Presentation made at the:
Council of Europe mid-term evaluation
of the Strategy for the Rights
of the Child (2016-2021)

High level conference
Strasbourg 13-14 November 2019

COUNCIL OF EUROPE

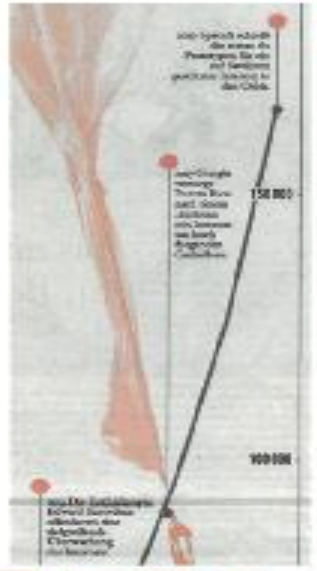
CONSEIL DE L'EUROPE

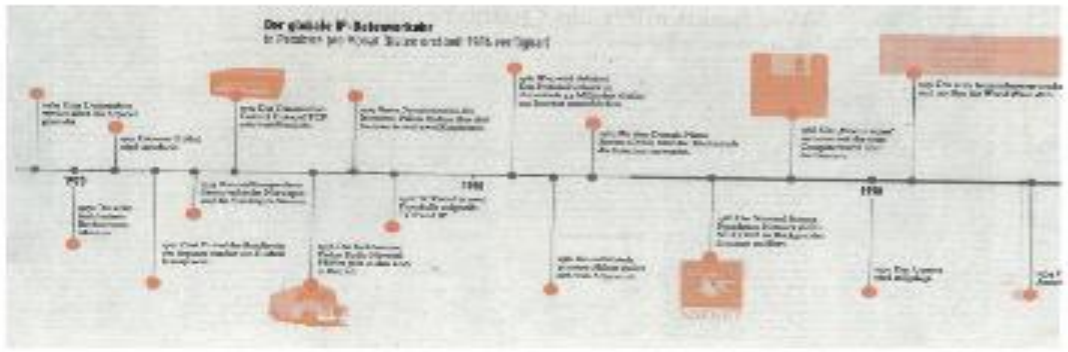
Reflection on a GDPR-compliant application of Microsoft Office 365 in schools

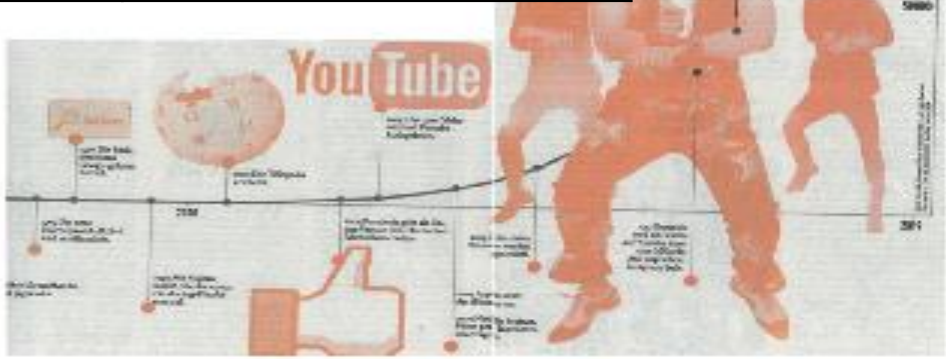
Dipl.-Inform. Julia Stoll
Head of the IT Unit 3.2
The Hessian Commissioner for Data Protection and Freedom of Information
Gustav-Stresemann-Ring 1, 65189 Wiesbaden, Germany
Fon: +49 611 14 08 150
Mail: julia.stoll@datenschutz.hessen.de

50th Anniversary of the Internet: The global IP-traffic

1969 (-1990)	Data packages via APRA Net	
1978	TCP is split into TCP and IP	
1983	Domain Name System (DNS) [like yellow pages]	
1994	Amazon is founded as an Online Shop	
1997	Search engine Google goes online	
2005	YouTube is established	
2012	YouTube video: 1 Billion clicks (Gangnam Style)	
2013	Edward Snowden	100‘000 Pbytes/month
2019	SpaceX: 60 satellites	150‘000 Pbytes/month







P. Heller: Ein halbes Jahrhundert im Internet – Das Netz der Netze wird 50. Die Macht, Dinge zu verändern, steckt von Anfang an in seiner Struktur. Doch auch die wandelt sich gerade. Frankfurter Allgemeine Sonntagszeitung, 26.10.2019, 43, p. 58-59

Prohibition with reservation of authorization and further preconditions for processing personal data

- The collection, procession and use of personal data are only permissible in accordance with the General Data Protection Regulation (GDPR), local data protection laws and specific laws, requiring a legal basis also including the consent of the data subject.
  - Clear definition of ‘personal data’ required
  - Characteristics of ‘consent’ with respect to data protection principles
- Personal data must be protected by appropriate technical and organizational measures, including
  - Purpose limitation, data minimization, storage limitation
  - Integrity, confidentiality, availability and resilience of processing systems and services
  - Accuracy, accountability
  - State of the art [of technology, J.S.], cost of implementation and the nature, scope, context and purposes of processing as well as the risks for rights and freedoms of natural persons

GDPR-article with respect to technical aspects

Article	Significance
Art. 5 & Art. 6 GDPR	Principles and lawfulness of processing personal data
Art. 7 & Art. 8 GDPR	Conditions for consent and child's consent in relation to information society services
Art. 9 GDPR	Special categories of personal data
Art. 30 GDPR	Records of processing activities
Art. 25 GDPR	Data protection by design and by default
Art. 32 GDPR	Security of processing
Art. 35 (& Art. 36) GDPR	Data protection impact assessment (and prior consultation)
Art. 42 (& Art. 43) GDPR	Certifications (and accreditation of certification bodies)
Art. 40 (& Art. 41) GDPR	Codes of conducts (and monitoring of approved code of conduct)

Reflection on a GDPR-compliant application of Office 365 in schools

- System architecture(s)
  - Internet: Hardware-based infrastructure,
  - Web: Software-driven infrastructure,
  - Component-based infrastructures: Hardware-based or/and software-driven?
- Redefining the meaning of “controller” and “processor” on the basis of
  - Micro services,
  - Technical configuration of software services in distributed environments,
  - Profiling, like scoring and automated decision making
- Shift to “pure” software-driven services on top of the Internet (over the top services)
- Focus on data related to subjects (personal data)
  - Technical data and its meta data (usage data),
  - Content and its meta data
- GDPR and the urgently needed e-Privacy Regulation

What does it mean for Office 365 in schools?

- *Why should Office 365 be applied in schools?*
  - *This is no question of data protection, but the answer is needed as foundation for data protection assessment.*
- What kind of personal data is processed based on which legal foundation by whom in which role and in which environments (at what geographic locations) for what purposes?
  - For which data subjects is consent a valid legal foundation in schools?
- What are the resulting organizational and technical requirements?
- How are those implemented?

➔ **Is this GDPR-compliant on each level?!**

References

- EU (European Union) : Charter of Fundamental Rights of the European Union (EuCH) in **different languages** viewed 31 October 2019: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT
- EU: EU Regulation No. 679/2016 (GDPR) in **different languages** viewed 14 January 2019: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679
- EU: EU No. 680/2016 in **different languages** viewed 14 January 2019: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1547479546351&uri=CELEX:32016L0680
- EDPB (European Data Protection Board, former Art 29 Working Party): Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248 rev.01, adopted on 4 April 2017 and as last revised and Adopted on 4 October 2017) viewed 01 November 2019: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
- EDPB: *Guidelines 1/2018 on certification and identification criteria in accordance with Article 42 and 43 of the Regulation 2016/679* (03 June 2019, adopted – including Annexes) viewed 11 October 2019: *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf*
- ISO (International Organization for Standardization, 2005): *DIN EN ISO/IEC 17000 Konformitätsbewertung - Begriffe und allgemeine Grundlage.* Berlin, Beuth Verlag.
- ISO (2012): *DIN EN ISO/IEC 17065 Konformitätsbewertung - Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen akkreditieren.* Berlin, Beuth Verlag.
- ISO (2019): *ISO 27552 Information technology - Security techniques - Extention to ISO/IEC 27001 and ISO/IEC for privacy information management.* Berlin, Beuth Verlag.
- EU: **ePrivacy Regulation** (former: ePrivacy Directive No. 58/2002) viewed 11 October 2019, lex spezialis with focus on electronic communication and based on:
  - https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017PC0010&from=DE (erster Verhandlungsentwurf)
  - https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications (different languages)

Annex – Resources

Some basic terms in Art. 8 EU Charta (EuCH, Title II: FREEDOMS):
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 on other legitimate bases laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

→ Prohibition with reservation of authorization and further preconditions processing personal data

Some basic terms in the GDPR: **‘personal data’ and ‘consent’**

Art. 4 GDPR – Definitions
For the purpose of this Regulation:

(1) ‘personal data’ means any information relation 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, psychological, genetic, mental, economic, cultural or social identity of that natural person;

(11) ‘consent’ of the data subject means any freely given, specific, informed an unambiguous identification of the data subject’s wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Some basic terms in the GDPR:
Art. 6(1)(a) and (f) – Lawfulness of processing

(1) Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(f) processing is 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, in particular where the data subject is a child.

Some basic terms in the GDPR:
Art. 8 GDPR – Conditions applicable to child's consent in relation to information society services

(1) Where point (a) of Art. 6(1) applies, in relation to the offer of information society services directly to a child, the procession of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to extend that consent is given or authorized by the holder of parental responsibility over the child. Member States may provide by law a lower age for those purposes provided that such lower age is not below 13 years.

(2) The controller shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology.

(3) Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.