ICT SAFETY COLLECTIVE

Information security & GDPR

Implementation at the University of Antwerp

Data protection officer | Koen Pepermans

- Research and teaching assistant methods of social sciences 1995-2002
- Faculty director, Faculty of Social Sciences since 2002

- Advisor on information security research UAntwerp since 2008
- Data Protection Officer and Head of Process Management and Privacy Office since april 2018
- Member of working group GDPR (VLIR)

- Involved in different research projects/publications on and off where possible
- Owner www.kpsoft.be
- Passionate about ICT for more than 35 years

Security and risk officer | Naomi Huygen

- Bachelor of Laws (UAntwerpen)
- Master of Safety Sciences (UAntwerpen)

- Security and risk officer since 2018
- Member of the IT department

- Main job responsibilities
  - Developing an Information Security Policy
  - Establishment of Security Awareness
  - IT Security Incident Tracking
  - Provide advice regarding IT security and risk issues

- Member of working group cyber security (VLIR)

Data Privacy | Jeroen Van den Bergh

- Graduated Informationmanagement | specialization Privacy & Cyber Security since 2017
- Data Privacy since 2017
- Member of the Privacy and Procesmanagement Office

- Main job responsibilities
  - Implementation of GDPR and follow up on Art 22. Constitution of Belgium
  - Developing and maintaining a privacy culture
  - Establishment of Privacy Awareness
  - Putting privacy plans and/or actions into effect
  - Provide advice regarding privacy and personal data risk issues
  - Still dabbles in informationmanagement

- Member of working group GDPR (VLIR)
- Secretary advisory board GDPR (UAntwerpen)

Governance Structure

Advisory Board Information Security & Privacy

- **What is its responsibility?**
  - Policy preparation regarding privacy & information security
  - Consultative body for developing policies and specific issues

- **Who is taking part in this?**
  - Data Protection Officer
  - Security and Risk Officer
  - Faculty Directors
  - Head of Departments
  - Data Stewards
  - Legal Experts

Overview

1. What is General Data Protection Regulation?
2. What is information security?
3. What is the link between both?
4. What is the link with Research Data Management?
5. Why is it important to comply with the regulations?
6. What can you do?
7. In a nutshell
8. Contact information

University of Antwerp

1. 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.

1.1 What is the GDPR | Principles

Lawfulness and transparancy

Obtain the data on a lawful basis, leave the individual fully informed and keep your word

Purpose limitation

Be specific on the purpose of the data collected

Data minimization

Collect the minimum data you need

Accuracy

Store accurate up-to-date data

Storage limitation

Retain the data for a necessary limited period and then erase

Accountability

Record and prove compliance. Ensure policies

Integrity and confidentiality

Keep it secure

1.2 What is the GDPR | Personal data

Personal data are described as all information about natural persons based on which they can be identified.

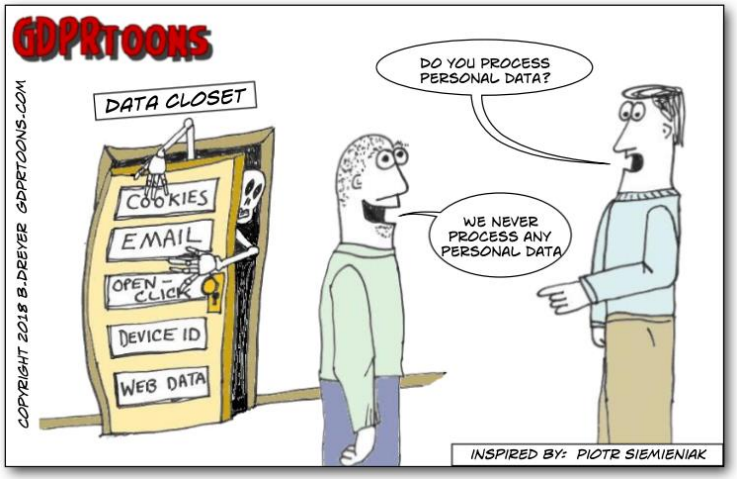
Sensitive personal data are described as particularly sensitive and therefore needs stronger protection, this also includes genetic and biometric data.

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;
- …

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/

1.3 What is the GDPR | 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

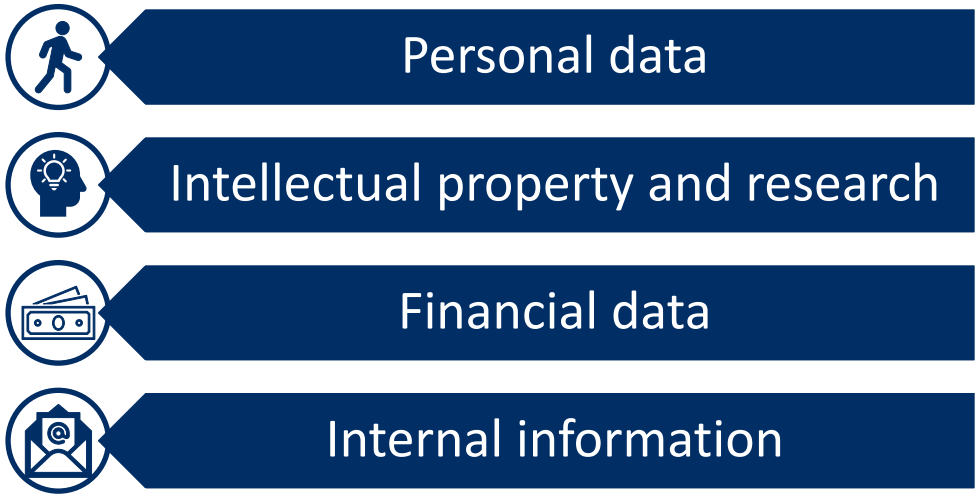
2. What is information security?

The protection of **information** and **information systems** from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide **confidentiality, integrity, and availability**.

© https://www.securitymadesimple.org/cybersecurity-blog/what-are-the-3-principles-of-information-security

2. What is information security? | Importance

As a university, we process a lot of information on information systems.



What would happen if…

C Unauthorised persons accessed confidential information?

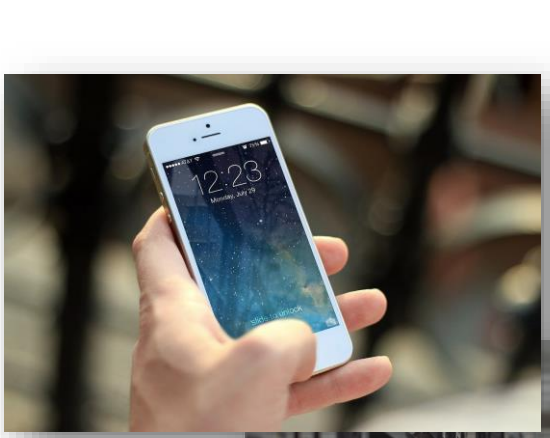
I Information was no longer accurate?

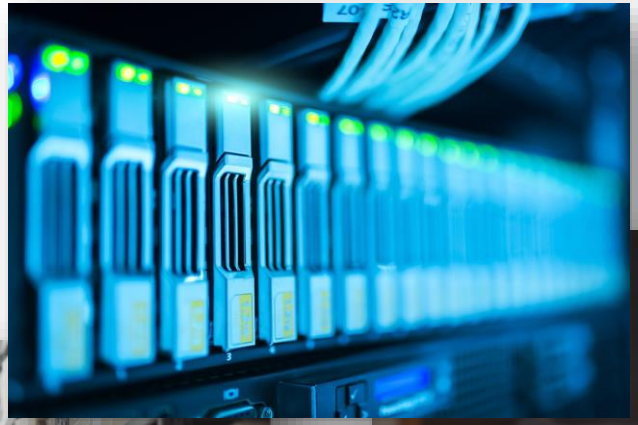
A Information was no longer available?

3. What is the relationship between GDPR and Information Security?

Personal data is a type of information. Whereas the GDPR focuses on personal data, **the focus of information security is broader**.

As the University of Antwerp, we must comply with the privacy legislation. However, it is important that we **protect information in the broad sense** in our own interest.

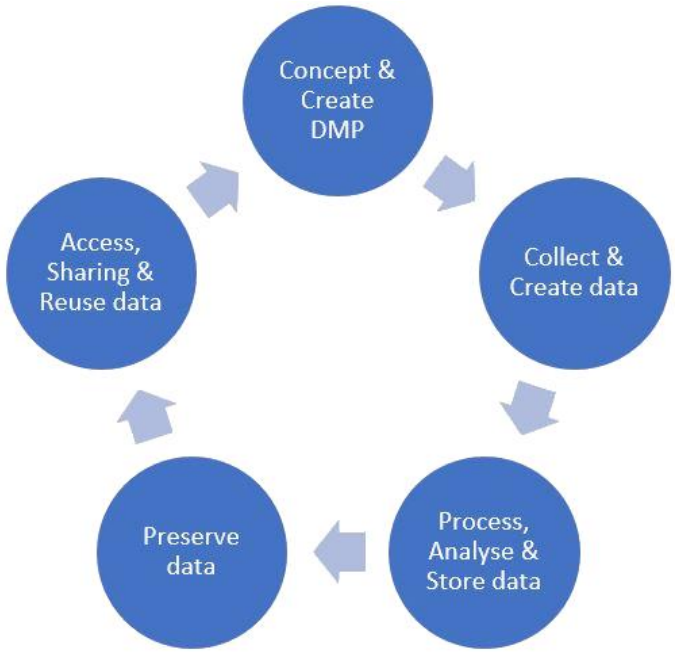




4. What is the link with Research Data Management?

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

5. Why is it important to comply with GDPR?

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

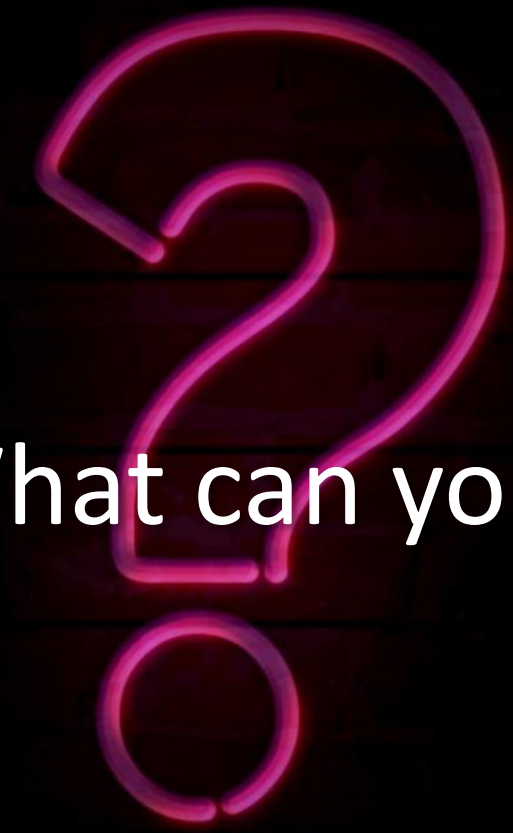
Good and ethical handling of data can increase the **confidence of citizens** and research objects in science and the university

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

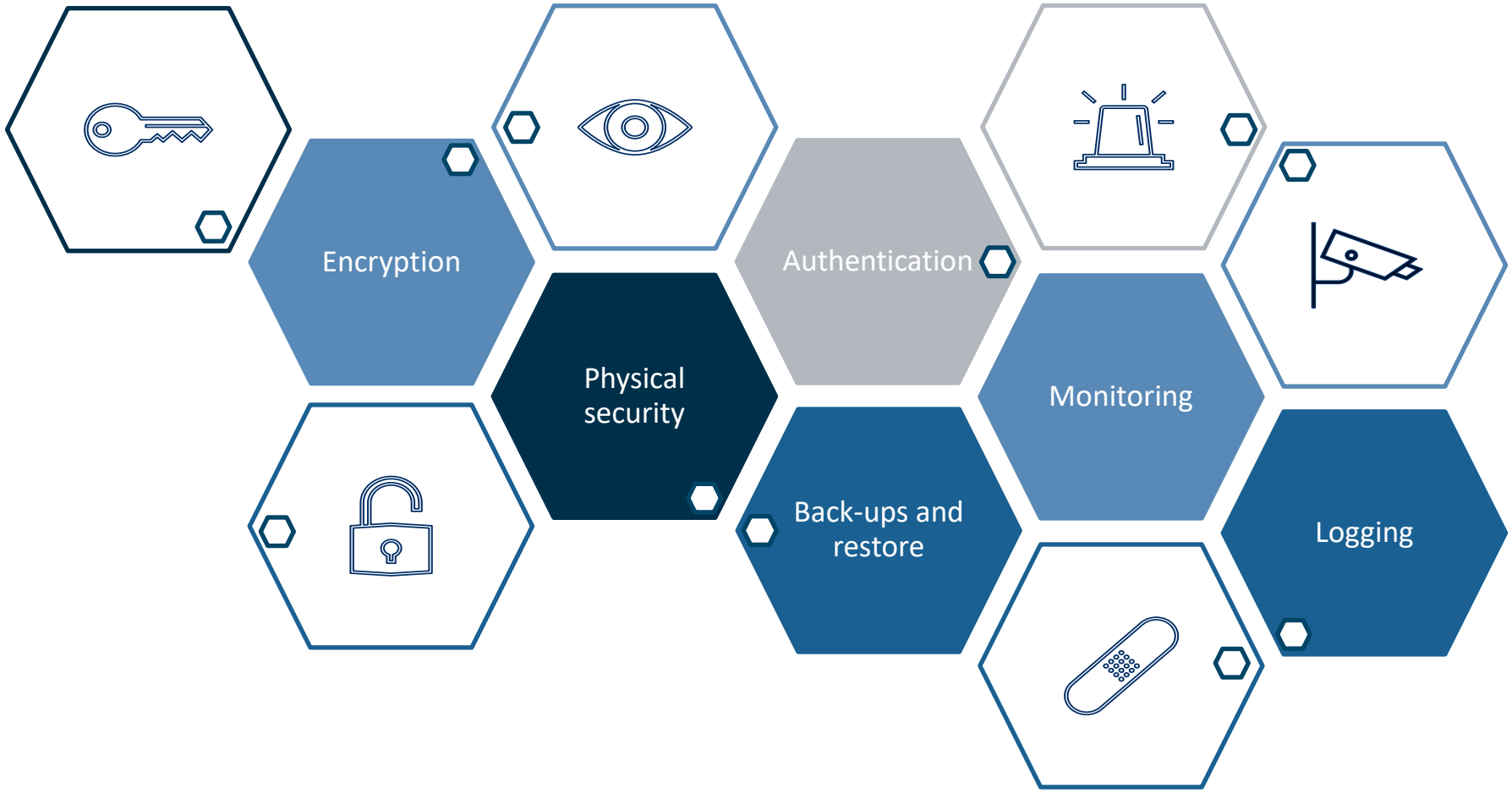
Meeting the new requirements for processing of personal data in administration and research is important for several reasons.

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

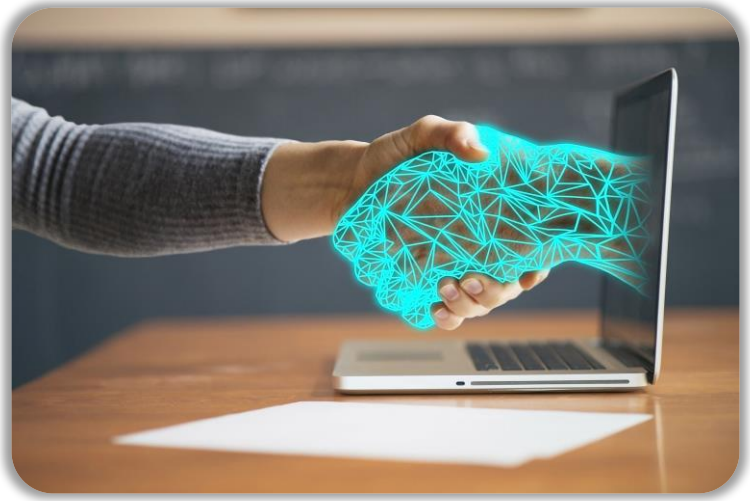


5. What can you do?

6.1 What can you do? | Technical measures



6.1 What can you do? | Organisational measures



Unfortunately, technical measures are not enough.

We need your help to keep the university and its data safe!

ICT Codes of conduct

Phishing Simulation

Internal Campaign

(Online) training

6.1 What can you do? | Internal campaign

To help our staff and students, we have developed an internal campaign.

Through this campaign, you will receive **various practical tips** on how to process information legally and secure.

https://pintra.uantwerpen.be/informatieveiligheid

6.1 What can you do? | Safe password (use)

Complex passwords

- Use **password phrases**:
  - My duck e@ts 2 times a day!
  - 27 characters, capital letter, number and special characters.
- Do **not** use **generally known** phrases ass a password!

Unique password for every account

- Do you have to remember too many passwords?
  - Use **password managers**!

Keep your password to yourself

- Do not give it to colleagues, family or friends.

6.1 What can you do? | Best Practices

Encrypt your drives so you can process (personal) data safely.

Be aware of the importance **of using the personal data for the purpose it was collected** when using the different systems.

Keep access to data limited to collaborators with a role in the processing of data.

Process your data as much as possible on **university resources** like:

Microsoft Teams | SharePoint | N drive

OneDrive for Business | H drive

Save costs!

Always **save important information on Teams, Sharepoint or N drive**, so it is accessible for your colleagues.

Be aware that information on OneDrive for Business or on H drive is in principle not accessible for other people.

Use **VPN** when you're **on a public WiFi**.

6.2 Practical Implementation | GDPR
a) Lawfulness & Transparancy

LAWFULNESS

- Contractual basis
- Legal obligation
- Public Task / interest
- Vital interest
- Legitimate interest
- Unambiguous consent

TRANSPARANCY

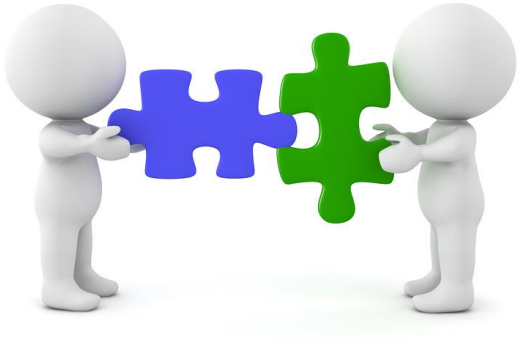
- Revise privacy statements regularly
- Informed consent adapted to the situation
- Be proactive
- Data Processing Registers as a supportive medium
- Use the correct documents for the right situation
    - DMP (research)
    - Antigoon (research)
    - Public websites
    - DPIA
    - ….

6.2 Practical Implementation | GDPR
b) Purpose limitation

- Comply with documentation from lawfulness principle
- Comply transparency obligations
- Secondary purposes
  - need to be compatible with the original purpose
  - Specific consent
  - A new clear legal provision

COMPATIBILITY

- Archiving purpose in the public interest
- Scientific or historical research purposes
- Statistical purposes
- New purpose is not different and not unexpected

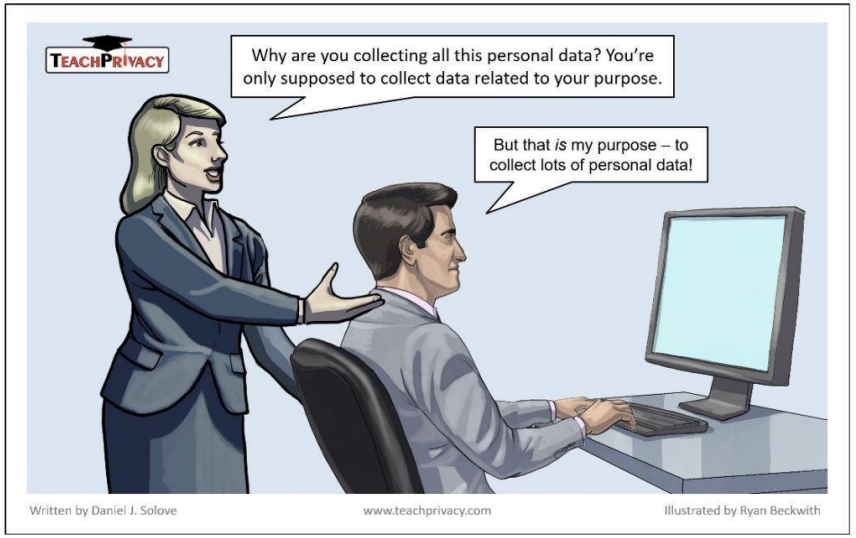


6.2 Practical Implementation | GDPR
c) Data minimization

How do you ensure data minimization?

How does the University of Antwerp do this?

- Narrow data collection
  - What is ‘’absolutely’’ necessary?
- Progressive data management – 3C’s (**Catalog**, Collaborate and **Comply**)
- User verification
- Strategic deletion
- ….. Accuracy and up-to-date



6.2 Practical Implementation | GDPR
d) Accuracy & Up To Date

How does the University of Antwerp keep data accurate and up-to-date?

- Employees have access to most of their personal data in Psoft
- Data is accessible by those who have the responsibility to keep it up-to-date
- The source of the data should always be checked
  - Especially in research
- Data subjects should have the right to correct their data
  - Where possible

6.2 Practical Implementation | GDPR
e) Storage Limitation

How can I comply with storage limitation?

- Regularly evaluate if data is still needed
- Follow the archive guidelines
- Exception on archiving purpose in the public interest
- Exception on research data
  - *Appropriate safeguards | pseudonymization, encryption, …*
  - FAIR Principles
  - Consent for publication
- Exception on statistical purposes
  - *Appropriate safeguards | pseudonymization, encryption, …*

6.2 Practical Implementation | GDPR
f) Accountability

- *How does the University of Antwerp proof its accountability?*
- *How can I proof my accountability?*

  - Clear leadership on Data Protection
    - Governance Structure
  - Documentation on currently adopted policies
  - Training awareness
  - Breach response
    - Breach notification within 72 hours
  - Compliance to individual rights
  - Records of processing – administration and research tasks

6.2 Practical Implementation | GDPR
g) Integrity and Confidentiality

- *How does the University of Antwerp maintain integrity and confidentiality?*

- Organizational measures
  - Personal data risk assessments
  - Internal teams for privacy and cyber security
  - Enforcing a privacy culture
- Technical measures
  - Password policy
  - Monitoring
  - Security and privacy by default
  - Robust IT security environment
- Legal measures
  - Contracts
  - Privacy policy

The University of Antwerp continuously strives to make the organization better and safer for its students, employees when it comes to Data Privacy and Protection!

6.3 Research

Role of the promotor

As a promotor you are obliged to work within the guidelines and procedures of the university.

The promotor must ensure that the information in the register is accurate and up-to-date.

The promotor must ensure that the appropriate security measures are taken and documented to protect the (research) data.

Questions from respondents (if applicable) must be responded to (in cooperation with the data protection officer).

The promotor must inform the researchers of the correct practices when using personal data

Role of the researcher

As a researcher you are obliged to work within the guidelines and procedures of the university

The researcher must follow the appropriate security measures and take part in protecting the (research) data.

Questions from respondents (if applicable) must be responded to (in cooperation with the promotor and data protection officer).

The researcher must be aware of the correct practices when using personal data

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

7. In a nutshell

- Keep the principles of GDPR in mind
- Make sure you work in a safe digital environment (for every type of data important)
- Be aware of the importance of using the personal data for the purpose it was collected when using the different systems
- Keep access to personal data limited to collaborators with a role in the processing of data
- If you export data to local files for specific tasks, do not keep them unnecessary
- Keep your data safe
- Be (a bit) paranoid when receiving requests or emails
- **When in doubt consult us via helpdesk or e-mail**

In a nutshell

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

Contact & more information

Privacy

- privacy@uantwerpen.be
- hesk.uantwerpen.be/privacy (helpdesk and FAQ)
- www.uantwerpen.be/en/about-uantwerp/organisation/mission-and-vision/privacy-policy/

Data breach

- https://forms.uantwerpen.be/nl/formulieren/personeel/data-protection/datalekken/

Information security

- https://pintra.uantwerpen.be/informatieveiligheid

Research data stewards

- Rdm-support@uantwerpen.be

ICT department

- helpdesk@uantwerpen.be
- Suspicious emails: abuse@uantwerpen.be

More information | Image usage

All images used in the presentation are property
of the respective owners and are used under fair use in education.

All the links to the sources of the images are in the annotations of the slides or on the slide itself.