

University of Luxembourg

Multilingual. Personalised. Connected.

General introduction to GDPR and Research

Dr Sandrine Munoz, Data Protection Officer of UL



- **What is personal data?**
- **Upcoming changes with the GDPR**
- **Specificities for Research**
 - Key disposals in the GDPR
 - Luxembourg Projet of Law 7184
- **Next steps**



What is personal data?

- Personal data: any information relating to an identified or identifiable natural person (called “data subject”)
 - Examples: name, address, social security number, date of birth, photo, free text in an electronic document, criminal sanctions, political opinions, IP address, data about geo-tracking, health data, ... → *“account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person”*
- Any information = any format (electronic, paper...)
- Includes any sort of statement about a natural person
- Pseudonymised data is personal data interpretation
- Anonymised data is not personal data (strict legal)
- Our supervisory authority: the Commission Nationale pour la Protection des Données “CNPD” → controls/audits to come with the GDPR



Upcoming changes with the GDPR



- **Existing rights have been reinforced:**
 - Right to information about the processing of personal data
 - Right to object to processing activities
 - Right to erasure
- **GDPR introduces new rights:**
 - Data portability
 - Right to get information in case of a data breach
- **New consent on GDPR is more demanding**
 - To be evidenced
 - Freely given, specific, informed and unambiguous

→ statement or clear affirmative action
- **Consent of a parent/tutor for a child under 16
the age of 16**



- Last guidance of the WP29 about transparency
http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

Table of mandatory information at the end of the document

- Last guidance of the WP29 about consent

http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

Note that Recital (33) of GDPR

Consent can be given to certain areas of scientific research



- Art. 85 Processing and **freedom of expression and information**
- Art.86 Processing and **public access to official documents**
- Art. 89 **Safeguards and derogations** relating to the processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
- **Disposals in national laws expected to specify the balance between academic expression and data subjects rights**
- **Disposals in national laws expected to specify the derogations**



Strengthening individuals' rights: particular limitations for scientific or historical research or statistical purpose

- Draft law 7184 implementing the GDPR and containing disposals about derogations to data subjects' rights (art.57/58) for processing of personal data for purpose of scientific or historical research or statistical purposes if implementation of appropriate safeguards (pseudonymisation, encryption, data management....)
- Draft law 7184 mentioning freedom of academic expression, that means:
 - No prohibition for processing of specific categories of personal data such as political opinion, ethnic origin
 - No limitation for processing of data related to criminal sanctions under specific conditions
 - Derogation to the right of information if that would compromise the direct collection of the data or the project publication or the public availability of data



Strengthening individuals' rights: particular limitations for scientific or historical research or statistical purpose

- **Advice of the CNPD on 28/12/2017**
<https://cnpd.public.lu/fr/decisions-avis/2017/1050-PL7184-gdpr.html>
- **Advice of the Conseil d'Etat on 3rd of April**

<http://www.chd.lu/>

Remain informed on the next steps of the adoption process as the GDPR will enter into force soon



- **Accountability:** the GDPR introduces a legal accountability obligation
→ controller and processor are responsible to implement the GDPR and have to document such implementation and compliancy
- **Controller:** legal entity which determines the purpose and the means used for the personal data processing, who decides it
- **Joint-controllers:** controllers which jointly determines the means and the purpose of a personal data processing
- **Processor:** legal entity which acts on behalf of the controller
- **Obligations for processors:**
 - New obligations regarding security, confidentiality and accountability
 - Support to the controller to allow the compliant with certain obligations → insert specific disposals in agreements/contracts with the processor
 - New conditions for engagement of a sub-processor



- No more CNPD notifications-or authorisations
 - Compliancy must be documented
 - A **Register** for recording processing activities has to be developed
 - The assessment of personal data processing is based on the Register; if needed, helps to determine possible mitigations actions and for which processing a Data Protection Impact assessment is required
 - Data Protection Impact Assessment is a process designed to describe the processing, assess the necessity and proportionality of a processing and help manage the risks for rights and freedoms of natural persons resulting from the processing of personal data
- criteria provided to determine in which cases a DPIA is mandatory:



- Detect if your research project involves processing of personal data ASAP
- Check the legal basis of your processing
- Refer to the policies and guidance of your institution
- Foresee security measures to protect your personal data
- In case of data sharing check if you are authorised and if you have a proper agreement in place
- Check the measures to implement to respect the data subjects rights
- Check if your project involves transfer of personal data outside EU or EEA and appropriate safeguards are in place
- Be prepared for the personal data breach
- Do not hesitate to contact your DPO or CISO in case of questions or doubts



- Questions?
- Remarks?

