GDPR & Academic Research 101

ADS Doctoral Day 21 March 2024

Koen Pepermans & Jeroen Van den Bergh
Data Protection Officer University of Antwerp

1 Who am I ? Who are we?

Data Protection Officer
Koen Pepermans

Jeroen Van den Bergh
staff member

- AAP and researcher 1995-2002
- Faculty director, Faculty of Social Sciences since 2002
- Advisor on information security research since 2008
- DPO since april 2018
- Chair of working group GDPR (VLIR)

Involved in different research projects/publications on and off where possible.

Governance structure

Advisory Board Privacy & Information Security UAntwerp

→ privacy policy preparation & information security issues

Questions about GDPR?

privacy@uantwerpen.be

hesk.uantwerpen.be/privacy (helpdesk and FAQ)

www.uantwerpen.be/disclaimer

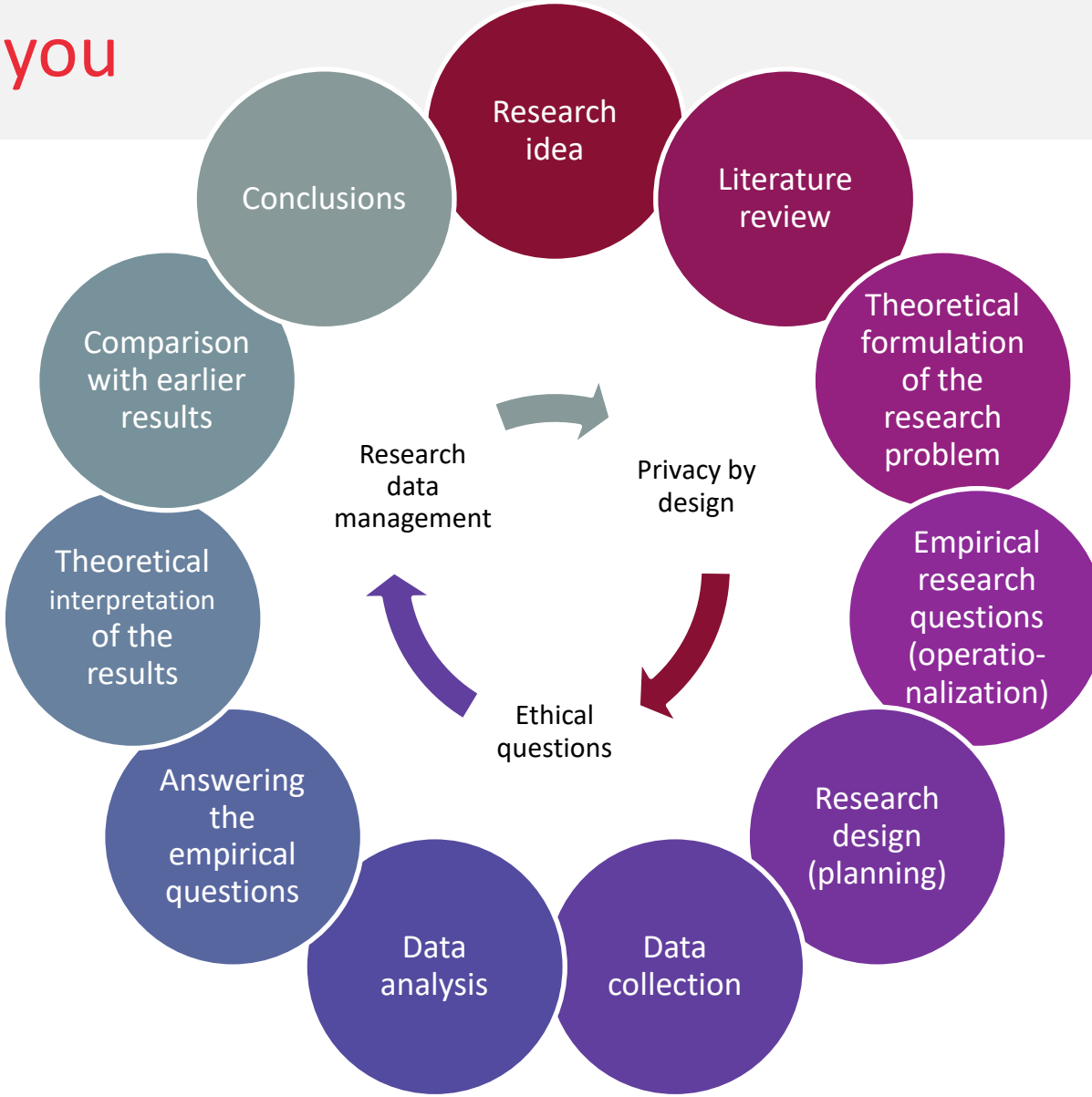
→ More information on the Pintra website

→ FAQ about GDPR and scientific research (in Dutch and English)

Some questions for you

Yes/no

- Are you using or planning to use personal data in your research?
- Do you feel you know what personal data are?
- Which kind of personal data?
- Do you know which steps you have to take when using personal data?
- Have you discussed this aspect with your promotor(s)?



2 Personal data

Personal data are described as all information about natural persons based on which they can be identified.
Sensitive personal data are described as particularly sensitive and therefore needs stronger protection, this also includes genetic and biometric data.
Pseudonymized personal data are personal data (whether sensitive) that can only be linked to an identified or identifiable person by means of a non-public key. Pseudonymized personal data remains personal data protected by the GDPR.

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone);
- an Internet Protocol (IP) address;
- a cookie ID;
- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person;
- Biometric identifiers (fingerprint, iris scan, face recognition, …)

But also …

"If, by looking solely at the information you are processing you can distinguish an individual from other individuals, that individual will be identified (or identifiable)."

Source: What is personal data? (2021). ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

3 What is the General Data Protection Regulation?

The *General Data Protection Regulation* aka GDPR (and *Algemene Verordening Gegevensbescherming* or AVG in Dutch) is the regulation that creates the framework for the data protection of personal data.

Why did we need a new set of rules in the EU?

- Fragmentation and legal uncertainty
- The perception that the online world creates significant risks for the protection of individuals
- Different rules limit economic growth
- Different implementation disturb and skew the common market

→ *cause: difference in implementation and use of the directive 95/46/EG*

The member states must screen and adapt national law for potential conflicts, terminology issues and double law rules with GDPR. They also must create new law for creating the necessary control bodies and for some specific domains where they have the opportunity to interpret the GDPR (f.e. scientific research, press, etc.)

→ The Belgian law was adopted July 2018.

4 Why is it important to comply with GDPR as a researcher?

Good and ethical handling of data increases the **quality and reliability** of the research and the research results

More and more questions about compliance when submitting a **publication**

A violation of the legal rules can lead to **reputational damage** and negative media attention to the university, your faculty, discipline or research group

Good and ethical handling of data can increase the **confidence of citizens** and research objects in science and the university

Obligation imposed by Flemish and Belgian authorities and funding agencies/clients (e.g. Horizon 2020, ERC, FWO, BOF, …)

A violation of the legal rules can result in **fines** that can amount to 20 million euros for the organization

Meeting the new requirements for processing of personal data in administration and research is important for several reasons.

If primary data are collected correctly, this also gives **legal certainty** to use these as secondary data in further analyses

5 General principles of GDPR

LAWFULNESS & FAIRNESS OF PROCESSING

Data subjects must give consent and be informed of how their data will be processed, and processing activities must align with how they are described.

PURPOSE & INTENT OF PROCESSING

Personal data can only be obtained for "specified, explicit and legitimate processing purposes" the subject has been made aware of and no other, without further consent.

DATA MINIMIZATION

Data collected on a subject should be limited to what is necessary in relation to the purposes for which it is processed.

ACCURACY & UP TO DATE

It is now the obligation of the data controller to ensure (to the best of their abilities) that the information collected is correct and current.

RETENTION LIMITATIONS

All personal information must now have an expiration date applied appropriate to its collected purpose, after which it must cease to be available.

SECURITY

Processors must handle data to ensure appropriate security, including protection against unlawful processing, accidental loss, destruction or damage.

Illustration from www.aprio.cm

6 Role of the University of Antwerp

Internally

- **Inform** and raise awareness
- Review and **control** of processing activities.
- **Ensure** information security measures.
- **Document** measures.
- Procedure to act quickly in case of a **data breach**
- Procedure to **guarantee** the rights of data subjects

Working together

- Representation at the Flemish Inter-University Council (VLIR) level (working group GDPR)
- Common solutions for the academic sector
  - FAQ for the researcher
  - Common questions in the register
  - In future a charter and/or code of conduct for scientific research
- Lobby-ing
- Within YUFE/Yerun (our academic networks)

Role of the University of Antwerp (2)

Data processing register for academic research

- Separate data processing register for academic research at the UAntwerp via **Antigoon** (the UA research database)
- For every new research project processing personal data
  - → *The same questionnaire is used by the 5 Flemish universities (engagement at VLIR level)*
  - → *The questionnaire also contains a brief risk analysis that indicates whether a full Data Protection Impact Assessment will have to be done*

Looking for assistance?

- DPO together with the Department of Research, Innovation & Valorisation Antwerp (RIVA) provides general information via Pintra-subsites and helpdesk
- Specific questions?
  - Need a Data Processing Agreement (contract)
  - A declaration by the DPO for the funding agency
  - A protocol for Flemish data
  - Advice on consent form
  - Advice on good practices
  - Other questions?




7 Role of every employee or researcher at UAntwerp

What can I do? Part I

- Educate yourself: information is available internally and online: Be aware of the importance of using the personal data for the purpose it was collected when using the different systems
- Be (a bit) paranoid! If you get an email, call or text message unexpectedly be careful
- Create a safe physical and digital working environment
- Lock your office & lock your screen
- Think before sharing data (keep access to personal data limited to collaborators with a role in the processing of data)
- Know and follow guidelines (GDPR, RDM, dual use, clinical trials, scientific integrity)

- Use the standard tools and software as much as possible provided by your university
- When using other software, go for a paid licence and check with colleagues, your IT departement, DPO and/or research departement
- Use the personal and shared file servers of your organisation (they normally come with backup and snapshots)
- Update your devices (laptop but also smartphone, tablet, smart devices)

When in doubt consult us via helpdesk or email

University of Antwerp

ICT SAFETY COLLECTIVE

What can I do? Part II

Report every incident or data breach!

- Encrypt your data in rest (f.e. Veracrypt, Bitlocker)
- Encrypt your laptop, computer of USB-stick/disk
- **Send only encrypted data (f.e. Belnet Filesender) and not via e-mail**
- Use VPN when working on an external network (f.e. airport WIFI)
- If you export data to local files for specific tasks, do not keep them unnecessary

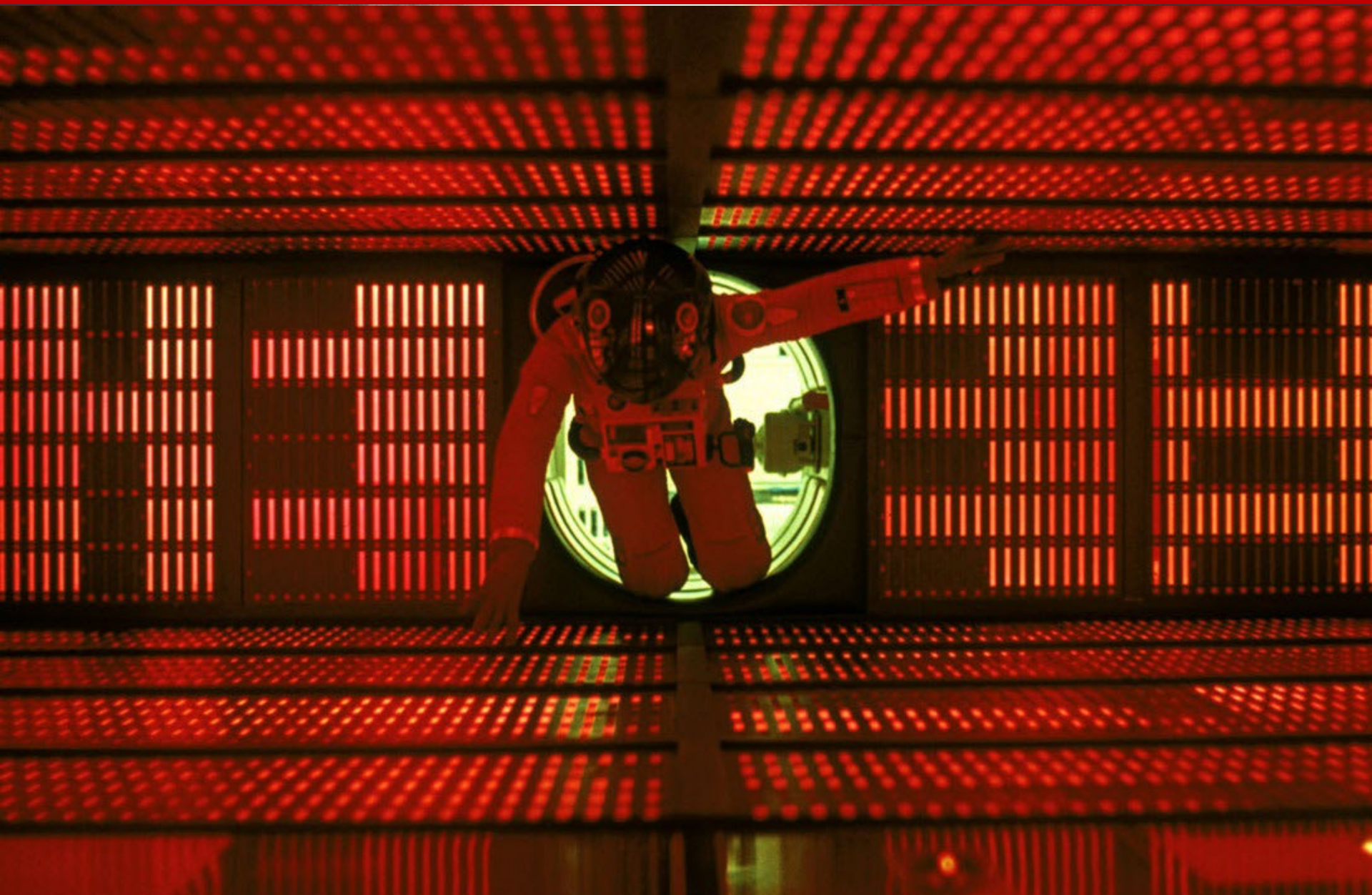
- Use different and long passwords for every application/website (with a password-manager)
- Use Multi Factor Authentication where possible (coming at Uantwerp)
- Don’t share passwords

- Make & test backups (and a backup of your backup)
- Data minimization: try to limit the data you use to what you really need
- Use pseudonomized data in your analysis as soon as possible

- Inform participants transparantly
- Be open about your goals
- Use a Research Data Management Plan
- View the questions from ethics committees and DPO’s as an opportunity to reflect not as a burden

Tip: how to achieve FAIR data and good Research Data Management
https://youtu.be/TEnq2P0r4mo

What can I do? Part III



Questions to ask regarding research: part I

Will I be using personal data? And do I need to?	Yes, no, not sure
What type of personal data?	Regular personal data Sensitive personal data
Will I use existing data or collect my own?	Primary data Secondary data
How will I or our team collect or have acces to these data?	Observation, survey, interview, experiment, statististical data (Kruispuntbank, Statbel, RIZIV), company HR-data, (existing) medical files, …
If secondary data, does my research fall within the information provided to the data subjects?	Yes, no, not sure
Is my research subjected to other regulations or rules?	f.e. Clinical trials, dual use, …
Do I have to subject my research (proposal) to an ethics screening?	In principle always when using personal data. **Ethics Committee for Social Sciences & Humanities (EA SHW)** Will the research involve human participants taking part in surveys, interviews, observation studies,…? **Committee for Medical Ethics UZA-UAntwerp (CME)** Will experiments be conducted on humans and/or human samples in the research?
Which legal basis is appropriate?	Informed consent Public interest Contractual (?)

Questions to ask regarding research: part II

How do I limit the risks for the participants?	Small N-analysis Encryption in rest Strict limits on access
Have I documented who needs access to the data?	At what level? All the data or a subset
Have I split the personal data from the research data where possible?	Best practice to separate personal identifiers from the earliest possible time from the research data (if possible) Pseudonomisation
What are the risks for my participants if there is a data breach?	By taking the previous steps this can be mitigated
Where do I store my data?	Use the standard tools provided by the university (Sharepoint/UA Network drives) and not free storage (f.e; Google Drive, free Dropbox)
Can my data be used for secondary analysis?	This depends on the information provided during the collection of the primary data.
How long will I need to keep the (personal) data?	The advice is in principle a maximum of 10 years
Will I collaborate with other partners?	Within the EU/EEA of outside? Need for Data Sharing Agreements etc.

→ More information in the FAQ GDPR for reseachers (see helpdesk Privacy)

Checklist for the researcher (example)

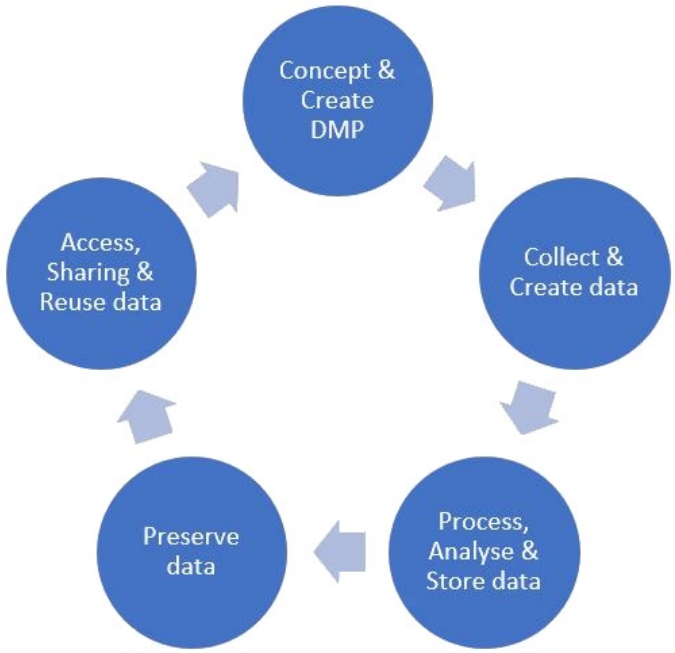
1. I understand whether my research data is personal data ☐
2. I have considered the need for a data protection impact assessment ☐
3. I have incorporated the necessary safeguards to use personal data ☐
4. I use contractors that process personal data securely ☐
5. I have suitable arrangements for international personal data transfers ☐
6. I shall use personal data fairly to recruit research participants ☐
7. I understand research participants' rights over their personal data ☐
8. I have prepared the necessary privacy information for participants ☐

Source: *Information Governance | University Services and Schools | Toolkit | The University of Aberdeen*. (2021). Information Governance - Aberdeen. https://www.abdn.ac.uk/toolkit/services/information-governance/

8 What is the link with Research Data Management?

The Research Data Management (RDM) includes all steps of the 'Research Data Life Cycle': **planning, creation, processing, analysis, storage, preservation, access, sharing and reuse**. All these steps are bound by conditions and regulations at both legal, ethical and technological levels.

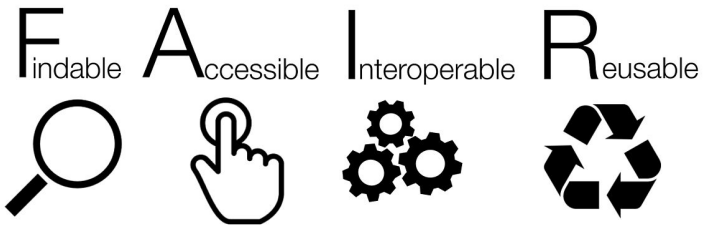
Pintra → Start > Mijn Subsites > Department of Research Affairs & Innovation > Publishing & Data > Research Data Management



The Research Data Life Cycle

Compliance with GPDR, together with research integrity, is one of the most important parts of this cycle when using/processing personal data.

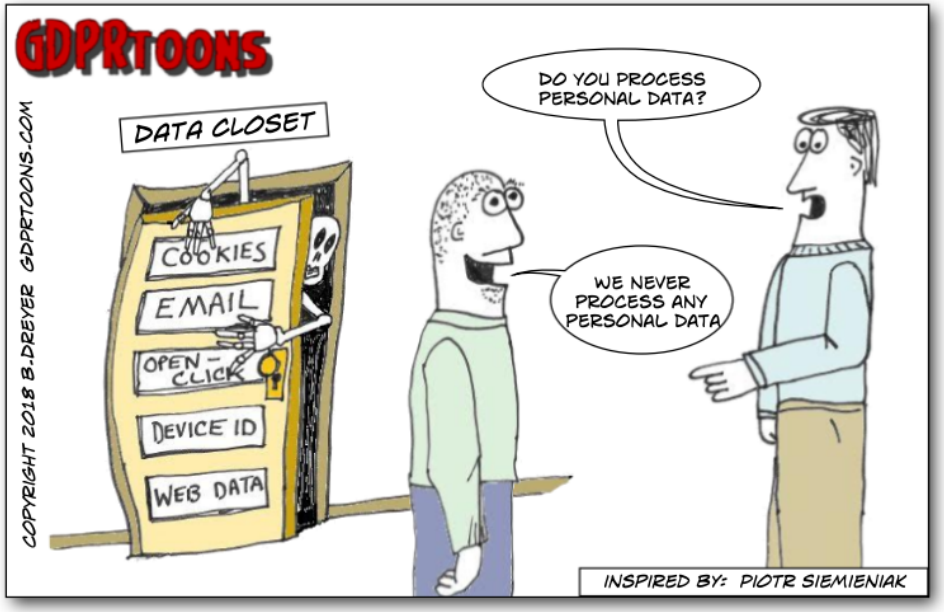
In **Data Management Plans** questions regarding the use of personal data are standard.
See also dmponline.be



9 GDPR and scientific research (1)

Role of the researcher (aided by the experts)

- As a researcher you are obliged to work within the guidelines and procedures of the university
- The researcher has to follow the appropriate security measures and take part in protecting the (research) data.
- Questions from respondents (if applicable) have to be responded to (in cooperation with the promotor and data protection officer).
- The researcher has to be aware of the correct practices when using personal data



GDPR and scientific research (2)

Role of the promotor

- As a promotor you are obliged to work within the guidelines and procedures of the university
- The promotor has to ensure that the information in the register is accurate and up-to-date.
- The promotor has to ensure that the appropriate security measures are taken and documented to protect the (research) data.
- Questions from respondents (if applicable) have to be responded to (in cooperation with the data protection officer).
- The promotor has to inform the researchers of the correct practices when using personal data

→ FAQ for researchers about GDPR compiled by VLIR workgroup GDPR available (Pintra and helpdesk)

10 Q&A

Some Questions

- What about self-made images
  - Images made by others
  - Images of designs by others

- How to 'correctly' mention these images in articles and possibly edit them

- Using AI images and copyright

- Posting images on social media

The following slides give a more detailed overview of the different aspects of GDPR.

These are provided to read if you are interested in more examples and definitions.

5. General principles of GDPR

Illustration from www.aprio.cm

5. General principles of GDPR
a) Lawfulness & fairness of processing

Are my data subjects adequately informed?

- Data subjects must always be adequately informed in clear language what the purpose of the data collection is.
- This obligation needs always to be met.
- Pro-active
- Privacy statement!
- **(Informed) consent**

5. General principles of GDPR
b) Purpose & Intent of processing

On what basis can I process/use these personal data?

- Contractual basis
- Legal obligation
- Public task/interest
- A vital interest
- Legitimate interests
- Unambiguous consent

- Contractuele basis
- Wettelijke verplichting
- Algemeen belang
- Vitaal belang
- Gerechtvaardigd belang
- Ondubbelzinnige toestemming

Often this means using informed consent as the main basis of data processing. There is a discussion if Flemish universities are considered public authorities which could mean that public interest is the main basis.

5. General principles of GDPR
c) Data minimization

DATA MINIMIZATION

Data collected on a subject should be limited to what is necessary in relation to the purposes for which it is processed.

Is it necessary to process this amount of data in my project in order to achieve my goal?

- Adequate – sufficient to properly fulfil the state purpose of processing
- Relevant – has a rational link to that purpose
- Limited to what is necessary – you do not hold more than you need for that purpose
- Best to worst data type - Anonymous > Pseudonymous > Personal data

5. General principles of GDPR
d) Accuracy & Up To Date

ACCURACY & UP TO DATE

It is now the obligation of the data controller to ensure (to the best of their abilities) that the information collected is correct and current.

Is all the collected data correct?

- Is all the data collected up to date?
  - Depends on what you are using it for
- Is all the data accessible by those who need it?
- Data subjects should have the right to correct their data
  - Depends on what you are using it for

5. General principles of GDPR
e) Retention Limitation

Should we store all these data?

- If you no longer need the data delete it and/or anonymize it
- If you keep data for longer than necessary, use security safeguards to protect the data
- Exception on research data for secondary use
- Data subjects have a right to erasure (if possible)

What about the FAIR principles? **F**indable **A**ccessible **I**nteroperable **R**eusable data
→ *Try to take this into account in the research design*

5. General principles of GDPR
f) Security

SECURITY

Processors must handle data to ensure appropriate security, including protection against unlawful processing, accidental loss, destruction or damage.

Have enough measures been taken to protect the integrity and confidentiality of personal data?
→ privacy by design

- Organizational measures
  - Agreements on processing
  - Limitations of information
- Technical measures
  - ICT, user policy, network security
  - Secure use of computers
  - Logging
- Legal measures
  - Contracts
  - Privacy policy

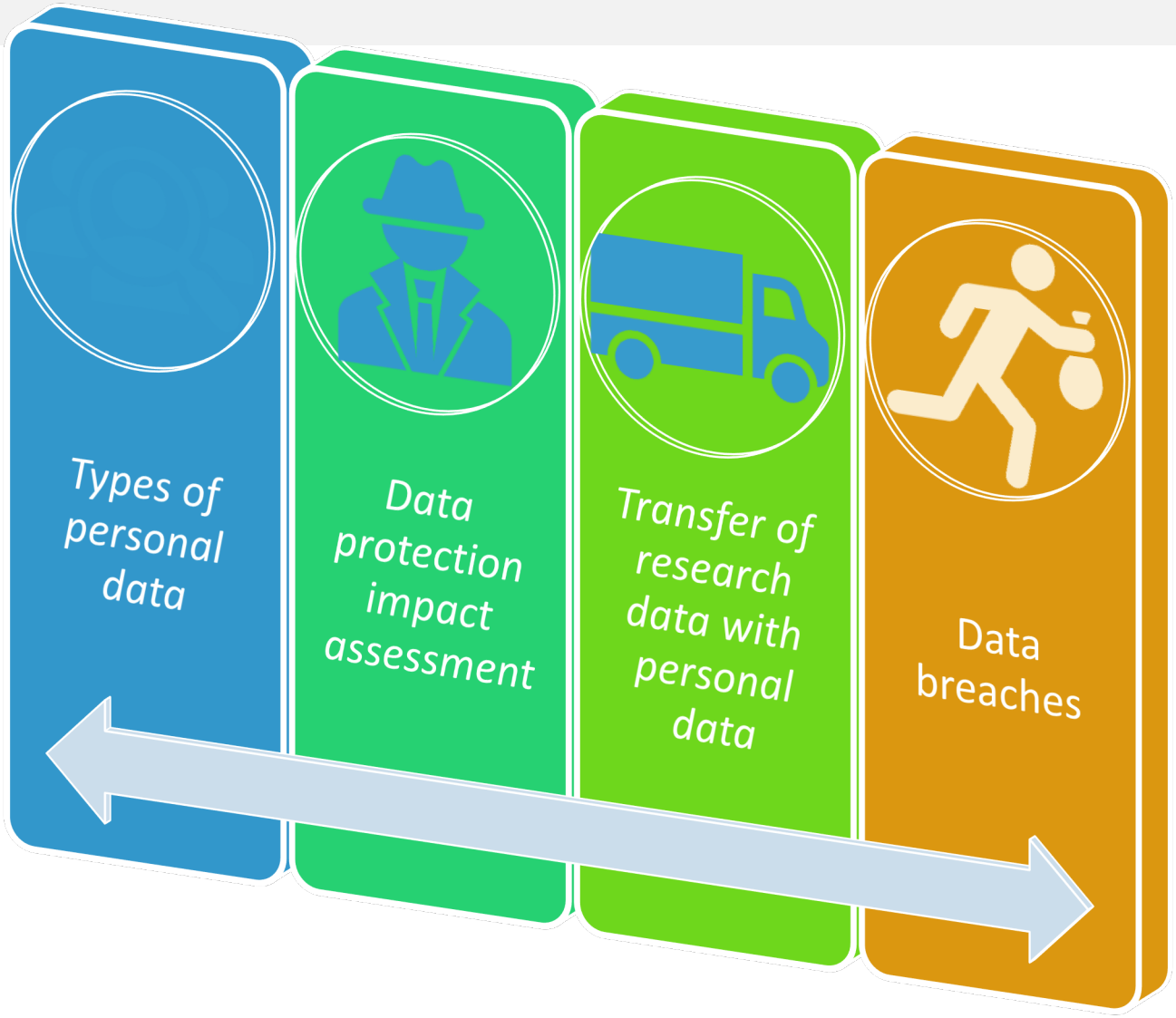
Importance of information security: campaign together with ICT and Process management and privacy office

6. Rights of the data subject

Are the rights of the person concerned sufficiently guaranteed?

- Right of access
- Right to rectification
- Right to erasure (or right to be forgotten)
- Right to restriction of processing
- Right to be informed
- Right to data portability
- Right to object to processing activities
- Right not to be subject to a decision based solely on automated processing, including profiling

7. Important definitions



7. Important definitions
a) Types of personal data

Types of personal data

Personal data are described as all information about natural persons based on which they can be identified. In addition to data with obvious 'identification data', such as name and date of birth, location and online data that are unique to a person (such as an IP address).

Sensitive personal data are described as particularly sensitive and therefore needs stronger protection, this also includes genetic and biometric data. Processing of sensitive personal data is as a rule prohibited but there are exceptions when there is a strong lawful ground for the processing of the data.
Data containing information about race, ethnic origin, political views, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, data about a person's sexual behavior or sexual focus. If this information becomes publicly available (eg as a result of a data breach), this can have very adverse consequences for those involved.

Pseudonymized personal data (formerly referred to as 'coded data') are personal data (whether sensitive) that can only be linked to an identified or identifiable person by means of a non-public key. Pseudonymized personal data remains personal data protected by the GDPR.

7. Important definitions
b) Data Protection Impact Assessment

Data protection impact assessment

A **data protection impact assessment** (DPIA, Gegevensbeschermingseffectbeoordeling of GEB in Dutch)

You must do a DPIA for processing that is **likely to result in a high risk** to individuals.

It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

Your DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

→ **Idea to add this to the register by default**

7. Important definitions
c) Transfer of research data with personal data

Transfer of research data with personal data

EU data protection rules apply to the European Economic Area (EEA), which includes all EU countries and non-EU countries Iceland, Liechtenstein and Norway. (On 28 June 2021, the European Commission announced that it had adopted an adequacy decision in respect of the UK's post-Brexit data protection regime.)

When personal data is transferred outside the European Economic Area, special safeguards are foreseen to ensure that the protection travels with the data.

The GDPR offers a diversified toolkit of mechanisms to transfer data to third countries:

- adequacy decisions (countries accepted as having a similar level of protection)
- standard contractual rules
- binding corporate rules
- certification mechanism (as accepted by certification bodies accredited on the national or European level)
- codes of conduct
- so-called "derogations" (specific exceptions provided in law)

→ Best practice is to include specific clauses in every contract with a partner university by default

7. Important definitions
d) Data breaches

Data breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

- If you become aware of a data breach (either yourself or by a communication from a third party), immediately inform the Data Protection Office via form, phone or e-mail > **privacy@uantwerpen.be** and also send a mail to **abuse@uantwerpen.be** for the IT-department
- If the breach is still ongoing, take appropriate measures (f.e. disconnect a server from the internet, move files to a secure location, change password of application)
- Every breach has to be registered at the university
- In case of a serious breach the Data Protection Authority (the former privacy commission) has to be notified within 72 hours

Q&A


GDPR
EU
DPO
data
protection
general
compliance
company
compliant
supervisory authority
consent
safety
processor
prepare
act
third party
breach
confidential
security
officer
protect
law
regulation
fine
transfer
access
privacy
technology
safeguard
password
european union
personal
business
secure
information
controller
filing system
rules
legislation

In a nutshell

http://www.top-sage-resellers.com/blog/gdpr-compliance-with-sage-300


GDPR