Personal data breaches
7. Technical and organizational protection measures
8. Your questions / discussion

Presentation of the data protection officer

Dipl.-Jur. Univ. Gernot Kirchner

phone: +49 371 531-12030
fax: +49 371 531-12039
email: datenschutzbeauftragter@tu-chemnitz.de
address: Straße der Nationen 62, 09111 Chemnitz
room: R. 1/184c (new: A10.184.3)

Presentation of the data protection officer

Dipl.-Jur. Univ. Gernot Kirchner

1990: born in Schlema, married, two children

2014: study graduation: first legal state examination

until 2015: research associate at JLU Giessen

until 2019: research associate at TU Chemnitz

since 1st March 2019: data protection officer of CUT

furthermore speaker and lecturer inter alia for
Saxon Administration and Business Academy, Chamber of Commerce and Industry Chemnitz, Chamber of Trade Chemnitz, Economic Development Erzgebirge etc.

Data protection officer of the CUT

- Non-directive **contact person / contact point**
- **Support and advice** (confidentiality)
- Explanation and specification of legal requirements
- **Data protection management**: allocation of responsibilities, risk assessments, awareness and training, controls, use of "privacy-friendly" technologies, IT security etc.
- **Proof / documentation requirements**, i.a. consultancy during carrying out a data protection impact assessment
- Support in the implementation of the **rights of data subjects**
- **Monitoring** compliance with legal requirements, internal regulations and the functioning of data protection management

(Independent) Saxon Data Protection Officer

Responsible supervisory authority in the Free State of Saxony pursuant to Art. 51 GDPR, §§ 14 ff. SächsDSDG:

Mr. Andreas Schurig
Devrientstraße 5
01067 Dresden
email: saechsdsb@slt.sachsen.de
phone: +49 351 85471-101
fax: +49 351 85471-109
web: https://www.saechsdsb.de/

Monitoring the application of data protection regulations

Protection of fundamental rights and fundamental freedoms of individuals during processing

Facilitating the free movement of personal data in the European Union

Structure

1. Presentation of the data protection officer
2. **Legal framework in data protection**
3. Data processing principles
4. Data protection for E-Learning
5. Rights of the data subject, Art. 12 et seqq. GDPR
6. Personal data breaches
7. Technical and organizational protection measures
8. Your questions / discussion

Legal framework in data protection

- Article 8 (1) of the Charter of Fundamental Rights of the European Union
- Article 16 (1) of the Treaty on the Functioning of the European Union
- Right to Informational Self-determination / General Personality Law, Article 1 (1), Article 2 (1) German Constitution
- Article 33 Constitution of the Free State of Saxony

Legal framework in data protection

- GDPR (General Data Protection Regulation)
- BDSG (Federal Data Protection Act)
- SächsDSG (Saxon Data Protection Act)
- SächsDSDG (Saxon Data Protection Implementation Act)
- SächsHSFG (Saxon University Freedom Law)
- SächsHSPersDatVO (Saxon University Personal Data Regulation)
- Tele Media Law (TMG), Telecommunication Law (TKG), Art Copyright Law (KunstUrhG), Criminal Code (StGB), etc.

Legal framework in data protection

- GDPR (General Data Protection Regulation) -

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**)

since 25th May 2018:
general applicable, binding in its entirety, directly applicable in all Member States

Legal framework in data protection

- GDPR (General Data Protection Regulation) -

This Regulation applies to the **processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union**, regardless of whether the processing takes place in the Union or not.

= general data protection rules for all controllers/processors in the whole EU

but: only compromise between all 28 EU Member States

Legal framework in data protection

- GDPR (General Data Protection Regulation) -

– Protection of natural persons (data protection is human protection)

– **Processing of personal data:**
… Information referring to identified / identifiable natural person (data subject)
  – an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier or to one or more factors specific to his/her identity
  – For example: last name, first name, date of birth, age, marital status, address, place of residence, telephone number, email address, IP address, identification number, social security number, bank account number, location data, online identifier etc.
  – Attention: special categories of personal data – processing in principle prohibited (Art. 9, 10 GDPR: for example health data, personal data, social data, biometric data, etc.)

Legal framework in data protection

- GDPR (General Data Protection Regulation) -

– **Anonymous information:**
… information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

– GDPR **does not concern** the processing of such anonymous information, including for statistical or research purposes.

Legal framework in data protection

- GDPR (General Data Protection Regulation) -

- … applies to the processing of personal data wholly or partly **by automated means** and to the processing **other than by automated means** of personal data which form part of a **filing system** or are **intended to form part** of a filing system.
- … 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

- **Controller in the meaning of Art. 4 (7) GDPR: CUT (or joint controllers)**
  - But: independent obligation of all members and project partners of CUT

Structure

1. Presentation of the data protection officer
2. Legal framework in data protection
3. **Data processing principles**
4. Data protection for E-Learning
5. Rights of the data subject, Art. 12 et seqq. GDPR
6. Personal data breaches
7. Technical and organizational protection measures
8. Your questions / discussion

Data processing principles

Data protectors can not protect data, they can at most control whether data is adequately protected.

Joachim Gauck
(former Federal President)

lawfulness

- purpose limitation
- data minimisation
- accuracy
- storage limitation

transparency

- information / access to personal data
- right to be forgotten
- right to object
- right to data portability
- responsibility / accountability

security

- technical and organisational measures
- Data protection impact assessment
- confidentiality
- integrity
- Notification duty

Data processing principles

***** Accountability *****
Attention: If you can not prove opposite, you are guilty.
(e.g. material and immaterial damages, fines)

Art. 5 Abs. 2 GDPR:

be able to demonstrate compliance with data processing principles

Art. 24 Abs. 1 GDPR:

ensuring compliance with the GDPR (evaluation, actualisation)

Art. 30 GDPR:

records of (all) processing activities

- **Accountability**
  - … controller is responsible for, and able to demonstrate compliance with data protection rules
  - **Data Protection Management System**
    … controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with data protection rules

Data processing principles

- **lawfulness**
  - … processed lawfully, that means you need **in each case a legal permission**
  - prohibition with permission reservation, Art. 6 GDPR
    - consent to the processing of personal data for one or more specific purposes
      … means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
    - necessary for the performance of a (pre-)contract to which the data subject is party
    - necessary for compliance with a legal obligation
    - necessary in order to protect vital interests
    - necessary for the performance of a task carried out in the public interest or in the exercise of official authority
    - necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data

Data processing principles
- lawfulness of surveys (1) -

– in principle: pseudonymized personal data
  – no necessity of identification of data subjects for the purposes – anonymization mandatory

– permission for processing: consent for one or more specific purposes (Art. 7 GDPR)

– furthermore: Information duty if collected from the data subject (Art. 13 GDPR)

Data processing principles
- lawfulness of surveys (2) -

- furthermore: Record of processing activities (Art. 30 GDPR)
  - in particular: technical or organisational measures to ensure data security
  - Storage limitation according Safeguarding Good Scientific Practice: “Primary data as the basis for publications should be kept on durable and secure media in the institution where they were created for ten years.”
- furthermore: Data protection impact assessment (Art. 35 GDPR, if required)
- furthermore: binding contract with processor (Art. 28 GDPR, if required)

Attention: transfers to third countries or international organisations (e.g. Google Forms) in principle not allowed – you have to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined, see Art. 44 et seqq.

Data processing principles

- **transparency (principle of good faith)**
  - … It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.
  - … to provide any information and communication relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language

Data processing principles

- **purpose limitation (data minimisation)**
  - … collected for specified, explicit and legitimate purposes
  - … not further processed in a manner that is incompatible with first purposes
  - … adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
  - … kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation)
  - … does not take place if purpose can reasonably be achieved by other milder means

Data processing principles

- Necessity -

A processing of [...] personal data is only required if the respective task **can not be fulfilled or not completely fulfilled without the specific date**. This also means that the task could otherwise be met only with disproportionately great difficulties, with an unreasonably higher effort or late. A data collection "in stock" is inadmissible. Necessity presupposes appropriateness, that is, data that are not at all suitable for achieving the processing objective are therefore not required. In particular, the option of **anonymisation and pseudonymisation** should be used. On the system side, precautions must be taken to ensure that the data is deleted at the earliest possible date, or at least that the personal reference can be removed by anonymisation or loosened by pseudonymisation.

Source:
„Datenschutzgerechtes eGovernment“, https://www.bfdi.bund.de/SharedDocs/Publikationen/PM29-04HandreichungDatenschutzgerechteseGovernment.html

Data processing principles

- **accuracy**
  - … accurate and, where necessary, kept up to date
  - … every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

- **data security (integrity and confidentiality)**
  - … processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Structure

1. Presentation of the data protection officer
2. Legal framework in data protection
3. Data processing principles
4. **Data protection for E-Learning**
5. Rights of the data subject, Art. 12 et seqq. GDPR
6. Personal data breaches
7. Technical and organizational protection measures
8. Your questions / discussion

Data protection for E-Learning

- **Legal basis:** GDPR and TMG (Tele media Act)

- **Permission for E-Learning:**
  - § 14 TMG / Art. 6 Abs. 1 S. 1 lit. b) GDPR: stock data
    … collect and use the personal data of a user insofar as they are necessary for the establishment, content or modification of a contractual relationship
  - § 15 (1) TMG / Art. 6 Abs. 1 S. 1 lit. b) GDPR: usage data
    … collect and use the personal data of a user, as far as this is necessary in order to enable and bill the use of tele media
  - § 15 (3) TMG / Art. 6 Abs. 1 S. 1 lit. f) GDPR: usage profiles
    … for the needs-based design of the tele media using pseudonyms, provided that the user does not object […] must inform the user of his right of objection […] usage profiles may not be merged with data about the bearer of the pseudonym

further information: Datenschutz bei E-Learning –Plattformen, July 2014,
https://www.dfn.de/fileadmin/3Beratung/Recht/handlungsempfehlungen/Datenschutz_bei_E-Learning-Plattformen.pdf

Data protection for E-Learning

- **Conclusion:** consent for one or more specific purposes (Art. 7 GDPR)
  … means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

- furthermore: transparency - information duty (Art. 13 GDPR)
- furthermore: Record of processing activities (Art. 30 GDPR)
  - in particular: technical or organisational measures to ensure data security
- furthermore: Data protection impact assessment (Art. 35 GDPR)

Data protection for E-Learning

– furthermore: binding contract with processor (Art. 28 GDPR, if required)

  – … the controller shall use only processors providing **sufficient guarantees** to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject

  – processes only on **documented instructions** from the controller
  – in principle: authorised persons have committed themselves to **confidentiality**
  – assists controller by **technical and organisational measures** and in ensuring his/her **compliance**
  – **deletes or returns** all the personal data to the controller after the end of the provision
  – allow for and contribute to **audits, including inspections**

Data protection for E-Learning

- furthermore: no transfers to third countries (e.g. YouTube), Art. 44 et seqq.
  - Recommendation: establishment of an own E-Learning-Platform in the EU

- furthermore, please remember:
  - strict necessity of processing personal data
  - data minimisation, in particular pseudonymization/anonymization (e.g. usage data)
  - privacy by design and default (Art. 25 GDPR)
  - concepts for extinction
  - technical and organisational measures to ensure data protection and security
  - etc.

Structure

1. Presentation of the data protection officer
2. Legal framework in data protection
3. Data processing principles
4. Data protection for E-Learning
5. **Rights of the data subject, Art. 12 et seqq. GDPR**
6. Personal data breaches
7. Technical and organizational protection measures
8. Your questions / discussion

Rights of the data subject, Art. 12 et seqq. GDPR

- Information duty when collecting personal data (Art. 13, 14 GDPR)
- Right of access, including copy of the personal data (Art. 15 GDPR)
- Right to rectification (Art. 16 GDPR)
- Right to erasure ('right to be forgotten') (Art. 17 GDPR)
- Right to restriction of processing (Art. 18 GDPR)
- Notification obligation regarding rectification or erasure of personal data or restriction of processing (Art. 19 GDPR)
- Right to data portability (Art. 20 GDPR)
- Right to object (Art. 21 GDPR)
- Prohibition automated individual decision-making, including profiling (Art. 22 GDPR)

Rights of the data subject, Art. 12 et seqq. GDPR

The controller shall provide information on action taken on a request under Articles 15 to 22 GDPR to the data subject **without undue delay** and in any event **within one month** of receipt of the request. That period may be extended **by two further months** where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request **by electronic form** means, the information shall be provided by **electronic means where possible**, unless otherwise requested by the data subject.

63. Recital, s. 4: Where possible, the controller should be able to **provide remote access to a secure system** which would provide the data subject with direct access to his or her personal data.

Structure

1. Presentation of the data protection officer
2. Legal framework in data protection
3. Data processing principles
4. Data protection for E-Learning
5. Rights of the data subject, Art. 12 et seqq. GDPR
6. **Personal data breaches**
7. Technical and organizational protection measures
8. Your questions / discussion

Personal data breaches

… means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Attention:
72-hours-notification-deadline to the supervisory authority
from Monday to Sunday

Personal data breaches

- Examples -

- Unintentional loss of USB-stick, laptop, other file storage devices or devices with personal data
- Dispose of personal data contrary to the law, e.g. dispose in trash (uncrushed), insecure storage of personal data
- Loss of personal date because of hacker-, phishing-attacks or malicious software
- Unencrypted mail transfer of sensitive personal data
- Disclose personal data without permission, e.g. email transfer in “cc” instate of “bcc”, disclose on websites, Online-Calendar (e.g. Google), use of Doodle, Dropbox, etc., private email accounts
- Loss or misdirection of post with personal data
- Unintentional delete or destroy of personal data
- Access to databases by unauthorised persons

Personal data breaches

- What should I do? -

- Immediate measures to protect humans and to stop the breach
- documentation about the breach, i.a. storing of all evidences
- (internal) notification to the Data Protection Officer
- Risk assessment by Data Protection Officer/controller
  - Severity of possible damages
  - Probability
- Notification to supervisory authority within 72 hours, Art. 33 GDPR
- Possibly notification to data subject, Art. 34 GDPR

Personal data breaches

- Why should I notify every breach to the Data Protection Officer? -

- Earliest possibility for Data Protection Officer to get knowledge about breach
- Data Protection Officer can assess risk / danger
- Minimization of negative impacts because of the publicity (storing evidences)
- Precautions in corporation with Data Protection Officer, supervisory authority
- Compensation of information asymmetry, i.a. to data subjects
- Prevention: incentive to avoid further breaches
- Duty because of the employment at Chemnitz University of Technology

Personal data breaches

- Own responsibility of each controller! -

- Attention: supervisory authority can also impose fines on individuals
- Employee are not privileged concerning data processing
- Fines up to 20.000.000 EUR (Art. 83 GDPR)
- Administrative offense pursuant to § 22 (1) SächsDSDG (up to 25.000 EUR)
- Criminal offense pursuant to § 22 SächsDSDG (up to two years imprisonment)
- Civil claims e.g. pursuant to employment

Structure

1. Presentation of the data protection officer
2. Legal framework in data protection
3. Data processing principles
4. Data protection for E-Learning
5. Rights of the data subject, Art. 12 et seqq. GDPR
6. Personal data breaches
7. **Technical and organizational protection measures**
8. Your questions / discussion

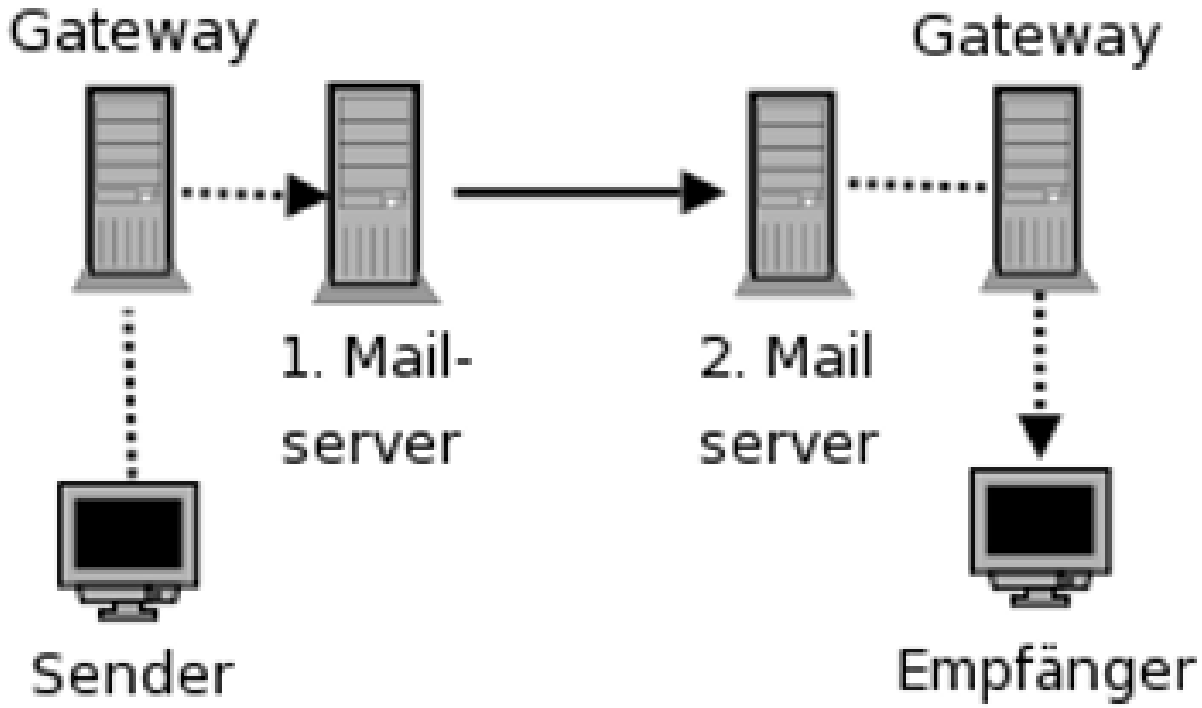
Technical and organizational protection measures

- Elementary danger situation -

- Spying out information
- Disclosure of sensitive information
- Violation of laws or regulations
- Unauthorized / Incorrect use or administration of devices and systems
- Abuse of permissions or personal data
- Social engineering
- Data loss
- Loss of integrity of sensitive information
- Etc.

Technical and organizational measures

- Private email account (e.g. Google, Yahoo, Microsoft) -



Source: https://www.privacy-handbuch.de/handbuch_31c.htm

Technical and organizational measures

- Software, applications etc. -

- **Doodle**: Scheduling appointments together with Content Delivery Network-Service “Cloudflare, Inc.” (USA)
  - alternative: DFN-terminplaner 4.0 (https://terminplaner4.dfn.de/)

- **Dropbox**: Sharing documents together with USA (California, San Francisco)
  - alternative: TUCcloud (https://www.tu-chemnitz.de/urz/storage/cloud/)

Technical and organizational measures

- Software, applications etc. -

- **Skype**: videoconferences together with Microsoft Corporation (USA)
  - alternative: TUC-Videoconference-Systems; DFN-proved Software-Clients; web based videoconferences with “Adobe Connect” and “Cisco WebEx” (https://www.tu-chemnitz.de/urz/vidcon/web.html)

- **Trello**: project management together with Content Delivery Network-Service “Akamai Technologies Inc.” (USA)
  - alternative: data hosting in EU (e.g. “factor” or “taskworld”)

Technical and organizational measures

- Software, applications etc. -

- **WhatsApp**: personal communication together with Facebook Inc. (USA)
  - alternative: external messenger services always processors in the meaning of Art. 28 GDPR (i.a. binding contract mandatory)
  - therefore: official email account (e.g. …@phil.tu-chemnitz.de)

- **Website "tefl-epal.com"**: together with Hostgator / WebsiteWelcome.com (USA)
  - alternative: Web space from Chemnitz University of Technology or EU-provider

Structure

1. Presentation of the data protection officer
2. Legal framework in data protection
3. Data processing principles
4. Data protection for E-Learning
5. Rights of the data subject, Art. 12 et seqq. GDPR
6. Personal data breaches
7. Technical and organizational protection measures
8. **Your questions / discussion**

Your questions / discussion

Thank you very much for your attention!

Dipl.-Jur. Univ. Gernot Kirchner

phone: +49 371 531-12030
fax: +49 371 531-12039
email: datenschutzbeauftragter@tu-chemnitz.de
address: Straße der Nationen 62, 09111 Chemnitz
room: R. 1/184c (new: A10.184.3)