What data protection is all about (and what has changed with the GDPR)

Walter Scholger
Zentrum für Informationsmodellierung
Austrian Centre for Digital Humanities
Karl-Franzens-Universität Graz
walter.scholger@uni-graz.at

Agenda

- General Data Protection Regulation
  - Applicability
  - Terms and definitions
  - Data Protection principles
  - Rights of data subjects
  - Privileges for research and education

- Examples (courtesy of University of Graz)
  - Consent form for interviews etc.
  - Consent form for Mailing Lists
  - Show Case: TEI-C Conference 2019

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

Article 8 - Protection of personal data

(1) Everyone has the right to the protection of personal data concerning him or her.

(2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

General Data Protection Regulation (GDPR)

- Regulation ≠ Directive
- 69 opening clauses
- 99 items
- 173 recitals
- in force since 24 May 2016
- directly applicable EU law as of 25 May 2018
- Implemented in national Data Protection Act amendments

Want to know more?

- ✓ GDPR Website (EU): https://gdpr-info.eu/
- ✓ GDPR on EURLEX https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
- ✓ CLARIN Legal Issues Committee White Paper https://www.clarin.eu/sites/default/files/CLIC_White_Paper_3.pdf

Applicabilty

This 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 (Art. 2).

Not applicable for data processing:

… by a natural person in the course of a purely personal or household activity

… 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.

Processing

… processing means 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

Cross-border transfer of personal data possible:

… in the European Union

… with third countries ensuring an adequate level of data protection

… if the data subject has explicitly consented

Personal Data

… personal data means any information relating to an identified or 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 such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

natural person = living person

Sensitive Data

- The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data clearly identifying a natural person, data concerning health, sex life or sexual orientation of a natural person is prohibited.

- Exceptions: explicit consent, data made public, protection of vital interests of the person or other persons (conditional: health care, science)

Anonymisation vs. Pseudonymisation

- Anonymisation

  … no longer identifiable at general discretion and taking all feasible means into account

  = not subject to GDPR!

- Pseudonymisation

  … means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information

Roles

Controller

… the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

Processor

… a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Data Subject

… a natural person, whose data is processed

Principles (Art 5)

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality
- accountabiliy

Lawfulness

- With the consent of the person concerned (for sensitive data: express consent!)
- Contract with data subject
- Compliance with legal obligations (e.g. social security)
- Safeguarding the legitimate interests of the person responsible or of a third party, provided that the interests of the person concerned do not outweigh each other.
- In "good faith" (What should the data subject reasonably expect in the case of lawful processing?)
- Transparency (information duties)

Purpose limitation

- Establishment of a clear and legitimate purpose (research exception: wider agreement).

Data minimisation

- Only collect the data necessary for processing.

Accuracy

- Data must be factually correct and up-to-date.

Storage limitation

- storage as long as necessary for the achievement of purpose (legal retention periods, internal reporting, archivability)
- Research exception: as far as no time limits are foreseen, unlimited!

Integrity

- Ensure "security by design" (i.e. through appropriate technical and organizational measures like access control ...)
- Information and training of employees!

Accountability

- Compliance with the aforementioned principles must be proven

Rights of the data subject (Art. 12-23)

- Information (at data collection)
- Access
- Rectification
- Erasure (right to be forgotten)
- Restriction of processing
- Data portability
- Objection

Right to information

- the processing purposes
- the categories of personal data to be processed
- the recipients or categories of recipients, in particular recipients in third countries or international organisations
- if possible, the envisaged duration for which the personal data will be stored (or criteria for determining this duration)
- the existence of a right to rectify or erase personal data relating to them, to limit the processing to be carried out by the controller and to object
- the existence of a right of appeal to a supervisory authority
- where the personal data are not collected from the data subject, any available information as to the source of the data
- a copy of all data!

Specific processing situations

Article 85:

For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations […] if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

Article 86:

… public access to official documents

Article 88:

… in the context of employment

Article 89

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Union or Member State law may provide for derogations from the rights [of access, rectification, restriction of processing or the right to object] (...) in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes (…), providing that appropriate safeguards are applied.

Article 89

- data minimisation is applied fully
- broad consent: the possibility of obtaining consents not only for the specific purpose, but for one or more research areas
- purpose extension: research is always "compatible purpose"
- storage extension: no limitation for duration
- erasure limitation: not applicable if the exercise of this right "is likely to render impossible or seriously impair" the achievement of the purposes of the research.

But: "appropriate safeguards"

- Pseudonymisation, transparency, opt-out policies, …
- Data management plans, codes of conduct, ethics commission

Show Case: Consent Form (generic)

"I consent to the processing of my personal data, specifically my [*insert specific categories of data, e.g. registration details, examination details, and specific categories of data, e.g. name, address*] for [*insert the purpose(s) for which the data will be used, e.g. organising events, sending newsletters, admissions procedures*] by the University of Graz. *[extend if necessary to include transmission of personal data]** This consent [*where more than one purpose of use is given, it should be clear that consent for each one may be withdrawn individually*] can be withdrawn at any time without explanation by emailing [*insert email address*]. Withdrawing consent does not affect the legality of earlier processing.

You can find our data protection declaration [*at the following link…/in the attachment*].

Show Case: Consent Form (E-Mail)

Dear Newsletter recipient,

The new provisions of the General Data Protection Regulation started to apply on 25 May 2018. If you would like to continue receiving our XYZ newsletter, please confirm this explicitly by clicking the link below/by replying to this email, after reading our Data Protection Declaration for newsletters (see link or attachment).

By confirming this you are giving consent for the University of Graz to process your personal contact details, your email address, first name and last name, in order to be able to send you the newsletter. This consent can be withdrawn at any time without explanation, by emailing xyz@uni-graz.at.
The legality of processing your personal data between the time of this consent and the time it is withdrawn, remains unaffected by any such withdrawal of consent.

If we do not receive your confirmation, you will no longer receive the XYZ newsletter.