eTRIKS

European Translational Information and Knowledge Management Services

efpia

imi innovative medicines initiative


# Ensuring Compliance with Personal Data Protection Regulations in eTRIKS and Supported Projects

# Disclaimer

Data protection and data privacy are complex subjects that play a major role in the collection, storage and processing of data in biomedical research. This training course is designed to provide you with a basic understanding of privacy laws and regulations as generally applicable to research projects carried out in the EU. Although this course is not intended to provide legal advice or guidance on how you should act in every situation, it should help you to identify and avoid potential privacy breaches. For more detailed information on the applicable laws and the specific privacy practices of your institution, you should consult your legal department or your supervisor.

# Presentation Overview

- Introduction to Personal Data Protection
  - What are Personal Data?
  - Why is Data Privacy Important?
  - The Data Protection Legislation of the European Union
- The Code of Practice for the Secondary Use of Medical Data in European Scientific Research Projects
- Conclusion and Summary

# What are Personal Data?

# 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

*(Art. 4, General Data Protection Regulation)*


# Any Information = Any Statement

- Includes any sort of statement about a natural person
  - "**Objective**" information
    - Presence of a certain substance in one's blood
  - "**Subjective**" information, opinions or assessments
    - Employment (John Smith is a good worker and merits promotion)

- Example: drug prescription information

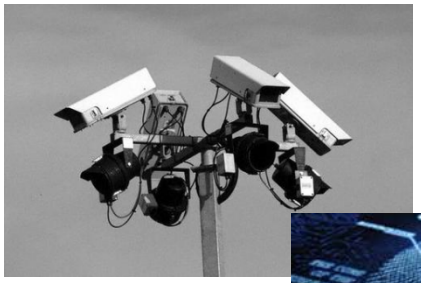
  Providing information about **prescriptions** written by a doctor to a pharmacist is communication of personal data

# Any Information = Any Format

- **All formats or media in whatever form**
  - Alphabetical, numerical, photographic, acoustic, etc.

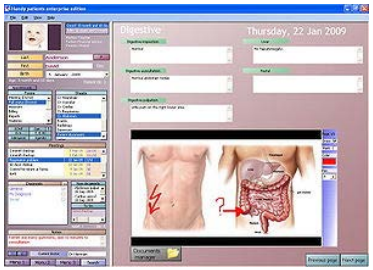
Examples:


  - Free text in an electronic document (e.g., e-mail)
  - Telephone banking
  - Video surveillance
  - Fingerprints and DNA data
    - Both an identifier and a content

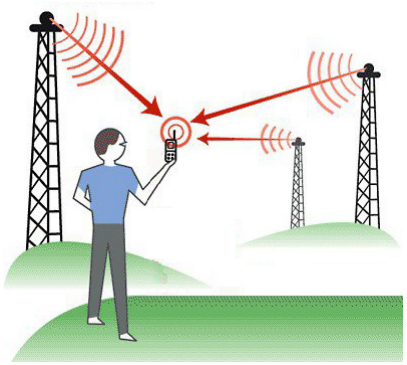


# Relating To = About Someone

- Information “relates” to a natural person when it is **about that natural person**
  - Employee documents in his personal file
  - Patient's medical records
  - Video surveillance images




- But also:
  - Credit card records
  - Car service records
  - Phone call log
  - Monitoring of phone position
  - Etc.



# Identified or Identifiable

- **Identified** ⇨ is "distinguished" from all other members of a group
- **Identifiable** ⇨ the natural person has not yet been identified, but it is possible to do it
- **Identification** is achieved through pieces of information

  e.g. height, hair colour, profession, function, date of birth, blood group, genetic variant

- Whether certain identifiers are sufficient to achieve identification is dependent on the **context**

  e.g. clinical trial versus phonebook

# Why is Data Privacy Important?

# Why is Data Privacy Important?

- Major risks for a person (also called “data subject”)
  - **Identity theft** and **Fraud**
  - **Discrimination**

- Serious **financial** & **individual** risks for non-compliance
  - Inability to perform research
  - Heavy fines / compensation for data subjects
  - Legal consequences / company officials liable to prosecution

- Potential damages to the **reputation and image** of a person or a company

# Identity Theft and Discrimination

- An estimated 15.4 million consumers in the U.S.A., about 6% of the adult population, suffered some form of identity theft in 2016*
- The majority experienced fraudulent use of credit card or bank account information: Total financial damage was about $16 billion
- Fraud can affect a person's credit rating
  - Ability to obtain a credit card
  - Inaccurate records can impair one's ability to do business

- Disclosure of health information can have negative impact on health insurance rates and employment

*link here

# Re-Use of Biological Samples and Associated Data – the Example of HeLa

- Data privacy and security is particularly important when dealing with health information.
- This has consequences for the use and re-use of data in biomedical research.
- The use of genomic data to identify a person's disease risk raises questions about maintaining anonymity of study participants
- Genomic data may, however, also present a privacy risk for relatives of a data subject
- In 2013, researchers posted online the sequenced genome of the first and most widely used human cell line called HeLa.

# Re-Use of Biological Samples and Associated Data – the Example of HeLa

- Since the identity of the tissue donor is known (Henrietta Lacks), her family raised concerns that publication of genomic data might reveal information about disease risk or other heritable traits among her descendants
- The National Institutes of Health met with members of the Lacks family and negotiated a policy for use of the genomic data from the HeLa cell line
  - This was reported in the New York Times (link here)
- The genomic data are now available under restricted access – requests for use are reviewed by a Data Access Committee that includes members of the family
  - For a report published in the journal Nature, follow this link

# Business & Image Damage

Inspection of a pharmaceutical company by the Italian Data Protection Authority (DPA) (2006)

- Conclusions published on the **Italian DPA website** mid-September 2008 (link here)
  - Company-controlled **processing of clinical trial data deemed not compliant** with Italian guidelines for clinical trials
  - Company required to stop clinical trials in Italy if not compliant before the end of the year
- The information was immediately published in major Italian **newspapers**, e.g. “La Stampa”

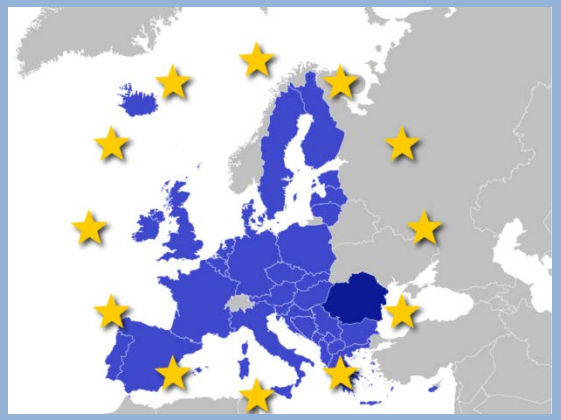
# Misuse of Personal Data in Social Media

Municipality of Milan and Associazione Vivi Down *versus* Google Italy

- A video was posted in Google Videos showing a disabled student (Down syndrome) being bullied and insulted
- Google Italy was charged with illicit processing of personal data for profit, with damage to the data subject
- Three **Google executives** were found guilty and sentenced to
  - 6 month suspended jail sentences
  - Legal costs
  - Publication in main newspapers

  - (link here to a description of the case)

# The Data Protection Legislation of the European Union



# Towards a Harmonisation of the Data Protection Legislation within the European Union (EU)

- **The Directive** 95/46/EC "on the protection of individuals with regard to the processing of personal data and on the free movement of such data (24 October 1995)"
  - The Directive forms the basis of current national or local data protection legislation in the EU, but some exceptions exist
- **The General Data Protection Regulation** (GDPR, Regulation 2016/679)
  - A **single set of harmonized rules** will apply to **all EU member states**.
  - The GDPR is a revision of the Directive with increased data protection measures
  - The GDPR will come into effect and replace the Directive on **25th May 2018**

# Scope of the EU Data Protection Regulation - 1

- The Regulation applies to the personal data of **natural persons**
  - **a natural person** is a living human being, with universal rights
  - The protection of their data is one of these universal rights

- The Regulation does not apply to
  - Personal data of **deceased persons**
  - Data of **legal persons**
  - The data protection laws applicable to deceased persons and to legal persons may vary among Member States of the EU

# Scope of the EU Data Protection Regulation – 2

The Regulation does NOT apply to the processing of **anonymous or anonymised data** (Excerpt from Recital 26, GDPR):

- The principles of data protection should apply to any information concerning an identified or identifiable natural person.
- Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.
- To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.
- To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

# Scope of the EU Data Protection Regulation – 3

The Regulation applies to the **processing of personal data:**

- **Processing** = collecting, recording, storing, holding, consulting, analysing, using…


- **Special categories** of personal data (**'sensitive data'**) under the GDPR [ see Article 9(1)] include:
  - racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership
  - **data concerning health** or sex life and sexual orientation
  - **genetic data (new)** and
  - **biometric data**, where processed to uniquely identify a person **(new)**

# Scope of the EU Data Protection Regulation – 4

- **Processing of sensitive personal data is prohibited, except under certain conditions**

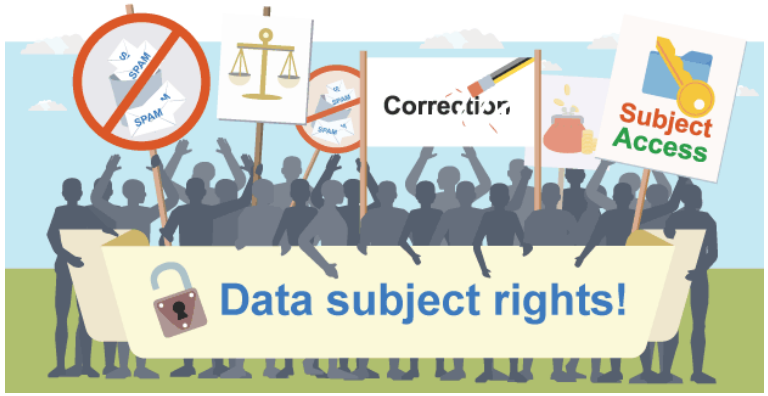
- The conditions most likely to apply to processing of data in biomedical research are:
  - 9(2)(a) – **Explicit consent of the data subject**, unless reliance on consent is prohibited by EU or Member State law, OR
  - 9(2)(j) - Necessary for archiving purposes in the public interest, or **scientific and historical research purposes** or statistical purposes in accordance with Article 89(1)

# Principles of the EU Data Protection Legislation

Personal data shall be:

- Fairly and **lawfully processed**
- Collected for **defined purposes**
- Adequate, relevant and **not excessive** in quantity
- Accurate and **up-to-date**
- **Not kept** for **longer** than necessary
- Processed **in line with the rights** of data subjects
- Kept **secure**
- **Not transferred** to other countries without adequate protection

# The Rights of the Data Subject




- The Right of Access
- The Right to be Informed
- The Right to Restrict Processing
- The Right to Object
- The Right to Rectification (NEW)
- The Right to Erasure (NEW)
  - Otherwise Known As The Right to Be Forgotten
- The Right to Data Portability (NEW)

# GDPR: Summary & Conclusions

## Objective of the GDPR:

One single data protection law for the EU

- Increased individual rights; increased obligations for processors
- Allows **free flow** of personal data **between Member States**
- **Forbids the flow** of personal data from EU **to third countries** not ensuring an adequate level of protection.
  (e.g., USA, China, Japan (waiver given under strict conditions)).
- The GDPR does not require that enabling legislation be passed by national governments
  - **50/99 articles have, however, scope for variance**
  - There will be differences in the laws enforced by Member States

# Developing our own Guidance:

A Code of Practice for the Secondary Use of Medical Data in European Scientific Research Projects

# Why Develop a Code of Practice?

- Develop a common framework to facilitate secondary use of medical data throughout the EU
  - Acceptable for EU collaborative research projects, IMI-JU, DPAs, patient associations and ethics boards

- Title: Code of Practice on Secondary Use of Medical Data in Scientific Research Projects
  - Definition of terms (in the scientific context)
  - Rules: what exactly is required to be done for each topic to comply with applicable regulations

# Description of the Code

- Collection, use and transfer of personal medical data
- De-identification and protection of anonymised data
- Information, consent and withdrawal
- Including secondary use of health care and genetic data in research projects
- Human biological samples
- Data security & involvement of data processors
- Documentation and data retention
- Medical data disclosure

# Description of the Code (cont.)

- Implementation of the code rules
- Code modifications
- APPENDICES
  - Appendix 1: Adherence Agreement (given as an example for projects which are willing to render this Code binding)
  - Appendix 2: Example of information sheet and consent form
  - Appendix 3: Examples of de-identification methods and guidance
  - Appendix 4: Secondary use summary
  - Appendix 5: Decision Tree for Secondary Use

# How should this Code be used?

- The Code is not a binding document
  - Intended as guidance to be used by IMI and other collaborative projects to address multi-partner / multi-country issues for compliance with personal data protection regulations
- This Code provides EU harmonized operational solutions to ensure compliance with the EU Data Protection Directive as well as the future General Data Protection Regulation
  - It does not cover all local exceptions, but includes some as examples
  - It provides a harmonized solution that can be adapted to applicable law where required

# Status of the Code and Next Steps

- Final draft dated August 27th, 2014
- Submitted to several authorities (Aug 2014 – Dec 2015): French and Belgian DPAs, Article 29 Working Party, the European Data Protection Supervisor
- IMI "Coordination and Support Action" for the Big Data for Better Outcomes program, including development of standards and guidance for the use of human samples and data in the context of data privacy and related legal aspects

# You Want to Know more about the Code?

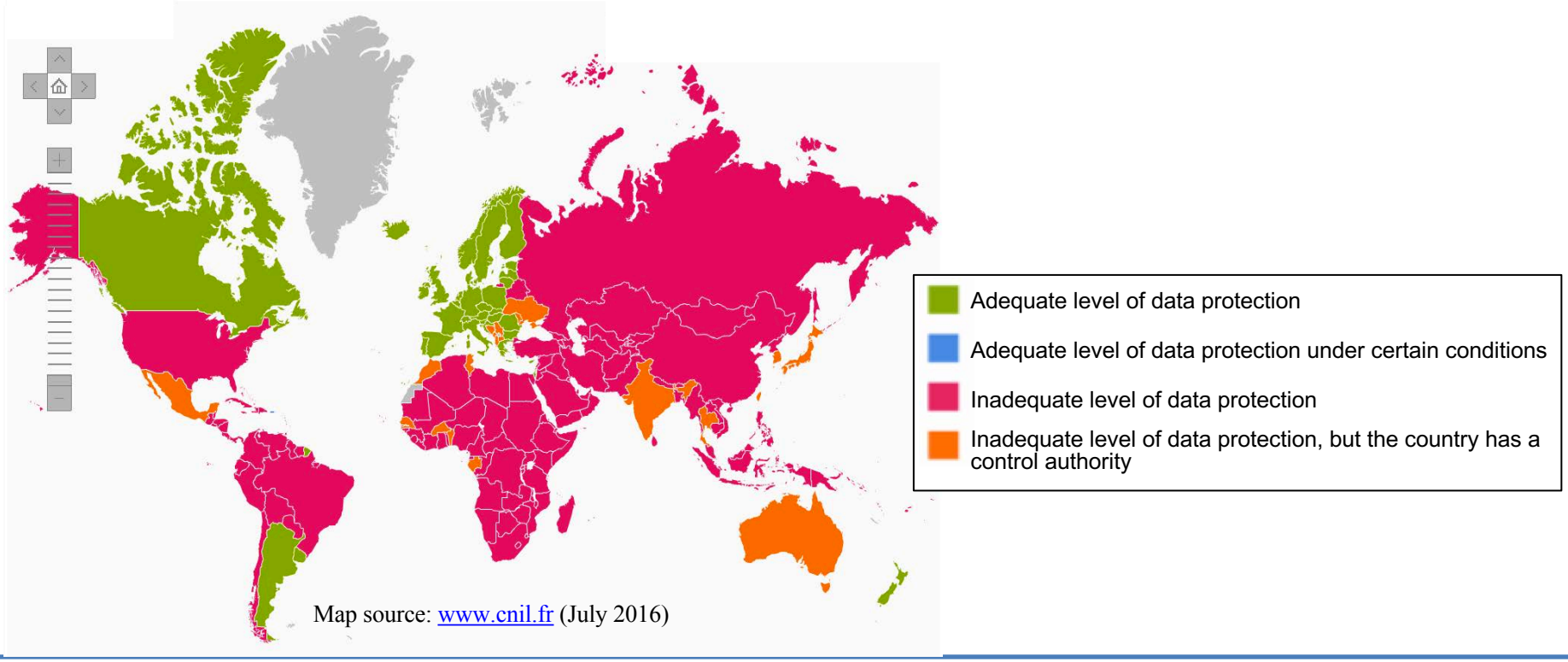
- Go to the eTRIKS or IMI web site, or click here
- Read the published article:

  **Code of practice on secondary use of medical data in European scientific research projects.** Anne Bahr & Irene Schlünder - International Data Privacy Law 2015 - *doi: 10.1093/idpl/ipv018 (free access)*

# Conclusion and Summary

# Data Protection World-Wide

- In the opinion of the European Commission, only a small number of countries outside the EEA offer an adequate level of data protection
- See here for information and restrictions on transfer of data



# Do not forget…

- Anonymous data are not subject to Privacy laws
  - You do not need to obtain consent to process these data
- Anonymisation of health data is itself processing of personal data
  - This requires the informed consent of the patient
  - But this processing does not require authorization from the data protection authorities
- The processing of personal data (i.e. data that indirectly or directly identify the data subject) must be compliant with:
  - The information provided in the consent form, including the purposes and the intended recipients of the data
  - Unless a waiver is given by a competent authority or the data are anonymised

# Questions?

Please contact:

David Henderson
david.henderson@bayer.com

Charles Auffray
cauffray@eisbm.org