ICT SAFETY COLLECTIVE

Information security & GDPR

General information session for the researcher

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

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

Overview

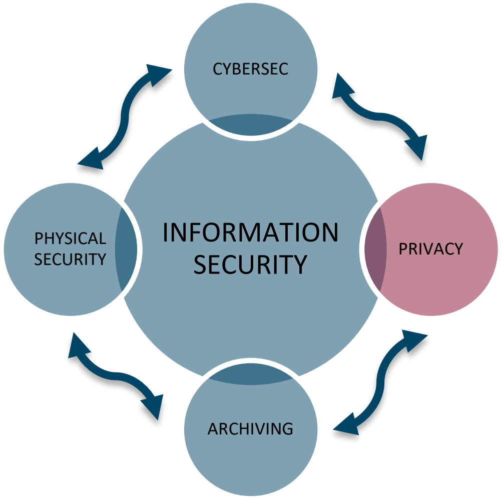
1. What is Privacy?
2. Why is it important to comply?
3. What does the university do?
4. What can you do?
5. In a nutshell
6. Contact information

1.2 What is privacy?

- Privacy is the right to be let alone, or freedom from interference or intrusion
  - Human Right according to UN Article 12

- Information privacy is the right to have some control over how your personal information is collected and used.
  - EU enforces information privacy through GDPR

- Privacy versus security…isn't it the same thing?
  - Not really
  - They are cousins
  - Data Privacy – governance of personal data
  - Security – Protecting data



1.2 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 personal data | Definition & Scope

ANY INFORMATION

✓Leading to identification
✓Sensitive

RELATING TO

✓An individual
✓A particular person
✓Impacts the person

IDENTIFIED OR IDENTIFIABLE

✓Direct
✓Indirect

NATURAL PERSON

✓Applies ONLY to a living human being

ONLINE IDENTIFIER & LOCATION DATA

✓Includes data provided by electronic devices we use

TO ONE OR MORE FACTORS

✓Includes data that when combined with unique identifiers and other info creates a profile to identify – pseudonymized data

1.2 Rights of the data subject

- The right to be informed
- The right of access
- The right to rectification
- The right to object to processing
- Right in relation to automated decision making and profiling
- The right to be forgotten
- The right to data portability
- The right to restrict processing

2. Why is it important to comply?

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

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

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

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

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

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

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

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

3.1 What does the university do? | 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 (Privacy)
  - Security and Risk Officer (IT)
  - Delegation from every faculty and administrative departement
  - Data Stewards (RIVA)
  - Legal Experts

3.2 What does the university do? | Actors

Procesmanagement & privacy office

- Privacy & privacy legislation

IT department

- Cybersecurity

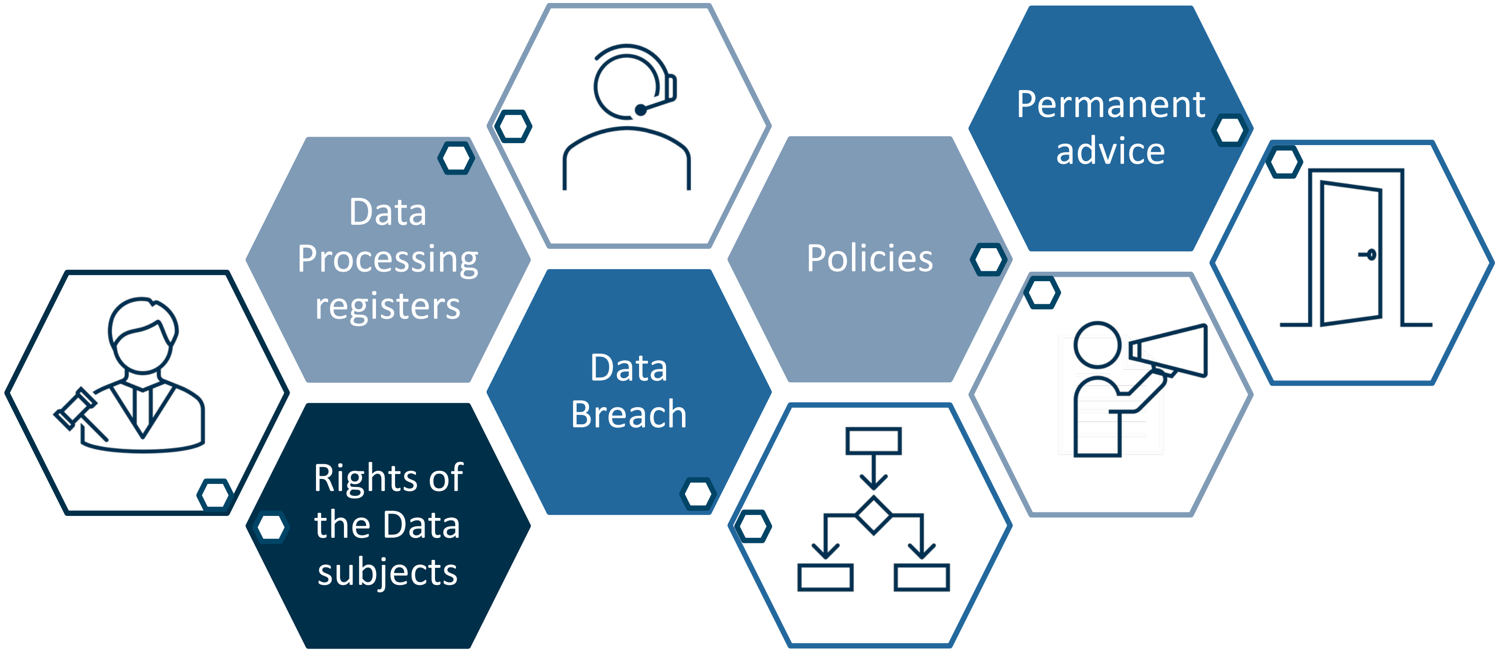
Library and archive department

- Securing information in the long run

RIVA

- Research – Intellectual property

3.3 Privacy | Organizational measures



Data Processing registers

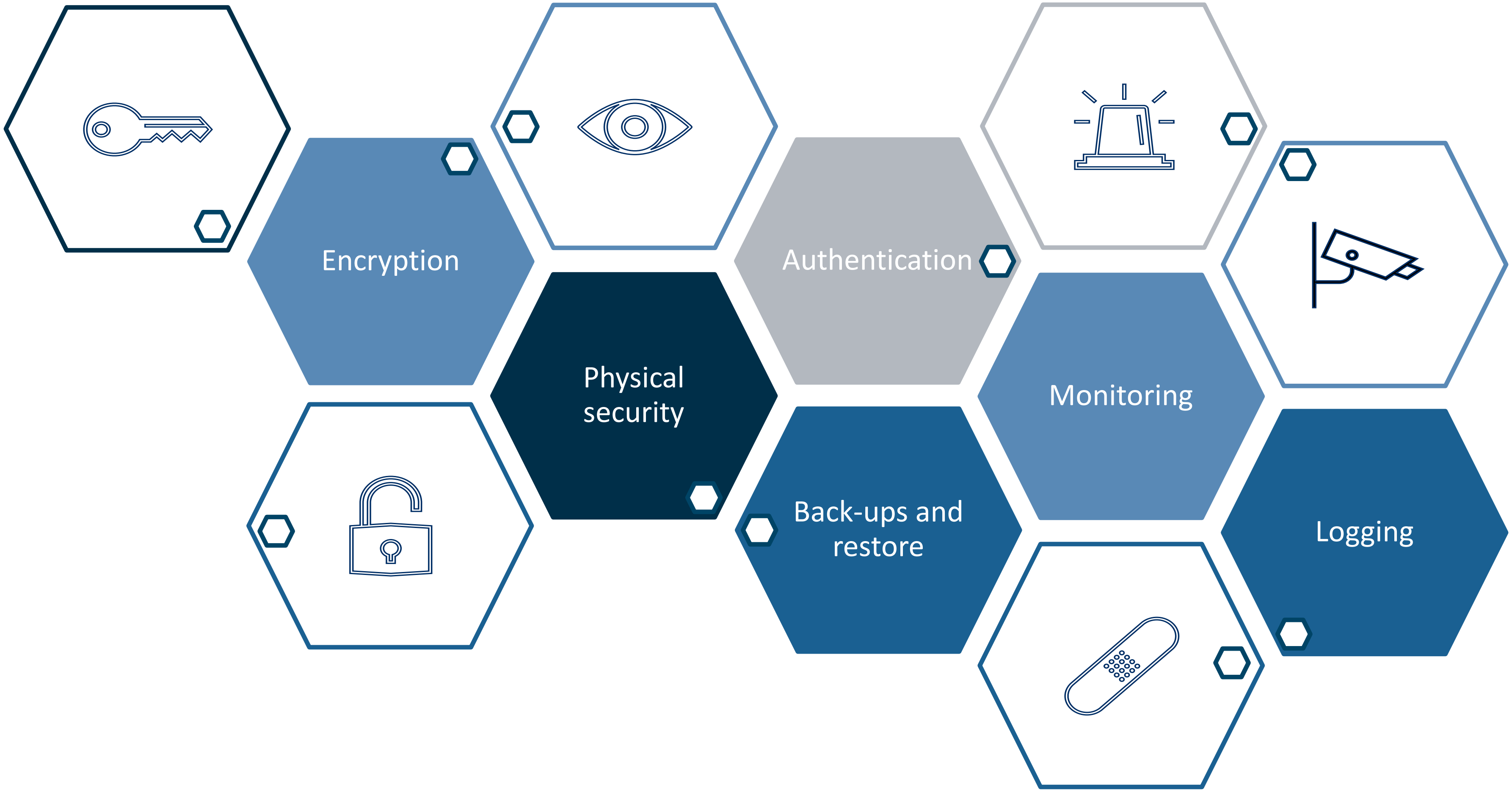
Rights of the Data subjects

Data Breach

Policies

Permanent advice

3.4 Cybersecurity| Technical measures


Encryption

Physical security

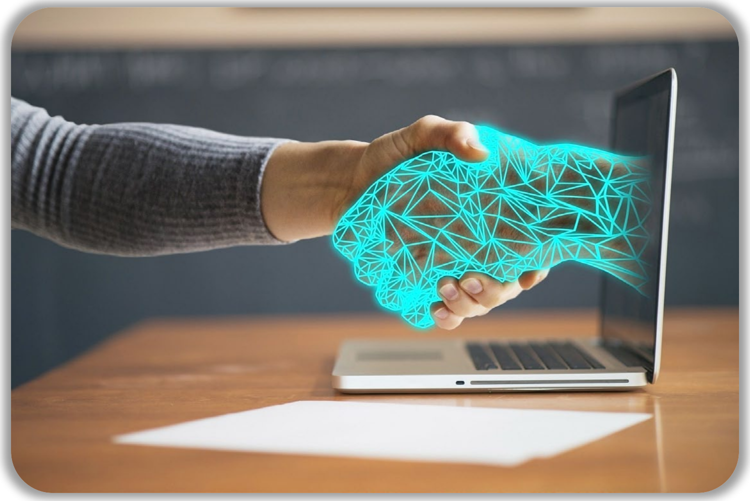
Authentication

Back-ups and restore

Monitoring

Logging

3.5 Cybersecurity| 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

4.1 What can you do? | Keynotes

Data Privacy

Governance of personal data
= GDPR

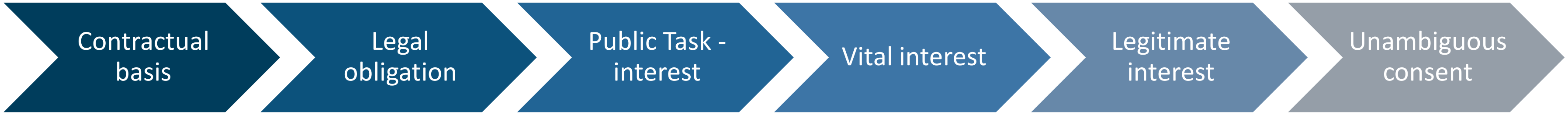
Security

Protecting data

= Cybersecurity

4.2 What can you do?| GDPR
a) Lawfulness

STEP 1 Lawfulness : Choose the reason why you process personal data



4.2 What can you do?| GDPR
a) Transparancy

STEP 2 Transparancy : Communication

- Revise privacy statements regularly
- Informed consent adapted to the situation
- Be proactive
- Use the correct media for the right situation
  - Public websites
  - Consent forms
  - Public notifications
  - ….

4.2 What can you do?| GDPR
b) Purpose limitation

STEP 3 Purpose limitation : Limit the use of the personal data only for the initial purpose

- Be clear why you are collecting personal data
  - ➢ What are you intending to do
- Comply with your documentation obligations to specify your purposes
- Comply with your transparency obligations to inform individuals about your purposes
- Ensure that if you plan to use or disclose personal data for any purpose that is additional to the original purpose that the new purpose is fair, lawful and transparent.
  - ➢ Check compatibility

Employees start their new job at the university their personal data will automatically flow to the IT environment to gain access to new systems – ***new purpose is compatible***

Students register at the university for X study subject. Faculty Y will send their personal data to their partners – ***new purpose is not compatible and requires consent***

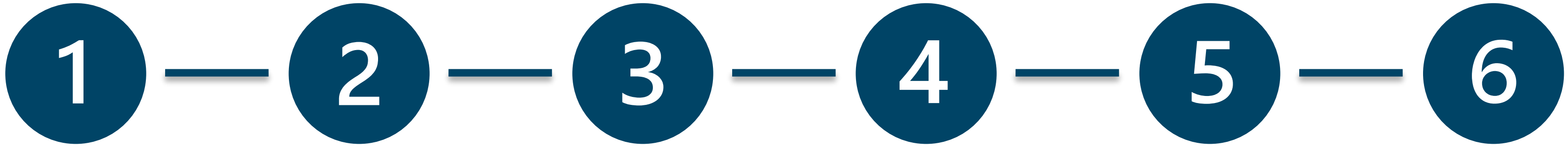
4.2 What can you do?| GDPR
c) Data minimisation

STEP 4 Data minimisation: Limit the amount of personal data you need for the purpose

You must ensure the personal data need is:

- Adequate
- Relevant
- Limited to what is necessary

What does this mean in practice?



Actively considering whether processing or holding data can be show necessary

Implementing mnimisation rules and processes at every step in the data lifecycle

Limiting collection, storage and usage through retention and destruction policies

Agreeing the time frame for which different categories of data should be held based on the purpose

Revising data where it needs to be retained for longer or shorter periods

Discarding irrelevant data promptly. Do not keep data just in case.

4.2 What can you do?| GDPR d) Accuracy

STEP 5 Accuracy: Personal data shall be accurate and where necessary, kept up to date

- Include an action or activity that allows end users to update and/or confirm any input of personal data
- Implement a specific, separate process with the objective of updating personal data captured in the previous step.

Practical Implementation | GDPR e) Storage Limitation

STEP 6 Storage limitation: Personal data will not be kept longer than necessary

- You can keep personal data as long as the purpose still applies
  - ~~*Just in case*~~
- You should consider whether you need to keep a record of a relationship with the individual once that relationship ends.
- Archiving, scientific/historical or statistical purposes → Longer than necessary with appropriate safeguards

4.2 Practical Implementation | GDPR
f) Integrity and Confidentiality

STEP 7 Integrity and confidentiality: How do I ensure the security of my personal data

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

Back-up

CYBERSECURITY!

Legal measures

Contracts

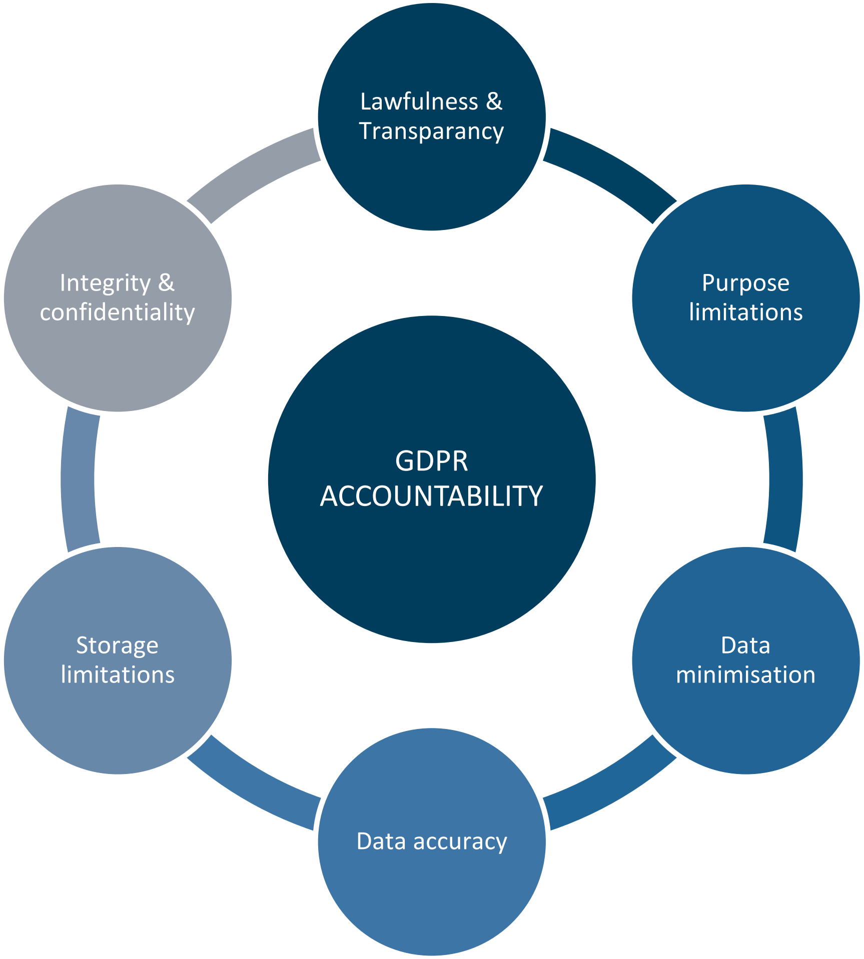
Privacy policy

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!

4.2 Practical Implementation | GDPR
g) Accountability

THE SIX GDPR PREVIOUS PRINCIPLES ENSURE ACCOUNTABILITY

Take responsibility!



4.3 What can you do? | Internal campaign

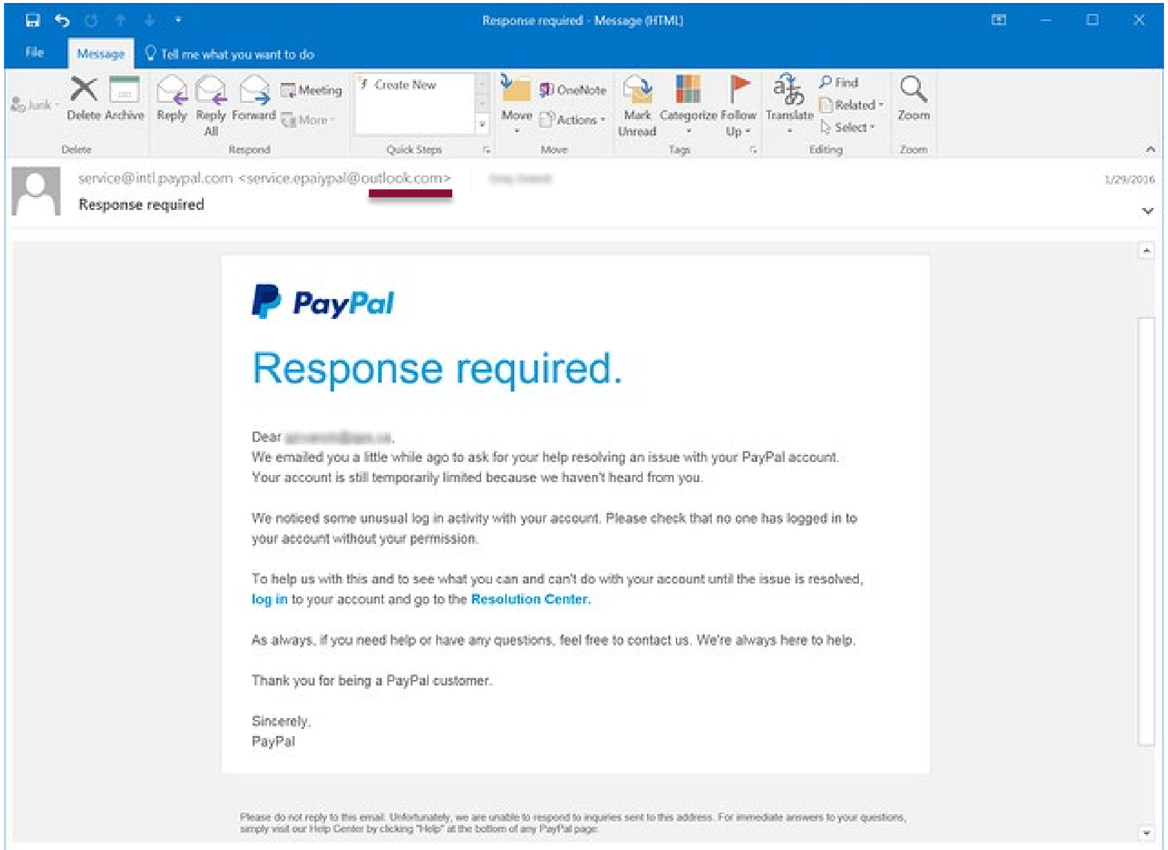
To help our staff and students, we have developed an internal campaign.

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

https://pintra.uantwerpen.be/informatieveiligheid

4.3 What can you do? | Phishing

- Is it **unexpected**?
- What is the e-mail address of the **sender**?
- Do you find the request **strange**?
- Where does the **link** lead to?
- Is this e-mail delivered in your **junk folder**?



service@intl.paypal.com <service.epaiypal@outlook.com> [redacted] 1/29/2016

Response required

PayPal

Response required.

Dear [redacted],
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

Send suspicious emails as an attachment to abuse@uantwerpen.be!

4.3 What can you do? | Online identity

Your accounts are **your online identity**.
Protect them well, so they cannot be abused.

4.3 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 **<u>not</u>** 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.

4.3 What can you do? | Other Best Practices

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

Use your computer's screen saver and don't leave your devices unattended.

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

4.4 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).

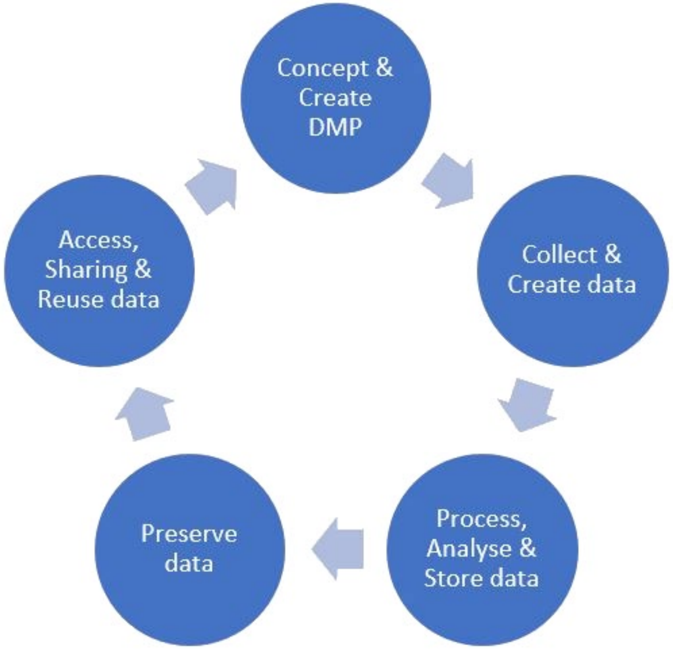
The researcher must be aware of the correct practices when using personal data

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

4.4 Research

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 cybersecurity, 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

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

- https://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.