GDPR report

Brussels, 12th June 2018

Matthias Pocs, Contributor

Data protection principles (1)

- Lawfulness (incl. consent)
  - Types of data processing must be based on legal acts.
  - Example: use cases with consent and ‚vital interest'
- Profiling prohibition, data accuracy
  - Avoid automatic decisions to be taken for granted without sufficient human verification .
  - Data must be accurate and regularly updated.
  - Example: no analytics planned
- Data availability
  - The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons of data protection
  - Example: no restriction of use of health data beyond GDPR requirements
- Purpose limitation
  - Data must be processed only for specified and non-incompatible purposes.
  - Example: purpose spec' in use case, policies/user rights def', third party uses for improvement of services (data protection, etc.)?
  - Conditions and safeguards for special categories of information must be observed or taken
  - Example: all exchanged data considered sensitive incl' metadata (e.g. existence of records in certain category of healthcare organisation)

Data protection principles (2)

- Data security (in the sense of data protection law)
  - Data must be processed with a level of security appropriate to the risks for the patients and other data subjects
  - Example: role-based access control security mechanism applied to the IPS (see ISO 22600-1: 2014, ISO 22600-2:2014)
- Data subject rights
  - Data must be processed in a transparent („who processes what when“) manner
  - Example: audit trail, checks in relation to NCP and data requestor
  - Patients and other data subjects must be able to know, correct and delete their data
  - Example: consent mgt' ("I'd like to be notified if data shared"), correction/deletion at data source's organisation (or read only), see also WP29 guidance on epSOS and EHR (WP189, WP131)
  - Data portability: ... able to receive and transmit their data (see also previous slide on data availability)
  - Right to be forgotten: ... across controllers.

Data protection principles (3)

- Data minimisation
  - Amount of data (categories) must be reduced given the purposes
  - Example: IPS reduces data categories compared to EHR (see also prEN 17269, draft prTS 17288, CEN-HL7 impl guidance)
  - Data must be deleted as soon as possible given the purposes
  - Example: IPS persist or no permanent storage
  - Data subjects must be able to be anonymised
  - Example: identification of data categories and techniques (see terminology ISO-IEC/DIS 20889, WP29 Opinion 05/2014 on Anonymisation Techniques (WP 216), use of unlinkability levels (e.g. ISO/IEC WD2 27551, section 7.5, table 2)
- Responsibility
  - System user rights must be enforced per „controller“/„processor“
  - Example: identif‘ of stakeholders like GPs, hospitals, cloud operators, NHS

New GDPR principles (1)

- Risk-based approach
  - Controllers must be able to take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing
  - Example: conformance to standards ("state of the art"), use cases (scope, context, purposes) defined, threat analysis from data subject's point of view, decentralised architecture (e.g. OpenNCP at EU level)
  - Concerning "rights and freedoms" use EU Charter of Fundamental Rights (see following two slides)
- *(New GDPR principles cont'd on slide 8)*

Fundamental rights (1)

- Charter = Charter of Fundamental Rights of EU
- See also CRISP Project's CEN-CENELEC Workshop Agreement 17147:2017

- Fair decision-making
  - According to paragraph 2 of Article 8 of the EU Charter data must be processed fairly.
- Privacy and data protection
  - According to Articles 7 and 8 of the EU Charter people have the right to protection of their privacy and personal data.
- Consent and autonomy
  - As mentioned above the second paragraph of Article 8 of the EU Charter personal data must be processed on the basis of the consent of the person concerned or some other legitimate basis laid down by law.
- Non-discrimination
  - The Charter includes general and specific non-discrimination requirements.
- Human dignity
  - Article 1 of Charter states that human dignity is inviolable and must be respected and protected.

Fundamental rights (2)

- Public health & access to health care
  - The Charter guarantees in Article 35 the fundamental right of access to preventive health care and the right to benefit from medical treatment under the conditions established by national laws and practices.
  - According to the first paragraph of Article 168 of the TFEU a high level of human health protection shall be ensured in the definition and implementation of all European Union policies and activities.
- Proportionality and mission creep
  - Article 52 of the Charter stipulates that any limitation on the exercise of the rights and freedoms recognised by the Charter must be proportionate.
    - limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.
  - Accordingly, the benefits for health care must be balanced with the impact on the rights and freedoms of patients.
  - The principle of proportionality includes the prevention of mission creep, also referred to as “function creep,” by taking precautions against misuse of technology originally intended for a legitimate use.

New GDPR principles (2)

- *(New GDPR principles slide 5 cont'd)*
- Accountability
  - Controllers must be able to demonstrate compliance with data protection requirements
  - Example: dedicated effort concerning 'demonstration of compliance', elements such as DPMS, 'provenance', e.g. tracking of composition and access of EHR (see also ISO/AWI 22697)
- Certification
  - An approved certification mechanism may be used as an element of 'demonstrate of compliance'
  - Example: something like Continua certification but for privacy topics

New GDPR principles (3)

- Data protection by design
  - Controllers must be able to implement measures during operation but also as early as at the time of the determination of the means for data processing
  - Example: changes at design time in eH dev and standardisation projects (see also CEN-CLC/JTC 8 EN DPbDbD 1st draft (N 129), clause 5.1)
  - Controllers must be able to implement pseudonymisation (in the sense of data protection law)
  - Example: identifiability/sensitivity analysis (see also EN-ISO 25237:2017)
  - Controllers must be able to demonstrate the effectiveness and integration of the pseudonymisation and other DPbD measures
  - Example: design-time documentation, planning for monitoring and compliance assurance, piloting/testing of pseudonymisation, use objectives from standards

Results incorporated in this contribution received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 727301 (SHiELD Project).