

# SEMINAR JURIDISCHE ASPECTEN VAN DATAMANAGEMENT

NAI-hbo, LCRDM & SURF



["Research Data Management"](#) by [jannekestaaks](#)



# Programma

10.00 uur **Welkom en introductie**

10.30 uur **Experts aan het woord!**

Duik in de wereld van AVG & onderzoeksdata

11.30 uur **Vragen**

Naar aanleiding van de presentaties en uit de praktijk

12.15 uur **Lunch**

13.15 uur **Workshop**

Aan de slag met juridische cases rondom data

14.30 uur **Presentaties workshop**

15.15 uur **Afsluiting**

## Sprekers / Organisatieteam

- Marlon Domingus (EUR)
- Esther Hoorn (RUG)
- Hans de Brouwer (NAI-hbo, Saxion)
- Raymond Snijders (NAI-hbo, Windesheim)
- Ingeborg Verheul (LCRDM)
- Sarah Coombs (NAI-hbo, Saxion)
- Leen Liefsoens (NAI-hbo, De Haagse Hogeschool)
- Eva Woertman (SURFmarket)

# Vragen

- Welke vragen leven er in de praktijk?



["Telephone data"](#) by [jannekestaaks](#)

# Workshop

- Aan de slag met juridische cases rondom data
- Programma
  1. 13.15 uur Bespreking van cases in 8 groepen van 5 deelnemers
  2. 14.00 uur Bespreking van cases in 4 groepen van 10 deelnemers
  3. 14.30 uur PresentatiesCoffee On The Go!
- Cases
  1. Datamanagementplan
  2. Verwerking van persoonsgegevens bij opslag en archivering van onderzoekdata
  3. Wie is de eigenaar van de data?
  4. Datarecht



["Research Data Management"](#) by [jannekestaaks](#)

# Case 1: Datamanagementplan

- Onderzoek naar het effect van het gebruik van de Nintendo Wii bij kinderen en jongeren met niet aangeboren hersenletsel (NAH) op fysiek, cognitief en sociaal functioneren.
- De jongeren zijn verbonden aan drie verschillende revalidatiecentra. De effectmetingen zullen bestaan uit vragenlijsten en een neuropsychologische test. Het team van onderzoekers bestaat uit personen van één van de revalidatiecentra, van het lectoraat van de hogeschool en van een medisch universitair centrum.
- Subsidie van een externe financier. Eén van de subsidiebepalingen is het opstellen van een datamanagementplan (DMP).
- Voorzie het onderzoeksteam van een DMP template: opsomming onderdelen en kort waar ze moeten op letten inclusief informatiebronnen/hulpmiddelen.

## Case 2: Verwerking van persoonsgegevens bij opslag en archivering van onderzoek

- Onderzoek naar de stress die studenten ervaren tijdens hun studie.
- Data uit
  - geanonimiseerde datasets van anderen
  - interviews / vragenlijsten met persoonsgegevens
  - panelgesprek opgenomen op video
- Vragen:
  1. Wat mag er wel en wat mag er niet bewaard worden voor langere termijn?
  2. Onder welke voorwaarden mag de onderzoeksdata bewaard worden? En hoe lang moet dat minimaal?
  3. Mag de onderzoeker alle data met persoonsgegevens wel voor zichzelf bewaren?
  4. Als de onderzoeker de datasets met anderen wil delen, waar moet dan op gelet worden?

## Case 3: Wie is de eigenaar van de data?

- Kan een lector onderzoeksdata meenemen naar een nieuwe werkgever of kan de oude werkgever dit blokkeren door zich te beroepen op het eigendomsrecht?
- Mag een onderzoeker de gegevens verzameld voor onderzoek aan zijn hogeschool ook commercieel gebruiken voor zijn eigen advieswerk?
- Een onderzoeksgroep bestaat uit meerdere onderzoekers vanuit verschillende hogescholen universiteiten en bedrijven. Onderzoeksdata worden door alle deelnemende partners verzameld en in een geïntegreerde database samengebracht. Moet er wat geregeld worden over het eigenaarschap van de data?

## Case 4: Datarecht

- Onderzoek naar het effect van Professional Learning Communities (PLC) op de resultaten van studenten. Onderzoek vindt plaats in een regio met vier scholen die samenwerken om de curricula toe te spitsen op de behoeftes van hoogbegaafde kinderen. De docenten die hierbij zijn betrokken hebben ook samen een PLC opgericht om samen te kunnen werken, elkaar te ondersteunen en professionaliseren.
- Data uit: rapporten en cito's van studenten, interviews, focusgroepen en plangesprekken.
- Geen open access verplichting, maar metadata welk open voor bekendheid. Verplichting om de raw, clean en final data 10 jaar te bewaren.
- Vragen:
  1. Mag de onderzoeker de data gebruiken voor vervolgonderzoek?
  2. Mag de data worden hergebruikt door een andere onderzoeker van een ander instituut binnen een ander onderzoek?



# Presentaties

- Cases
  1. Datamanagementplan
  2. Verwerking van persoonsgegevens bij opslag en archivering van onderzoekdata
  3. Wie is de eigenaar van de data?
  4. Datarecht10 minuten per case



["Research Data Management"](#) by [jannekestaaks](#)

# Juridische Aspecten van Datamanagement: IPR en Gegevensbescherming

SURF Seminar Juridische Aspecten van Datamanagement

21 mei 2018

Marlon Domingus, CIPP/e, CIPM

# IPR

Intellectual Property Rights (IPR) and research data:

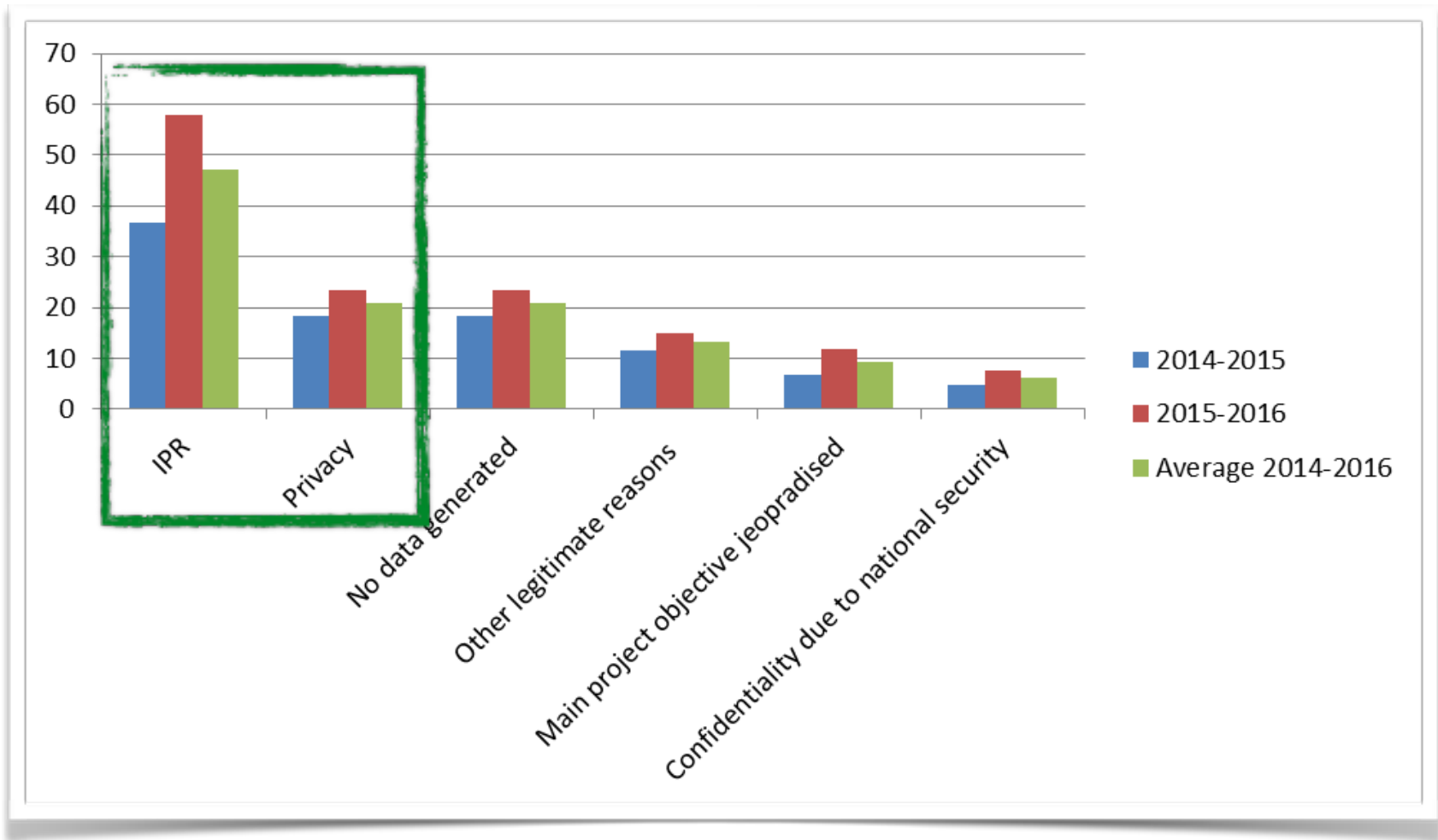
It is important to **identify the owner of the data**: the researcher, funder or institution. Responsibilities for stewardship of the data both during a project (if the work is project-based) and when funding has come to an end should also be clear.

In cases of multi-party research projects (for example 7 university, 2 business and 3 government agencies working on one project) the **partnership agreement** which underpins the collaboration before the research starts should identify how resulting research data will be managed and who owns it.



Source: Esther Hoorn LLM, University of Groningen: *The landscape of present rules and requirements regarding to research data, for instance in the recently revised Code of Conduct for Scientific Practice and in the regulations applied by research funding bodies*. WIKI Research Data Ownership. See online: <https://wiki.surfnet.nl/pages/viewpage.action?pageId=47449662>

# Why are legal aspects important? Data Governance.



# Lessons Learned: IPR Helpdesk

The image shows a screenshot of the European IPR Helpdesk website. At the top, there is a navigation menu with the following items: SERVICES, NEWS, EVENTS, LIBRARY, TRAINING, AMBASSADORS, HELPLINE, and CONTACT. Below the menu is a banner with a blue background and a network diagram. The banner text reads: "NEW WEBINAR TOPIC! CONSORTIUM AGREEMENTS!". Below the banner is a section titled "European IPR Helpdesk" with the text: "We believe that knowing how to manage Intellectual Property Rights (IPR) is the ticket to innovation and competitiveness in Europe. The IPR Helpdesk offers free of charge, first-line support on IP and IPR in EU funded research projects and EU SMEs involved in transnational research projects, especially within the Enterprise Europe Network". To the right of the banner is a sidebar with the European IPR Helpdesk logo and the website address "www.iprhelpdesk.eu". Below the logo is a blue box with the text "European IPR Helpdesk Fact Sheet IP joint ownership". Below this is a table of contents for the fact sheet, dated "October 2015<sup>1</sup>".

European IPR Helpdesk

SERVICES NEWS EVENTS LIBRARY TRAINING AMBASSADORS HELPLINE CONTACT

NEW WEBINAR TOPIC! CONSORTIUM AGREEMENTS!

European IPR Helpdesk

www.iprhelpdesk.eu

European IPR Helpdesk

Fact Sheet

*IP joint ownership*

October 2015<sup>1</sup>

Introduction..... 1

1. IP joint ownership ..... 2

2. Allocation of shares between joint owners in collaborative research projects ..... 4

2.1. Background ..... 4

2.2. IP joint ownership ..... 4

3. Conditions of use and exploitation of the jointly owned IP..... 5

3.1. Rights of use ..... 5

3.2. Rights of exploitation ..... 6

3.3. Dissemination and confidentiality ..... 7

4. Management of the jointly owned IP ..... 8

4.1. IPR protection ..... 8

4.2. IPR infringement and enforcement issues..... 9

5. Governing law and jurisdiction ..... 9

Useful Resources .....10

# IPR Helpdesk: Copyright Essentials

Copyright is an intellectual property right (IPR) that grants authors, artists and other creators protection for their literary, artistic and scientific creations, generally referred to as “works”.

No matter if you are a copyright owner or a copyright user, the understanding of the copyright basics is crucial to any business. In essence, it must be borne in mind that safeguarding your own copyright and securing the permission of third parties before using copyrighted materials is not only legally required but also a good business practice.

# IPR Helpdesk: Copyright Essentials

**Copyright protection** is obtained automatically in the EU, as in any country which is a signatory to the Berne Convention. It arises **from the moment the work is created** and no registration or other formality is required.

The copyright system allows authors to benefit commercially from their work, through: **Economic** rights and **Moral** rights.

## Some examples of economic rights

- right of reproduction, e.g. to make copies of the work such as printed publications or sound recordings
- right of distribution, e.g. to distribute copies of the work
- right of fixation, e.g. to record the work in, for example, a CD or DVD
- right of communication to the public, e.g. broadcasting via radio, TV or Internet
- right to perform the work publicly, e.g. to authorise live performances of the work such as in a play
- right to make "derivative works", e.g. to authorise modifications, translations, adaptations such as turning a novel into a screenplay, or other new uses of a work.

# IPR Helpdesk: Copyright and other IPRs

	Pros	Cons
<b>Copyright</b>	<ul style="list-style-type: none"> <li>• Automatic protection</li> <li>• No registration costs</li> <li>• Moral rights can be perpetual</li> <li>• Long-term protection for economic rights</li> <li>• Software and databases can also be protected by copyright</li> </ul>	<ul style="list-style-type: none"> <li>• Requirement to qualify as a work</li> <li>• No priority</li> <li>• 20 years protection for neighbouring/related rights<sup>18</sup></li> <li>• There may be some extra requirements for designs to be copyrighted in some countries<sup>19</sup></li> </ul>
<b>Patents</b>	<ul style="list-style-type: none"> <li>• Exclusive rights</li> <li>• 12 months priority</li> <li>• Stronger protection</li> </ul>	<ul style="list-style-type: none"> <li>• Costly and lengthy procedures</li> <li>• 20 years protection</li> <li>• Disclosure requirement</li> <li>• Extra requirement for software to receive European patent protection<sup>20</sup></li> </ul>
<b>Industrial designs</b>	<ul style="list-style-type: none"> <li>• 3 years protection for unregistered designs</li> <li>• 6 months priority</li> <li>• Harmonisation at EU level</li> <li>• Some harmonisation at international level<sup>21</sup></li> </ul>	<ul style="list-style-type: none"> <li>• Maximum non-renewable 25 years protection for registered Community designs<sup>22</sup></li> <li>• No renewable protection for unregistered Community designs</li> </ul>
<b>Databases</b> <sup>23</sup>	<ul style="list-style-type: none"> <li>• Exclusive rights</li> <li>• Secure protection</li> </ul>	<ul style="list-style-type: none"> <li>• No priority</li> <li>• EU right only</li> <li>• 15 years protection<sup>24</sup></li> </ul>
<b>Trade marks</b>	<ul style="list-style-type: none"> <li>• Renewable indefinitely for periods of 10 years</li> <li>• 6 months priority</li> <li>• Harmonisation at EU level</li> <li>• Some harmonisation at international level<sup>25</sup></li> </ul>	<ul style="list-style-type: none"> <li>• Obligation to use<sup>26</sup></li> </ul>



## IPR Helpdesk: Joint Ownership

**Joint ownership (co-ownership)** refers to a situation in which two or more persons have proprietary shares of an asset: they co-own a property. **Joint ownership of IP**, in particular, frequently arises in **collaborative projects** when the **results have been jointly generated by the partners** and the share of work is not easily ascertainable.

Conditions of use and exploitation of the jointly owned IP:

- Rights of use
- Rights of exploitation
- Dissemination and confidentiality

# IPR Helpdesk: Joint Ownership - Sample Clauses

RIGHT OF USE

OWNERSHIP OF INTELLECTUAL PROPERTY RIGHTS

RIGHT OF USE – background

RIGHT

RIGHT OF EXPLOITATION – second option [consent not required]

DISSEMINATION

1. If a Party intends to publish information and other research materials related to the collaboration project hereof, such a party shall, prior to publication, provide [...] days as examination period for the other party to verify whether the contents of such dissemination disclosed should be kept confidential. Such other party may request in writing to extend the examination period, due to the importance of the information disclosed.

CONFIDENTIALITY

2. Confidential Information shall not be disclosed, copied, reproduced, or otherwise made available to any other third party without the consent of the other Parties. Each Party agrees to use its best efforts to maintain the confidentiality and to keep data and research materials confidential until published or until corresponding patent applications are filed;
3. Confidentiality obligation shall expire at the earlier of the date when the information is publicly known or [...] years after the expiration or termination date of this Agreement. Each Party may request an extension to this term when necessary to protect confidential information relating to foreground not yet commercialised.

[sample clauses]

e of its interest in  
to the other Party

Its to third parties

f the foreground shall  
to the type of license  
it by the Parties.

[sample clauses]



# Interesting Approach: IPR and Open: 4 Logics

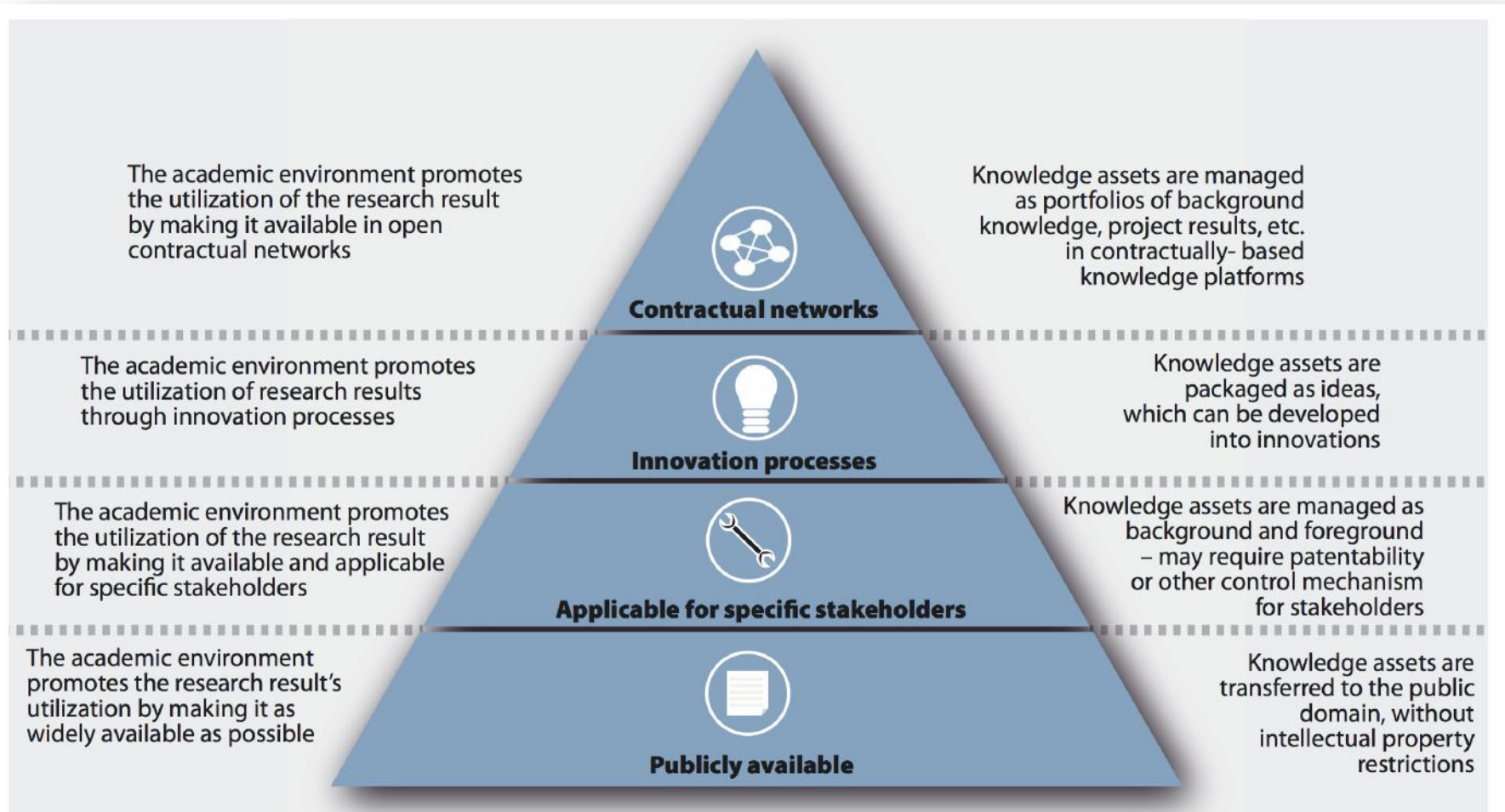


Figure 26. Four logics for academic environments that promote utilization

# 5 Habits of Responsible Researchers

SURF Seminar Juridische Aspecten van Datamanagement

21 mei 2018

Marlon Domingus, CIPP/e, CIPM

# What to know and what to do

## Context: General Data Protection Regulation (GDPR)

### KNOW:

1. GDPR: personal data and special categories of personal data
2. GDPR: privacy principles and privacy by design
3. GDPR: accountability: demonstrate compliancy with General Data Protection Regulation
4. GDPR: risk assessment: Data Protection Impact Assessment (DPIA)
5. GDPR: cross border data transfer
6. Security and privacy
7. Register of processings
8. EUR Privacy app

### DO:

1. Register your research
2. Participate in a DPIA
3. Take adequate organisational and technical measures
3. Have suitable agreements with partners: Data Processing Agreements and Terms of Service
4. Contact privacy your officer for support

# 5 Habits of Responsible Researchers



**1. Safe research project** Plan, document and verify the various aspects of your research: the research purpose, methodology, integrity, ethics and privacy. (1) Create a Data Management Plan, (2) register your research project in the EUR Register of Processings, (3) Submit your proposal to an Internal Review Board or Ethical Committee, and follow up on the provided feedback and recommendations.



**2. Safe People** When you collaborate, know what the responsible level of trust is you should assume. What are your experiences with the *people, organisations* involved? With which *countries* is collaboration required? Some countries, organisations may be whitelisted or blacklisted. The level of trust with peers, non academics and service providers determines the nature of the agreements and organisational and technical measures necessary; especially related to access, and privileges granted to work with the data.



**3. Safe Settings** Only use algorithms, software, platforms, services, contracts and agreements appropriate with regards to the nature of your data. Use the [EUR data classification](#) to know how to treat personal data when collecting, storing, analysing, deleting, publishing and archiving. For your team and the individuals participating in your project: make the default settings transparent, understandable, privacy friendly and secure.



**4. Safe Data** Share data responsibly within your project and within the different work packages. Make sure people have access on a *need to know* basis and make sure there is logging of who touches the data. Work only in safe environments, both physically and digitally, and protect the data by using [encryption](#) and a [secure collaboration platform](#).



**5. Safe Outputs** Share data responsibly within your publications, public datasets, teachings and presentations. Know who you share the data with and for which purpose the data is used and reused. Is this (re)use still compliant with the conditions of the informed consent for instance? Which level of pseudonymisation (weak or strong) is appropriate?

Inspired by the forthcoming publication by Khaled El Emam and Luk Arbuckle: 'The Five Safes of Risk-Based Anonymization', which is based on the work by: Tanvi Desai, Felix Ritchie and Richard Weipton: *Five Safes: designing data access for research*. Bristol Business School Working Papers in Economics. 2016. Online: <http://eprints.uwe.ac.uk/28124/1/1601.pdf>

# 5 Habits of Responsible Researchers

## 2. Typical measures to take before and during a research project.



# 5 Habits of Responsible Researchers

## 3. Typical Actions

### 3.1. Implement appropriate technical and organisational measures:

1. **Individual participating in your research (data subject).** Is the participant well informed, aware of possible risks for her/him and aware of the purpose of the research?
2. **Data.** Is the data de-identified and encrypted?
3. **Access Management.** How is access managed and controlled for the PI / team (expanded) / public?
4. **Software / Platform.** Are the *Terms of Service* for used software / platform checked (where is the data and who has access and has which usage rights)?
5. **Devices.** Are devices used safe? Encrypted drive, encrypted communication, strong password / two factor authentication.
6. **Partners.** Are the research partners / service partners trusted and are appropriate legal agreements made, with regards to roles, rights and responsibilities?
7. **Safe and secure collaboration.** Is the ((cross border) communication to, in and from the) collaboration platform end to end encrypted, are roles and permissions defined and implemented, is logging and monitoring implemented?
8. **Risk definition and mitigation.** Are risks defined and mitigated? Is a risk audit procedure started?

### 3.2. Risk assessment: What are the risks related to your data processing?

What are privacy risks in your scenario and what are the corresponding appropriate safeguards? Does your processing demonstrate the privacy principles and is your processing ethical? What are your and your service provider's security measures? Are these audited regularly externally, and available for you? Does your service provider take the correct role (processor / controller) and related responsibility and accountability?

Participate in a *Data Protection Impact Assessment* (DPIA) to answer these questions.

Please contact: [privacy@eur.nl](mailto:privacy@eur.nl) to start your DPIA. A DPIA is done during your research design and takes 1,5 hour.



# 5 Habits of Responsible Researchers

## 4. Support

Please contact your privacy officer for support before, during and after your research project.

Email: [privacy@eur.nl](mailto:privacy@eur.nl) See [here](#) (MyEUR) for your EUR Privacy Officer.

See the **EUR Privacy & Security app** with basic info for you as a researcher.

Download the app at: [Apple App Store](#) or [Google Play Store](#)

See also: infographics on Privacy; [Why](#), [What](#) and [How](#).

See also: how to [work safely](#) out of the office.

See also: online training: [Privacy in Research](#), created in collaboration with SURF.

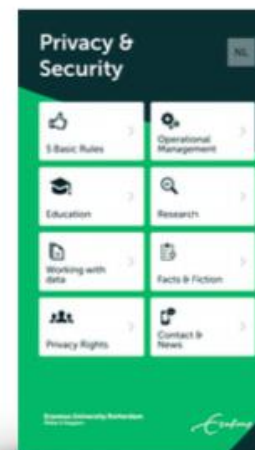
See also: the [VSNU code of conduct for processing personal data in research](#).

The new version is expected **February 2019**.

Please contact *Erasmus Research Services*


for data management support: [researchservices@eur.nl](mailto:researchservices@eur.nl)

or related research services: <https://www.eur.nl/en/research/research-services>.




# The General Data Protection Regulation (GDPR)

### TERRITORIAL SCOPE




**EU Establishments**  
**Non-EU Established Organizations**  
 Offer goods or services or engaging in monitoring within the EU.

### THE PLAYERS




**Data Subjects**  
**Data Controllers**  
**Data Processors**  
**Supervisory Authorities**

### PERSONAL DATA



**Identified** **Identifiable**

### SENSITIVE DATA



**Religious or Philosophical Beliefs**  
**Trade Union Membership**  
**Sex Life**  
**Racial or Ethnic Origin**  
**Political Opinions**  
**Health**  
**Genetic Data**  
**Biometric Data**


## RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

### LAWFUL PROCESSING


Collection and processing of personal data must be for "specified, explicit and legitimate purposes" –with consent of data subject or necessary for

- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests

### Security




### Data Protection Officer (DPO)




Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.

### Record of Data Processing Activities




Maintain a documented register of all activities involving processing of EU personal data.

### Data Protection by Design



built in starting at the beginning of the design process


### Data Impact Assessment



For high risk situations

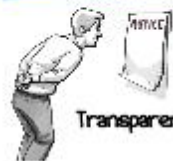
# GDPR

### CONSENT



Consent must be freely given, specific, informed, and unambiguous.

### RIGHTS OF DATA SUBJECTS



**Automated Decision Making**  
 "Right not to be subject to a decision based solely on automated processing, including profiling."

**Transparency**


**Access and Rectification**

**Right to Erasure**

**Purpose Specification and Minimization**

**Right to Data Portability**


### ENFORCEMENT



**Fines**  
 Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.

**Effective Judicial Remedies:**  
 compensation for material and non-material harm.

### DATA BREACH NOTIFICATION




A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects

Notify supervisory authorities no later than 72 hours after discovery.

### INTERNATIONAL DATA TRANSFER




**Adequate Level of Data Protection**

**Binding Corporate Rules (BCRs)**

**Privacy Shield**

**Model Contractual Clauses**

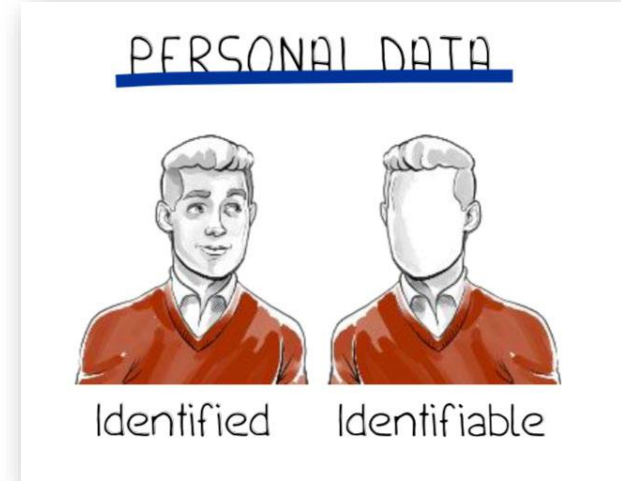


[www.teachprivacy.com](http://www.teachprivacy.com)

Workforce awareness training by Prof. Daniel J. Solove

Please ask permission to reuse or distribute

# 1. Personal Data



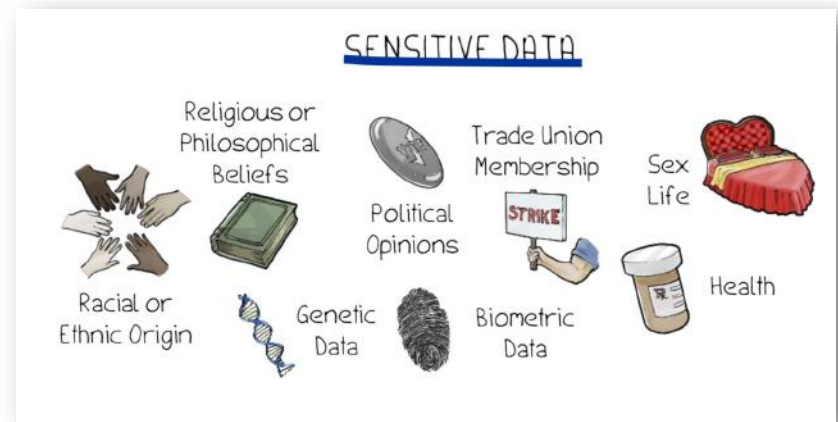
## **"Personal Data" (GDPR\*, Article 4):**

Any information relating to an identified or identifiable natural person:

a name, an identification number, location data, an online identifier, one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

\* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Online available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

# 1. Special Categories of Personal Data



## "Special Categories of Personal Data (Sensitive Data)" (GDPR, Article 9):

Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

\* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Online available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

## 2. Privacy Principles

**Principles relating to processing of personal data (GDPR\*, Article 5).** Demonstrate compliancy with the principles:

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

\* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Online available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

## 2. Privacy By Design [Ann Cavoukian]

### *The 7 Foundational Principles*

#### 1. **Proactive** not Reactive; **Preventative** not Remedial

The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

#### 2. Privacy as the **Default Setting**

We can all be certain of one thing — the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, *by default*.

#### 3. Privacy **Embedded** into Design

*Privacy by Design* is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

#### 4. Full Functionality — **Positive-Sum**, not Zero-Sum

*Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy *vs.* security, demonstrating that it *is* possible to have both.

#### 5. End-to-End Security — **Full Lifecycle Protection**

*Privacy by Design*, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, secure lifecycle management of information, end-to-end.

#### 6. **Visibility** and **Transparency** — Keep it **Open**

*Privacy by Design* seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

#### 7. **Respect** for User Privacy — Keep it **User-Centric**

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.



# 3. Accountability

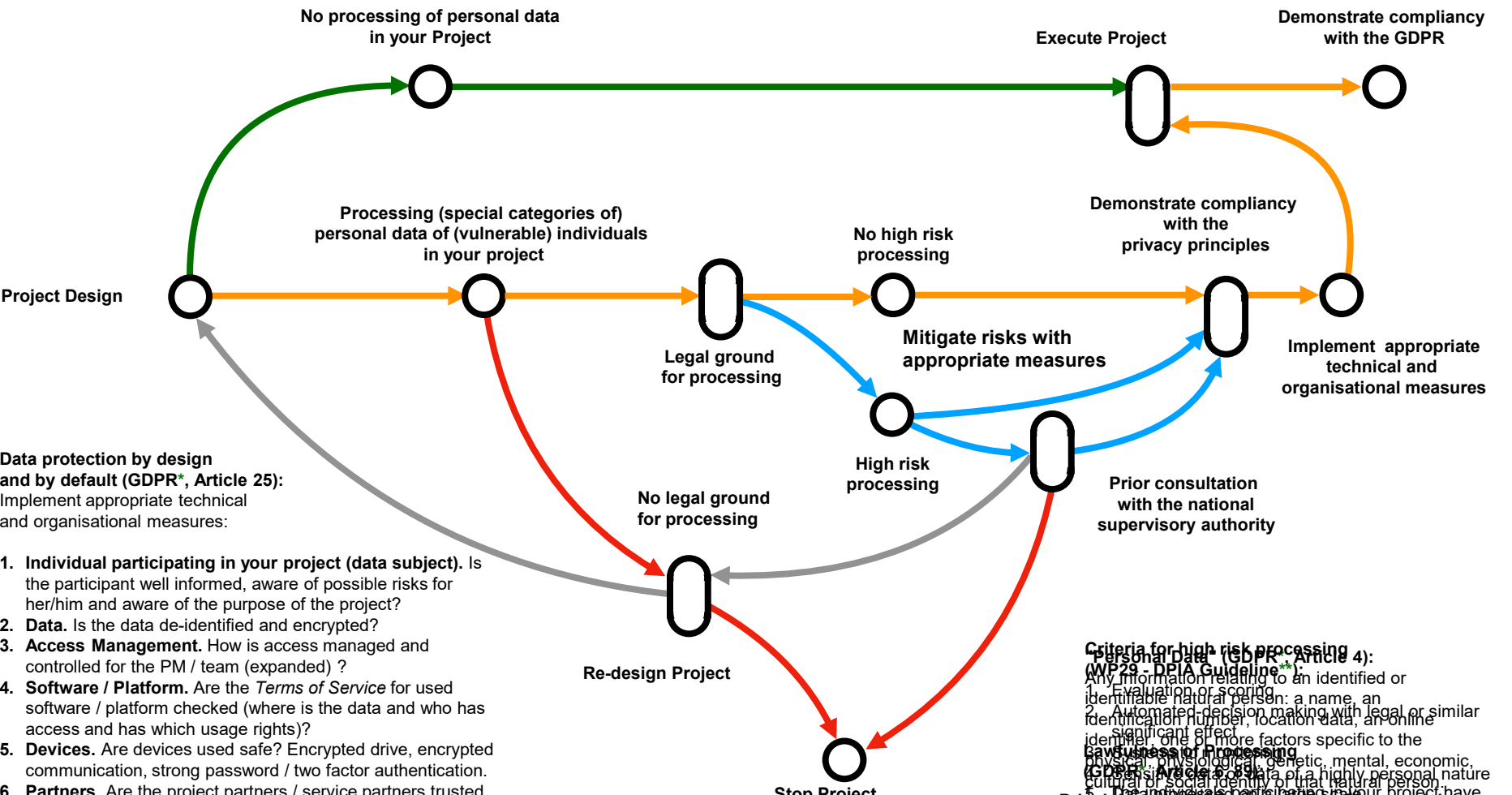
## Who

**University:** provide **necessary general conditions** to enable project managers to comply; policy, guidelines, infrastructure and skilled and available support staff.

**Dean:** provide **additional necessary discipline specific conditions** to enable project managers to comply; policy, guidelines, infrastructure and skilled and available support staff.

**Researcher:** follow **privacy principles & use the privacy enabling conditions** (policy, guidelines, infrastructure and skilled and available support staff).

# 4. The Privacy Impact Assessment (PIA) Route Planner for projects Inspired by Harry Beck's London Metro Map



- Data protection by design and by default (GDPR, Article 25):**  
Implement appropriate technical and organisational measures:
- 1. Individual participating in your project (data subject).** Is the participant well informed, aware of possible risks for her/him and aware of the purpose of the project?
  - 2. Data.** Is the data de-identified and encrypted?
  - 3. Access Management.** How is access managed and controlled for the PM / team (expanded) ?
  - 4. Software / Platform.** Are the *Terms of Service* for used software / platform checked (where is the data and who has access and has which usage rights)?
  - 5. Devices.** Are devices used safe? Encrypted drive, encrypted communication, strong password / two factor authentication.
  - 6. Partners.** Are the project partners / service partners trusted and are appropriate legal agreements made, with regards to roles, rights and responsibilities?
  - 7. Safe and secure collaboration.** Is the ((cross border) communication to, in and from the) collaboration platform end and encrypted, are roles and permissions defined and being and monitoring implemented?
- 8. Risk Definition and mitigation.** Are risks defined and mitigated?  
Is a risk audit procedure started?  
February 2018

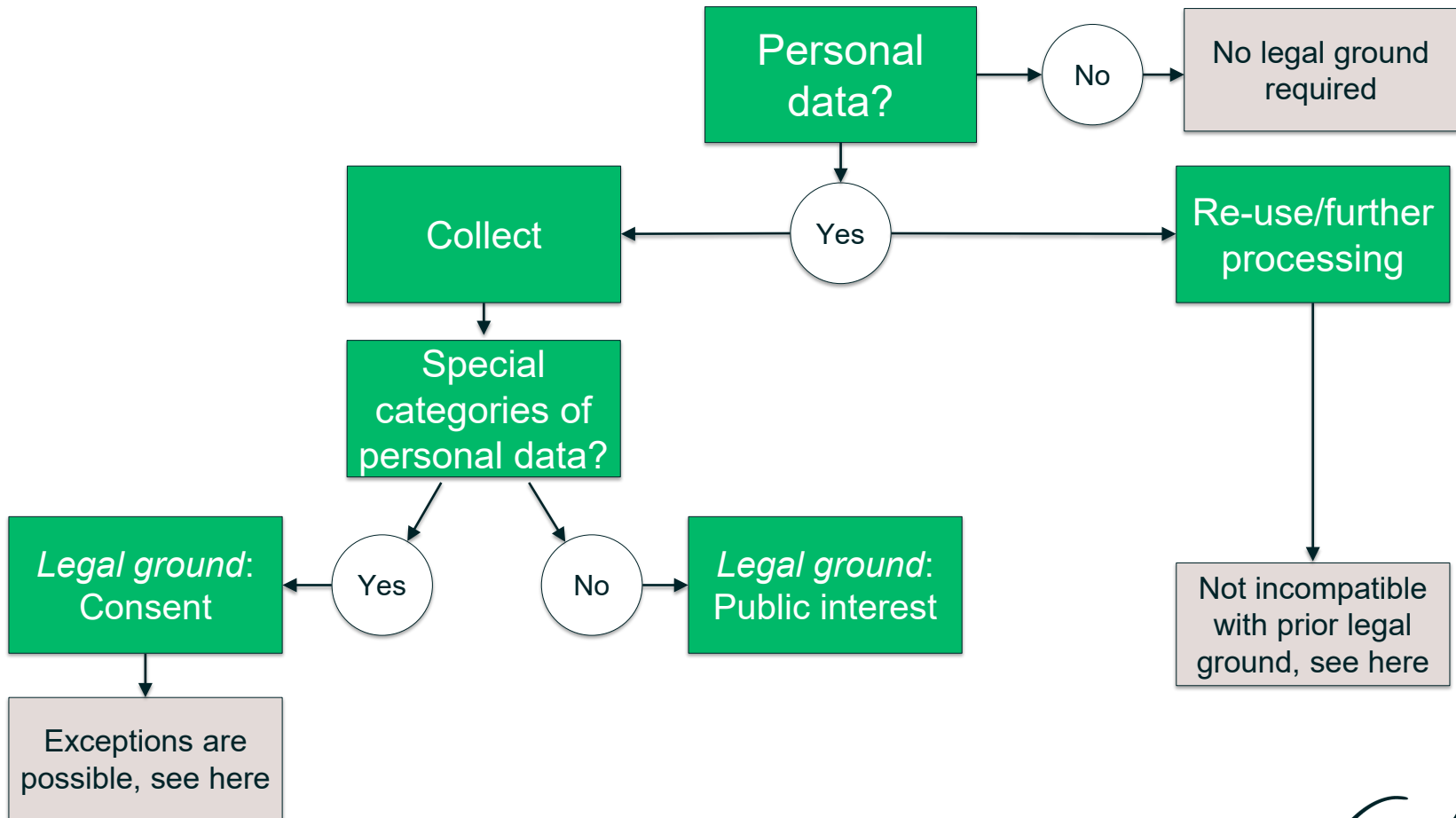
**Criteria for high risk processing (WP 29 - DPIA Guideline, Article 4):**  
Any information relating to an identified or identifiable natural person: a name, an identification number, location data, an online identifier, one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, social or identity of that natural person

**Principles relating to processing of personal data (GDPR, Article 5):**  
1. Lawfulness, fairness and transparency  
2. Purpose limitation  
3. Data minimisation  
4. Accuracy  
5. Storage limitation  
6. Integrity and confidentiality  
7. Accountability

Demonstrate compliance with the principle of lawfulness, fairness and transparency by ensuring data minimisation, purpose limitation, accuracy, storage limitation, integrity and confidentiality of personal data. Demonstrate compliance with the principle of accountability by ensuring data subjects from exercising a right or using a service or a contract concerning a natural person's sex life or sexual orientation.



# Lawfulness of processing



*Erasmus*

# Exceptions

Bijzondere persoonsgegevens mogen bij wetenschappelijk onderzoek verwerkt worden indien er **expliciete toestemming** is van de deelnemer.

Op deze hoofdregel geldt specifiek voor wetenschappelijk onderzoek **een uitzondering** welke enkel op gaat als:

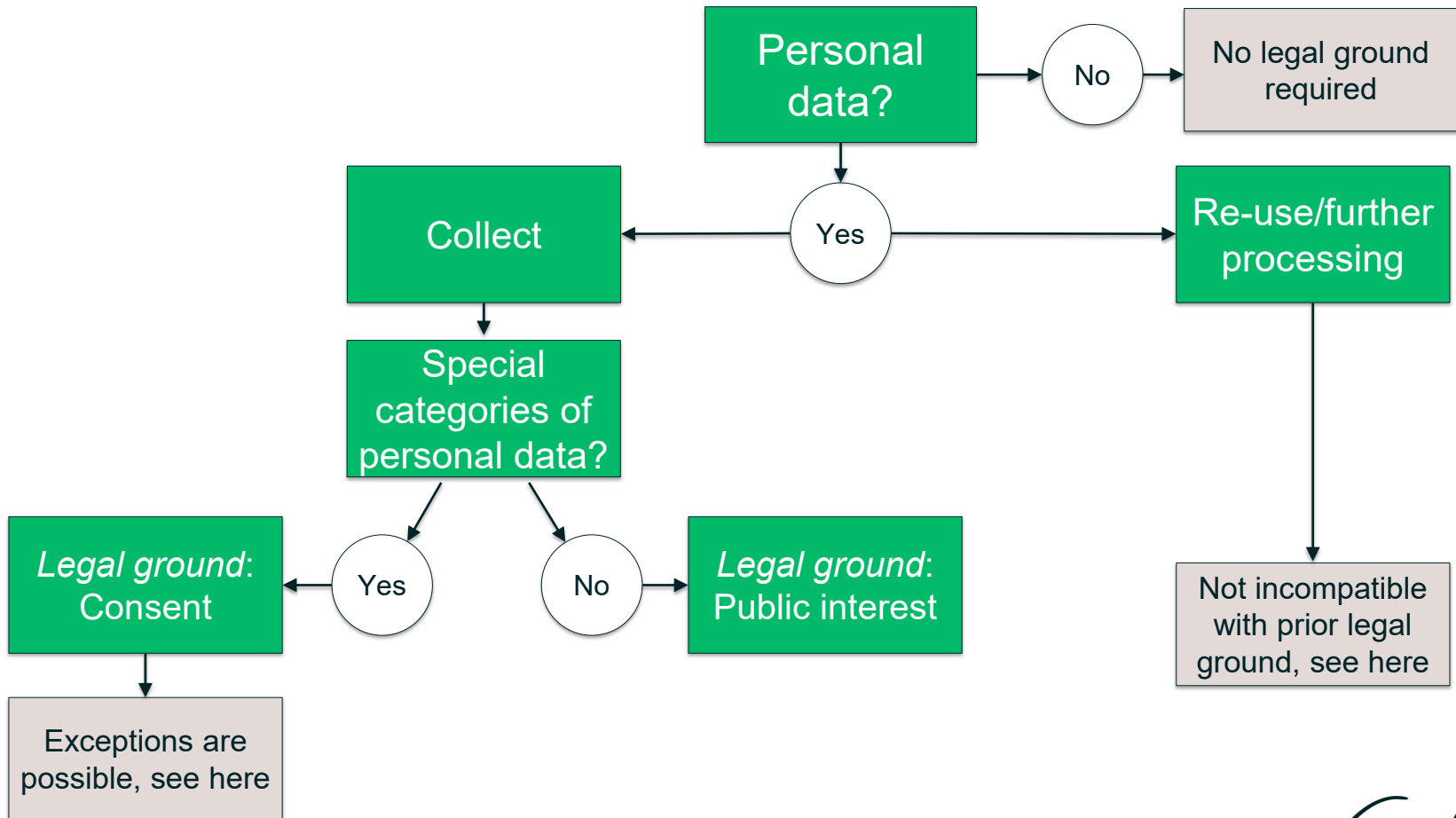
1. Het vragen van toestemming onmogelijk blijkt of een onevenredige inspanning vergt.
2. De verwerking noodzakelijk is met het oog op het onderzoek. Kan het onderzoek ook zonder deze gegevens worden uitgevoerd? Kunnen de gegevens ook op een andere manier worden verzameld?
3. Het onderzoek een algemeen belang dient.

Ook dient er te zijn voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de deelnemer niet onevenredig wordt geschaad.

Een voorbeeld waarbij de uitzondering geldt is covert research en misleiding, mits aan bovenstaande eisen is voldaan.

The logo of Erasmus University, featuring the word 'Erasmus' in a stylized, cursive script.

# Lawfulness of processing



*Erasmus*

# Reuse

1. Je gaat een dataset hergebruiken in **hetzelfde** onderzoeksgebied.

- Hebben deelnemers van het initiële onderzoek toestemming gegeven voor gebruik van hun gegevens?
  - **Ja?** Je hoeft niet opnieuw toestemming te vragen. Wel moet je de deelnemers informeren over jouw onderzoek als dit kan. Kan dit niet, dan moet je informeren op een openbare plek, bijvoorbeeld via het Privacy Statement.
  - **Nee?** Je hoeft geen toestemming te vragen. Wel moet je de deelnemers informeren over jouw onderzoek als dit kan. Kan dit niet, dan moet je informeren op een openbare plek, bijvoorbeeld via het Privacy Statement.

2. Je gaat een dataset hergebruiken in **een ander** onderzoeksgebied.

- Hebben deelnemers van het initiële onderzoek specifiek toestemming gegeven voor hergebruik in een ander onderzoeksgebied?
  - **Ja?** Je hoeft niet opnieuw toestemming te vragen. Wel moet je de deelnemers informeren over jouw onderzoek als dit kan. Kan dit niet, dan moet je informeren op een openbare plek, bijvoorbeeld via het Privacy Statement.
  - **Nee?** Je moet toestemming vragen om de data te hergebruiken. Kan dit niet, neem dan contact op met je Privacy Officer.



You are processing personal data for your research. Are legal agreements required?

Do you work with another party for your research?

NO

No legal agreement is necessary.  
Use EUR approved systems and software.

YES

Is this party external to the Erasmus University?

NO

No legal agreement is necessary.  
Use EUR approved systems and software.

YES

Are personal data exchanged between you and this party?

NO

No legal agreement is necessary.  
Use EUR approved systems and software.

YES

A legal agreement should be made. Contact your privacy officer

The Erasmus logo, featuring the word "Erasmus" in a stylized, cursive script.

# Glossary

- **Processing** Processing covers a wide range of operations performed on personal data, by both manual and automated means. It includes the 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 of personal data.
- **Personal data** Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly. Name, address, or telephone numbers are examples of personal data.
- **EUR approved systems** Any software / platform or system provided by the EUR.
- **Erasmus University** The publicly-funded university.
- **Exchange** An act of giving out information from one party to another, or vice versa, or an act of interchanging information between parties

The logo of Erasmus University, featuring the word "Erasmus" in a stylized, cursive script.

# Glossary

- **Data controller** Responsible for stating why and what personal data will be processed. For research by EUR researchers, in many cases, Erasmus University will be the data controller
- **Processor** Party that processes personal data for the data controller. This includes e.g. storage, analysis, or destruction. There should be an agreement between the data controller and the processor if they differ
- **EEA (European Economic Area)** Area consisting of all EU countries plus Liechtenstein, Norway, and Iceland
- **Joint Controller Agreement** Agreement necessary when two or more data controllers decide on the purposes and means ('why' and 'how') of processing of personal data.
- **Tooling/Tools** Technical applications or programmes used to process (personal) data, e.g. Qualtrics, Fileshare etc. Tooling is sometimes provided by a third party
- **Third party** A natural or legal person or organisation which processes personal data on behalf of a controller. To exchange personal data with a third party, there needs to be an agreement.
- **Processor agreement** An agreement between the data controller and the processor to indicate responsibilities and rights between these parties. Essential when personal data are being exchanged

The Erasmus University logo, featuring the word "Erasmus" in a stylized, cursive script.

# Research and the Exemptions

Scientific research\* should be interpreted in a broad manner including for example:

- technological development and demonstration,
- fundamental research,
- applied research and
- privately funded research.

\* Recital (159)

Coupling information\*\* from registries, researchers can obtain new knowledge of great value. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions

\*\* Recital (157)



# Research and the Exemptions

## Article 89

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for **derogations** from the rights referred to in:

Article 15 [Right of access by the data subject]

Article 16 [Right to rectification]

Article 18 [Right to restriction of processing]

Article 21 [Right to object]

# Research and the Exemptions

## Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; **further processing** for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes [purpose limitation];

# Research and the Exemptions

## Article 9

Processing of **special categories** of personal data

(j) **processing is necessary** for archiving purposes in the public interest, **scientific or historical research purposes or statistical purposes** in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

# Research and the Exemptions

The **further retention** of the personal data\* should be lawful where it is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

\* Recital (65)

**Coupling information\*\*** from registries, researchers can obtain new knowledge of great value. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions

\*\* Recital (157)

# Research and the Exemptions

Research is not explicitly designated as its own lawful basis for processing, but, in some cases, it may qualify under Article 6(1)(f) as a **legitimate interest** of the controller.

Thus, while the GDPR explicitly permits re-purposing collected data for research, it also may permit a controller to collect personal data initially for research purposes, without requiring the data subject's consent.

Gabe Maldoff, How GDPR changes the rules for research. April 19 2016.

Source: <https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/>

# 5. Cross Border Data Transfers



The screenshot shows the top navigation bar of the European Commission website. On the left is the European Commission logo. On the right, there is a language selector set to 'English EN' and a search box with a 'Search' button. Below the navigation bar is a breadcrumb trail: 'Home > Law > Law by topic > Data protection > Data transfers outside the EU > Adequacy of the protection of personal data in non-EU countries'. The main heading is 'Adequacy of the protection of personal data in non-EU countries' in white text on a dark blue background. Below the heading is a sub-heading: 'How the EU determines if a non-EU country has an adequate level of data protection.'

## Adequacy decisions

---

The European Commission has the power to determine, on the basis of article 45 of [Regulation \(EU\) 2016/679](#) [↗](#) whether a country outside the EU offers an adequate level of data protection, whether by its domestic legislation or of the international commitments it has entered into.

# 5. Cross Border Data Transfers

## Adequacy Decision

The European Commission decides whether a country outside the EU (a so called 'third country') offers an adequate level of data protection. This decision is called the 'adequacy decision'.

## GDPR: EU and EEA

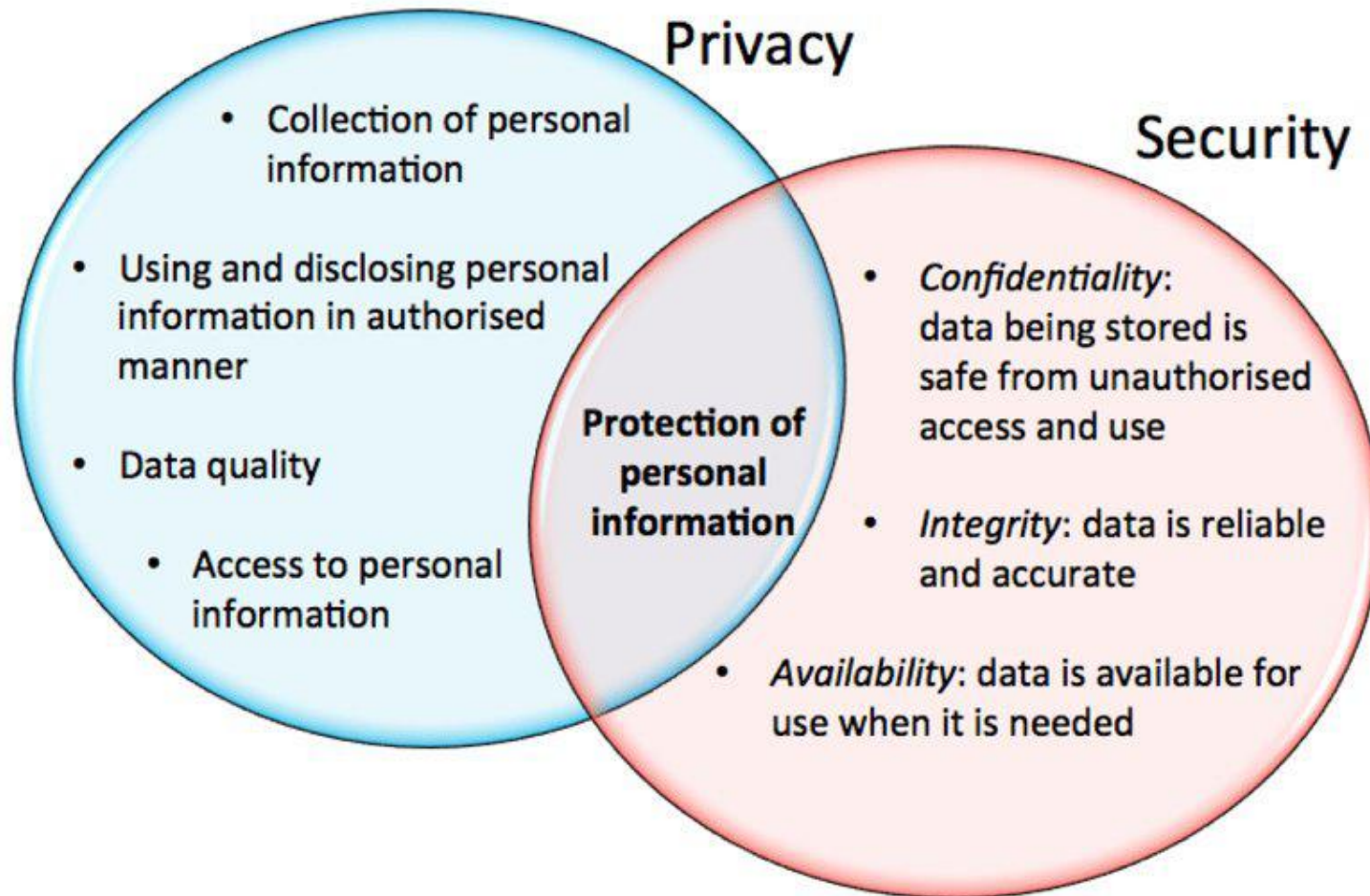
The General Data Protection Regulation (GDPR) applies in the 28 Member States of the EU, as well as in the three European Economic Area (EEA) countries, not in the EU: Norway, Iceland, and Liechtenstein. These three countries will become subject to the GDPR at the same time as the EU countries.

## Adequate

The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing \*adequate protection\*.

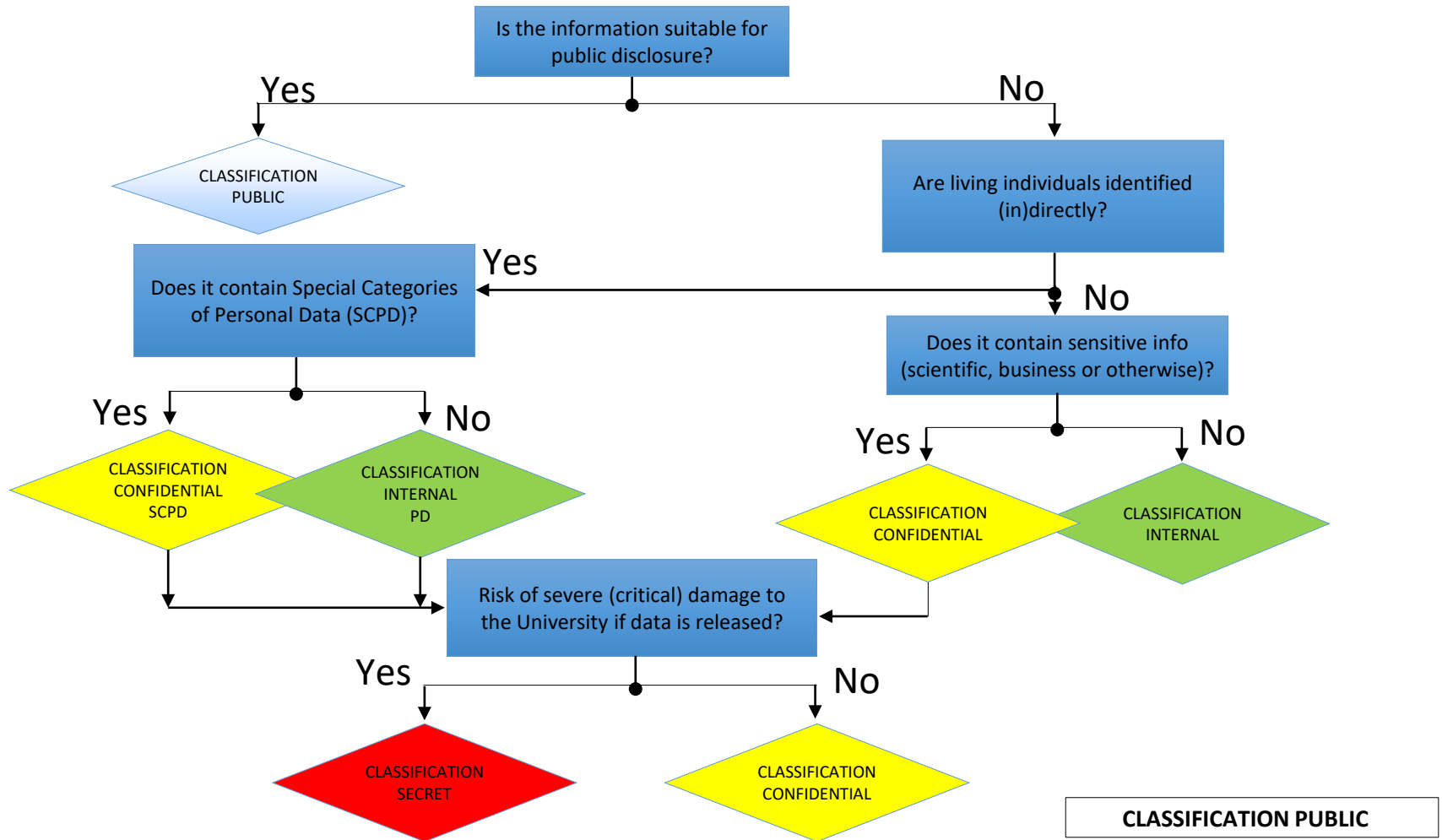
Adequacy talks are ongoing with South Korea.

## 6. Security and privacy: data classification





# 6. Security and privacy: data classification



CLASSIFICATION PUBLIC

# 6. Security and privacy: data classification

## EUR Data Classification Model

	CLASSIFICATION PUBLIC	CLASSIFICATION INTERNAL (*PD)	CLASSIFICATION CONFIDENTIAL (*SCPD)	CLASSIFICATION SECRET
Level of Need-To-Know	May be viewed by all members of the public	<p>May be seen by all members of the Erasmus University Rotterdam. Should be additionally labeled as PD if the document consist Personal Data.</p> <p>PD may be accessible only by Erasmus University Rotterdam members that have "need-to-know" to process PD.</p> <p>* (PD) Personal Data</p>	<p>Accessible by restricted members of staff or students, on a "need-to-know" basis. Should be additionally labeled as SCPD if the document consist Special Categories Personal Data.</p> <p>SCPD &amp; PD may be accessible only by Erasmus University Rotterdam members that have "need-to-know to process PD or SCPD.</p> <p>*(SCPD) Special Categories Personal Data</p>	<p>Accessible only to designated or relevant members of staff or scientists, due to its potential critical impact on the Erasmus University Rotterdam, including critical financial or critical reputational damage.</p>
Level of risk if released inappropriately	None	<p>Low</p> <p>Should it fall into the wrong hands could be harmful (slightly damaging) to people or organization.</p>	<p>Medium</p> <p>Should it fall into the wrong hands could cause serious damage to people or organization.</p>	<p>High</p> <p>Should it fall into the wrong hands could cause severe (critical) damage to people or organisation.</p>

# 6. Security and privacy: data classification

EUR Data Classification Model

	CLASSIFICATION PUBLIC	CLASSIFICATION INTERNAL (*PD)	CLASSIFICATION CONFIDENTIAL (*SCPD)	CLASSIFICATION SECRET
Transmission / Transport / Storage / Archiving	No Restrictions	<p>PAPER information must be stored in lockable cabinets and kept from persons that don't have any "need-to-know" (visitors, cleaners, movers etc...)</p> <p>Remove sensitive mail content before sending the mail to external organizations (declassify to CLASSIFICATION PUBLIC)</p> <p>Sending INTERNAL/PD information (documents) outside own organization must be done with Surffilesender. Use of password is mandatory. Password sharing allowed through the mail.</p> <p>Sending INTERNAL/PD information to own private email environment is prohibited.</p> <p>NETWORK Storage: INTERNAL/PD Information must be stored in shared folders</p>	<p>PAPER information must be stored in lockable cabinets and kept from persons that don't have any "need-to-know" (see INTERNAL, including the co-workers from other departments or units)</p> <p>Printing CONFIDENTIAL information should be reduced to minimum.</p> <p>Remove sensitive mail content before sending the mail to external organizations (declassify to CLASSIFICATION PUBLIC)</p> <p>Sending CONFIDENTIAL/SCPD information (documents) outside own organisation must be done with Surffilesender. Use of password is mandatory. Password sharing only through SMS.</p> <p>Sending CONFIDENTIAL/SCPD information to own private email environment is prohibited</p>	<p>PAPER information must be stored in security safe or vault. Need-to-know strictly reserved for a designated few. Hard copies of documents should be hand delivered internally.</p> <p>Printing SECRET information should be avoided. Copying SECRET documents should be avoided. Copied or printed documents must be marked with a follow number and registered which recipients received a copy.</p> <p>Securing the document with the password (encryption) is mandatory. Password sharing only through SMS.</p> <p>Remove sensitive mail content before sending the mail to external organizations (declassify to CLASSIFICATION PUBLIC)</p>

# 7. Register of processings

<b>General</b>		<input checked="" type="checkbox"/>	Please select:	
<b>1. Please specify the type of your research</b>			Academic	
			Non-Academic	
<b>2. Which individuals / groups (partners / providers) outside the EU, have access to your dataset?</b>				
		<input checked="" type="checkbox"/>		
<b>Details concerning the research and datasets</b>			Select all that apply:	
<b>3. Which categories of personal data do you use in your dataset?</b>			Given name and surname	Financial data
			Business contact information	Logging information records
			Private contact information	Location data (GPS tracking or wifi tracking)
			Address information	Images (photos or videos)
			Gender	Profiling data (e.g. consumer profile)
			Date of birth or age	Demographic data
			Personnel number/student ID number	Other
			Marital status	Not Applicable
			Bank account data	
<b>4. Do you process special categories of personal data?</b>		<input type="radio"/>	Yes	
		<input type="radio"/>	No	
		<input type="radio"/>	Not Sure	
<b>4.a Which special categories of personal data do you use in your dataset?</b>		<input checked="" type="checkbox"/>	Select all that apply:	
			Nationality	Physical or mental health data
			Race or ethnic origin	Sexual preference or orientation
			Political views	Criminal data
			Religious or philosophical beliefs	Social security number / ID number
			Union membership	Not Sure
			Biometric data (such as fingerprints)	Not Applicable
		Genetic data (DNA)		

# 7. Register of processings

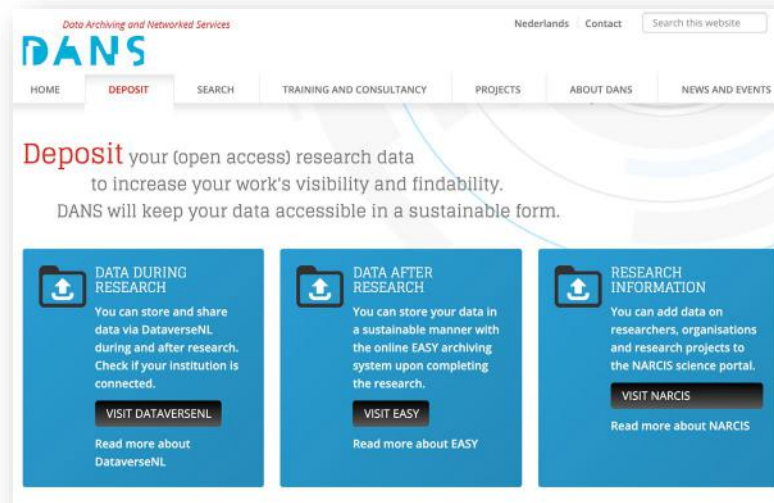
		✓		
<b>5. Who are the subjects of your research?</b>		✓	Select all that apply:	Justify your answer below:
			Children (<16 years)	
			Vulnerable groups	
			[University] students / alumni	
			[University] employees	
			Other	
<b>6. How do you obtain the data for your research?</b>		✓	Select all that apply:	Justify your answer below:
			Directly from individual	
			Publicly available data	
			Existing datasets	
			Other	
<b>7. What is the size of your subject population?</b>		✓	Select the size of the population:	
			less than 10.000	
			more than 10.000	
<b>8. Which hardware and software do you use?</b>		✓	Select all that apply:	
			[University] hardware	[University] licensed software
			Own device	non-[University] licensed software
<b>9. Please specify your software (not available with [University] credentials).</b>		↓	For example, OneDrive, Google Drive, Surveymonkey:	
<b>10. Does your research involve any of the following activities?</b>		✓	Select all that apply:	Justify your answer below:
			Evaluation/scoring	
			Systematic monitoring	
			Matching or combining datasets	
			Not Applicable	
<b>11. Supporting documentation.</b>		✓	Select all that apply:	
			Research data management plan	
			Agreement(s) with third parties	
			Consent form from the data subject	

# 8. Open Science and Privacy

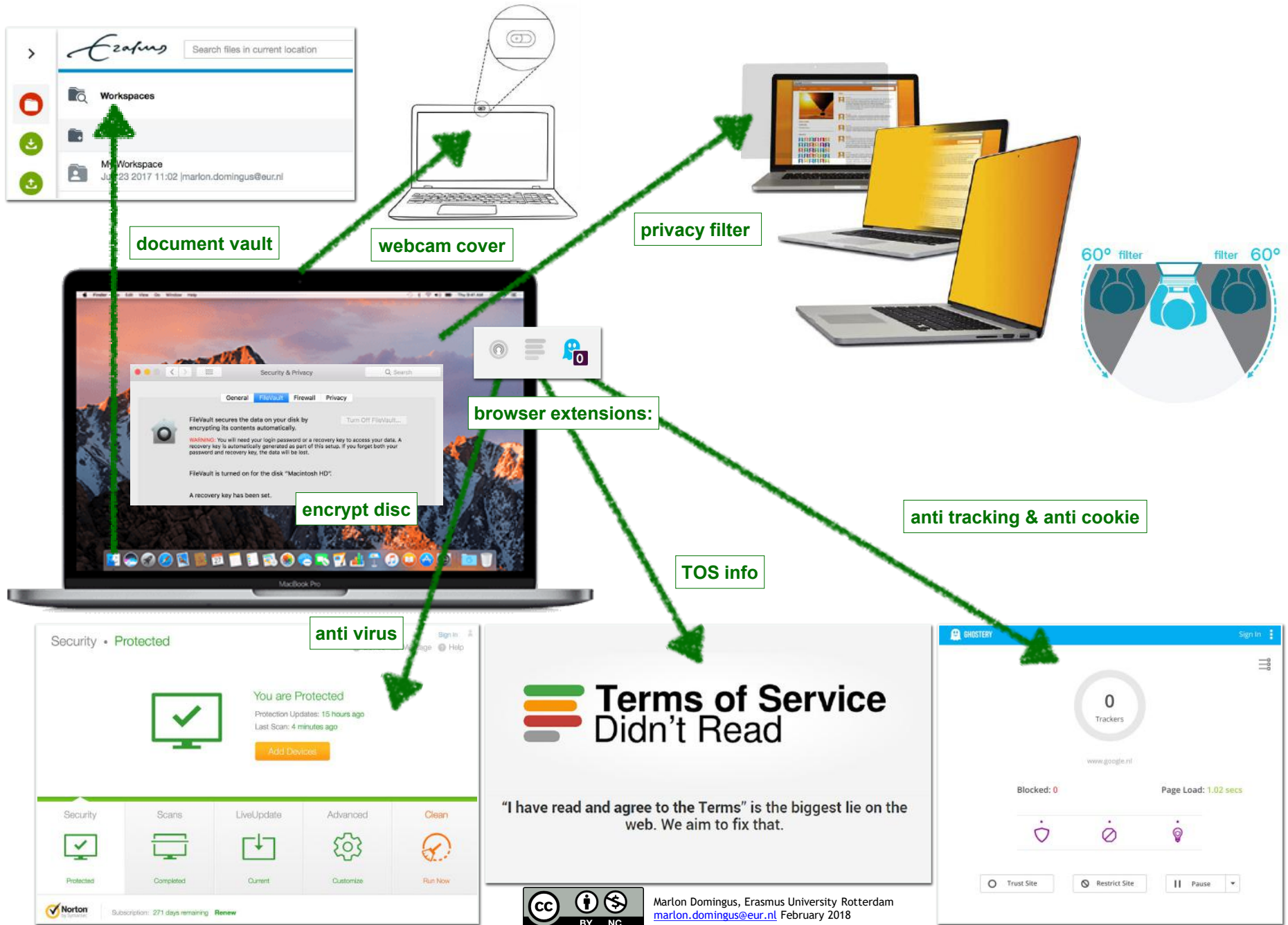
Door de instelling aan DANS aangeleverde anonieme data kunnen in [DANSeasy](#) worden gearchiveerd

Regisseren van [toegang](#) tot de onderzoeksdata:

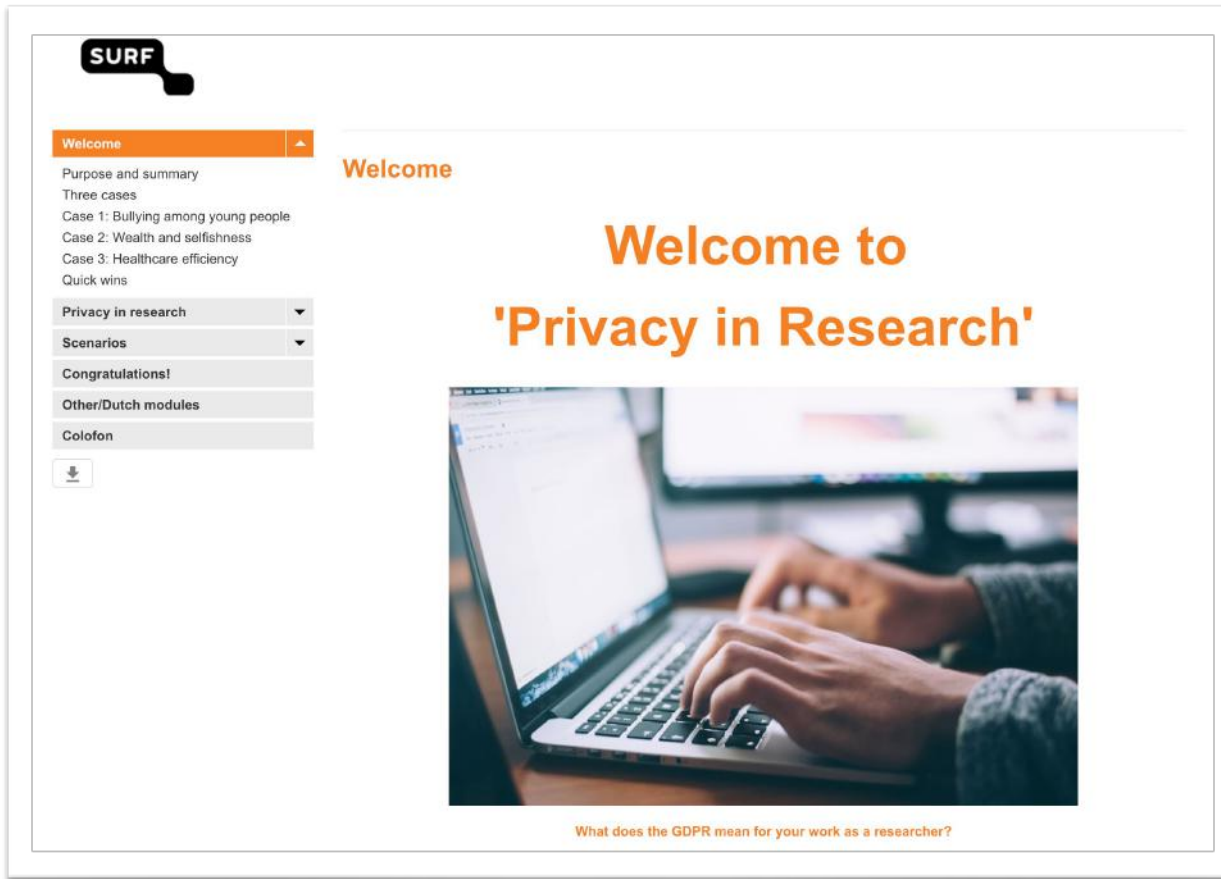
1. Open Access (CC0 Waiver) [metadata en data files toegankelijk voor iedereen]
2. Open Access voor Registered Users [metadata toegankelijk voor iedereen en data files toegankelijk voor geregistreerde gebruikers]
3. Restricted Access voor Registered Users [metadata toegankelijk voor iedereen en data files alleen toegankelijk na goedkeuring van de depositor op verzoek een Registered User]
4. Dark Archive [metadata en data files alleen toegankelijk voor een bekende lijst van Registered Users]



# The EUR Researcher's Guide To Mobile Security



# Take Aways



The image shows a screenshot of a course page from SURF. The SURF logo is in the top left. A navigation menu on the left includes 'Welcome', 'Privacy in research', 'Scenarios', 'Congratulations!', 'Other/Dutch modules', and 'Colofon'. The main content area features the title 'Welcome to Privacy in Research' in large orange text, a photograph of hands typing on a laptop, and the subtitle 'What does the GDPR mean for your work as a researcher?'.

**SURF**

**Welcome**

- Welcome
- Purpose and summary
- Three cases
  - Case 1: Bullying among young people
  - Case 2: Wealth and selfishness
  - Case 3: Healthcare efficiency
- Quick wins

**Privacy in research**


**Scenarios**

**Congratulations!**

**Other/Dutch modules**

**Colofon**

**Welcome to 'Privacy in Research'**



**What does the GDPR mean for your work as a researcher?**

Source: EN: [https://maken.wikiwijs.nl/125518/Privacy\\_in\\_Research](https://maken.wikiwijs.nl/125518/Privacy_in_Research)  
NL: [https://maken.wikiwijs.nl/117199/Privacy\\_in\\_Onderzoek](https://maken.wikiwijs.nl/117199/Privacy_in_Onderzoek)



# Questions?



**drs. Marlon Domingus, CIPP/e, CIPM**  
Data Protection Officer  
Erasmus University Rotterdam  
[dpo@eur.nl](mailto:dpo@eur.nl)

*Credits:* Annemieke Wiersema, Priscilla van Berkel, Robin van Vleuten, Navid Kamalzadeh en Ian van Loon voor slides 13 - 19.



Stay in touch via: <https://www.linkedin.com/in/domingus/>

# Infographics

## A RESEARCHER'S PRIVACY REFERENCE CARD

General Data Protection Regulation (GDPR)  
WHY? / WHAT? / HOW?

**INFORMATIONAL PRIVACY**  
**Protection of personal data**  
Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned.

**BE A TRUSTWORTHY RESEARCH PARTNER**  
Your focus on respecting fundamental rights and freedoms will not go unnoticed by research funders, research partners and the general public.

**PROTECT DATA SUBJECT'S RIGHTS**  
Be transparent about what happens with the data subject's data.

**LIMIT LIABILITY**  
Data subjects are to be fully and effectively compensated for the damage they suffer with regards to the processing of their personal data.

Controllers or processors involved in this processing are to be held liable for the entire damage. Furthermore, penalties including administrative fines are to be imposed for any infringement of the data subject's fundamental rights and freedoms.

**AVOID BAD PRESS**  
Damage to your reputation or your university's reputation, due to data leaks or other cases in which data protection where inadequate, is, for obvious reasons, generally undesirable.

**Privacy is a fundamental right.**  
Article 8, Charter of Fundamental Rights of the European Union; Protection of personal data.  
In a practical sense: why should I care about privacy and data protection in my research?

**ACT IN ACCORDANCE WITH THE LAW**  
Natural persons, whatever their nationality or residence, have the fundamental right to the protection of their personal data.

Processing of this data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation.

**TO BE ELIGIBLE TO EXTERNAL RESEARCH FUNDING**  
Research funders stipulate applying personal data protection practices in their funding conditions.

**BE A TRUSTWORTHY RESEARCHER**  
Be trustworthy by using of the subject's data with integrity, as a shared responsibility within the research institute.

**SHARE, ARCHIVE, PUBLISH RESEARCH DATA**  
Applying personal data protection practices, which no longer permits the identification of data subjects, ensures usage and reuse of your research data, which enables relevant data citations, thus providing visible credits for your work.

**SUPPORT:**  
Email: [researchsupport@eur.nl](mailto:researchsupport@eur.nl)  
Phone: +31 10 4088006

Marlan Domingos, November 2016, version 1.0  
<https://creativecommons.org/licenses/by-nc/4.0/>

## A RESEARCHER'S PRIVACY REFERENCE CARD

General Data Protection Regulation (GDPR)  
WHY? / WHAT? / HOW?

**INFORMATIONAL PRIVACY**  
**Protection of personal data**  
Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned.

**PURPOSE LIMITATION**  
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

**DATA PROTECTION IMPACT ASSESSMENT**  
A data protection impact assessment is performed to evaluate, in particular, the origin, nature, particularity and severity of the risk to the rights and freedoms of natural persons. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to process the personal data.

**STORAGE LIMITATION**  
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes.

**Privacy is a fundamental right.**  
Article 8, Charter of Fundamental Rights of the European Union; Protection of personal data.  
In a practical sense: what is privacy and data protection? What are the key concepts that I should be aware of?

**PERSONAL DATA?**  
'Personal data' means any information relating to an identified or identifiable natural person ('data subject').

**LAWFULNESS OF PROCESSING**  
Processing of personal data is lawful if the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

**INFORMED CONSENT**  
Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research.

**DATA MINIMISATION**  
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

**PSEUDONYMISATION**  
Pseudonymisation of personal data is one of the measures that can reduce the risks to the data subjects concerned, and help controllers and processors to meet their data-protection obligations.

**SUPPORT:**  
Email: [researchsupport@eur.nl](mailto:researchsupport@eur.nl)  
Phone: +31 10 4088006

Marlan Domingos, November 2016, version 1.0  
<https://creativecommons.org/licenses/by-nc/4.0/>

## HOW TO TREAT PERSONAL DATA IN RESEARCH?

Responsible use of personal data before, during and after research.

**PRIVACY BY DESIGN AND BY DEFAULT**

**BEFORE RESEARCH**

- Confidentiality**  
In your research design, address these six security and privacy goals, as identified by: [www.datenschutzzentrum.de](http://www.datenschutzzentrum.de)
- Participate in a data protection impact assessment** to identify risks and formulate countermeasures.
- Communicate the security and privacy measures** for your research in your data management plan and with all participants and data subjects.

**DURING RESEARCH**

- Make sure your data subjects** are well informed about the purpose of the research and their risks, before they sign the informed consent form.
- Only generate and use data** that are relevant for the purpose of your research; data minimisation.
- Use a computer with an encrypted hard drive**, encrypt your sensitive data, use SURFdrive for safe and secure file storage and sharing.

**AFTER RESEARCH**

- Anonymise and / or pseudonymize the data** and work with the de-identified data.
- Work safe: don't leave printouts on the printer or desk**, don't use public wifi, don't work where others can easily watch your screen or can hear you talk.
- During research feel free to consult us** in case of practical issues or just to reflect on aspects.
- Share your experiences with us**, contact us for support before, during and after research: [DATASUPPORT@URIB.EUR.NL](mailto:DATASUPPORT@URIB.EUR.NL) +31 10 4088006

**SEE ALSO:**  
[HTTPS://WWW.EUR.NL/RESEARCHMATTERS/RDM/RDM\\_SERVICES/](https://www.eur.nl/researchmatters/rdm/rdm_services/)

## PRIVACY For Academic Research COOKBOOK

case study: Eindhoven University of Technology

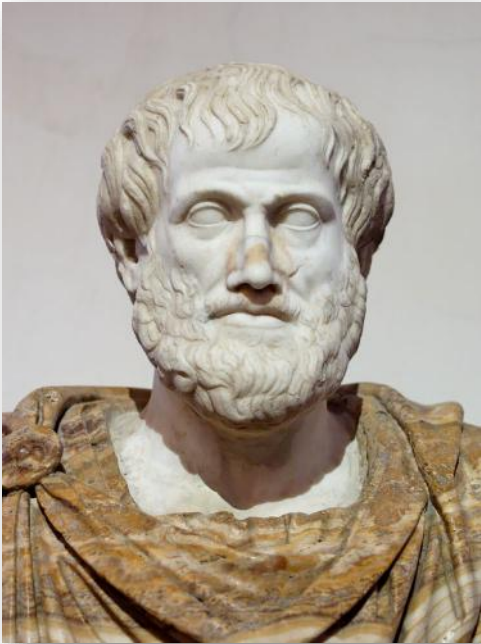
\* images are clickable links \*

- 1**  
Recognise that Research Data Management is a collaborative endeavour to enable responsible research. If personal data is used, safeguarding privacy for data subjects is a concern. Perform a Privacy Impact Assessment and add it to the data management plan.
- 2**  
Invest in exploiting the what, why and how of safeguarding privacy in academic research and provide the relevant support: infrastructure, tooling, instruments for data protection.
- 3**  
Assess the privacy readiness of your organisation and recognise the differences in perspective across the university. Develop a common language by collaborating in shaping privacy in academic research.
- 4**  
Define and implement a privacy strategy. Many great starting points are available.

Marlan Domingos | [domingos@lib.eur.nl](mailto:domingos@lib.eur.nl) | March 2017

# The GDPR Perspectives: Philosophy

[General Data Protection Regulation](#)



## Aristotle

GDPR Recital (4): 'The right to privacy is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.'

Aristotle's understanding of *moral virtue* provides logic for this balancing. *What would be adequate, given the situation, and what would be proportional (not too much and not too little).*

See more [here](#).



## Immanuel Kant

The GDPR has an underlying Kantian moral philosophy.

With Kant, we see as our *moral right*: safeguarding our own privacy and as our *moral obligation*: safeguarding the privacy of the individuals involved in our research.

See more [here](#).



Marlon Domingus  
Erasmus University Rotterdam  
[marlon.domingus@eur.nl](mailto:marlon.domingus@eur.nl)  
September 2017

**Credits:** [Aristotle](#): after Lysippos [Public domain], via Wikimedia Commons.  
[Kant](#): This file comes from Wellcome Images, a website operated by Wellcome Trust, a global charitable foundation based in the United Kingdom. See [Wellcome blog post](#).

The Erasmus University logo, featuring a stylized signature of the name 'Erasmus' in a cursive font.

# The GDPR Perspectives: Ethics

Kantian Moral Philosophy in two practical questions:

Q1 - Are you comfortable if you and your processing are on the frontpage of tomorrow's newspaper?

Q2 - Are you comfortable if your minor child is subject of your processing?

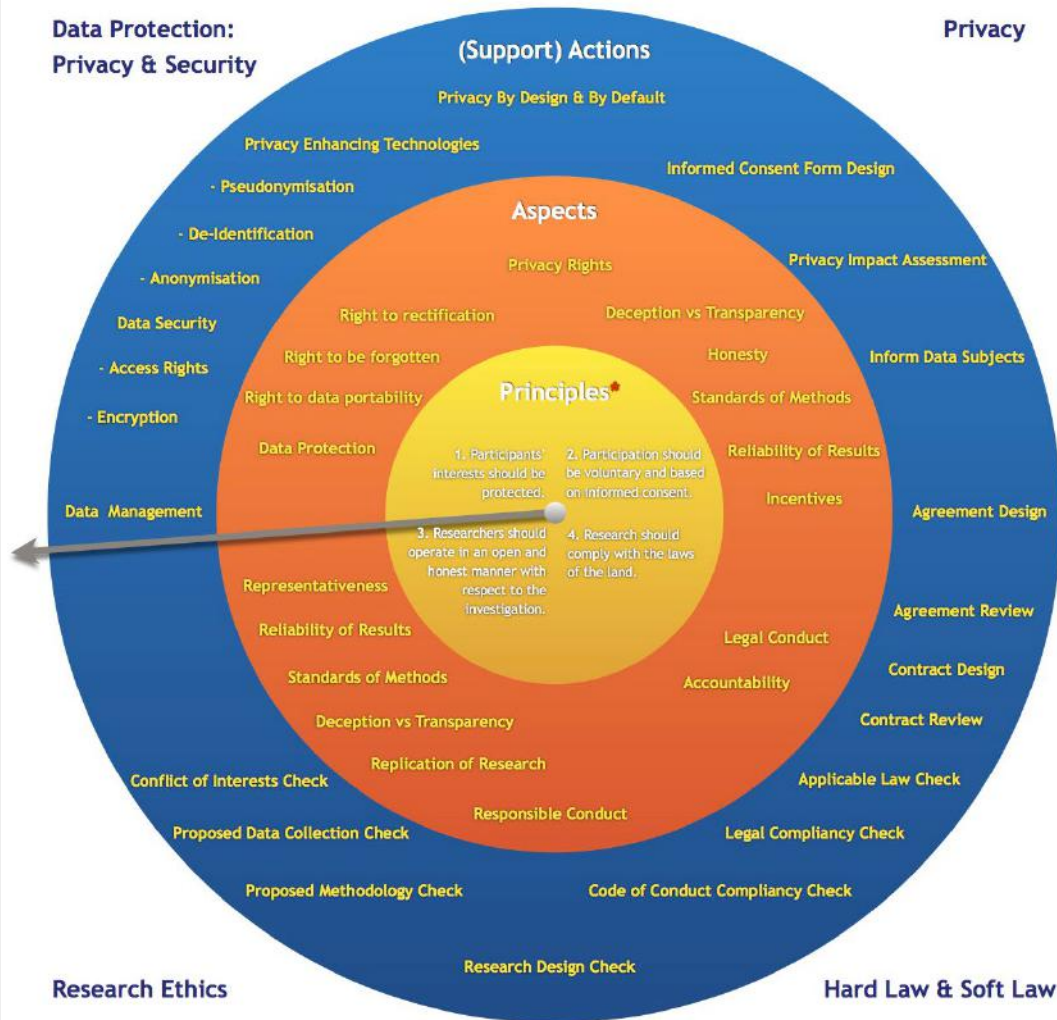
A stylized, handwritten-style logo for Erasmus, featuring a large, flowing 'E' followed by the word 'Erasmus' in a cursive script.

# Understanding Integrity.

An inquiry into the principles of proper academic practice.

## A Moral Compass.

Marlon Domingus. Erasmus University Rotterdam. May 30 2017.



## How to use the compass

In the core, the four Denscombe principles, serve as a starting point. In the next layer, the aspects related to these principles are listed. In the outer layer, the actions for faculty and/or research support staff are listed.

The arrow aligns the principles with the corresponding aspects and actions

Thus four quadrants appear, with a focus on the distinct aspects of research integrity. Traditionally ethics committees look at the aspects of the lower left quadrant. How to address the aspects in the rest of the compass? Suggestion: work together with the Data Protection Officer and the Legal Department for a new governing approach to assessing proper academic practices.



\* See: Martyn Denscombe, pp 329 - 343, The Good Research Guide. For small-scale social research projects. Fourth Edition. Maidenhead, England McGraw-Hill/Open University Press 2010.

# Research in Six Steps

CASE:

1

## Planning

- (DPIA)
- RDM
- Ethical Approval

## Data Collection

- Informed consent
- Joint Controller Agreements

## Data structure

- Pseudonymise personal data
- Encrypt keyfile and store separately from research data

## Store

- Store pseudonymised data in end to end encrypted collaboration platform

## Analyse

- Provide access and edit rights to research team members with start and end date. Use safe software.

## Publish & archive

- Publish data in a trusted repository
- Provide access compliant to Informed Consent

### COLLABORATION



**University &  
Non Academic  
Expert Centres**

### GEOGRAPHY



**Research  
within the  
Netherlands**

### DATA



**Video, audio,  
text, statistical  
data,  
databases**

# Research in Six Steps

## Planning

- (DPIA)
- RDM
- Ethical Approval

## Data Collection

- Existing data
- New measurements

## Data structure

- Pseudonymise personal data
- Encrypt keyfile and store separately from research data

## Store

- Store pseudonymised data in end to end encrypted collaboration platform

## Analyse

- Provide access and edit rights to research team members with start and end date. Use safe software.

## Publish & archive

- Publish data in a trusted repository
- Provide access compliant to Informed Consent

### COLLABORATION



**Public - Private**

### GEOGRAPHY



**EU funded research project, also outside the EU**

### DATA



**text, statistical data, databases**

# Research in Six Steps

CASE:

3

Planning

Data  
Collection

Data  
structure

Store

Analyse

Publish &  
archive

COLLABORATION



GEOGRAPHY



DATA

