

Personal data in Research

<https://doi.org/10.5281/zenodo.8318561>



Radboud University 

You can find the latest version of this presentation at
<https://doi.org/10.5281/zenodo.8318561>

This powerpoint can be supplemented by material on the RDM website of the Radboud University, found at <https://www.ru.nl/rdm>

Topics covered in this presentation include:

- What is the GDPR? When, where and how does it apply to academic research?
- What exceptions are there for special categories or sensitive personal data?
- How does personal data affect your storage and security practices?
- How to best handle personal data during each phase of your research?
- What are the privacy rights of your participants?
- How does personal data affect your possibilities to archive, share and publish data?

This work is licensed under a Creative Commons Attribution 4.0 International License

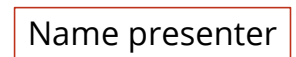
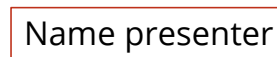
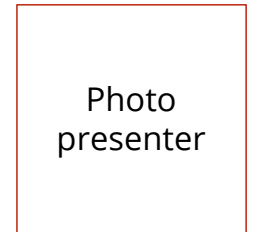
Who are we?

❖ **Research Data Management (RDM) Support Team**

❖ **The central hub for research data at the RU**

❖ **Supported by datastewards in each institute**

❖ **Located in the University Library**

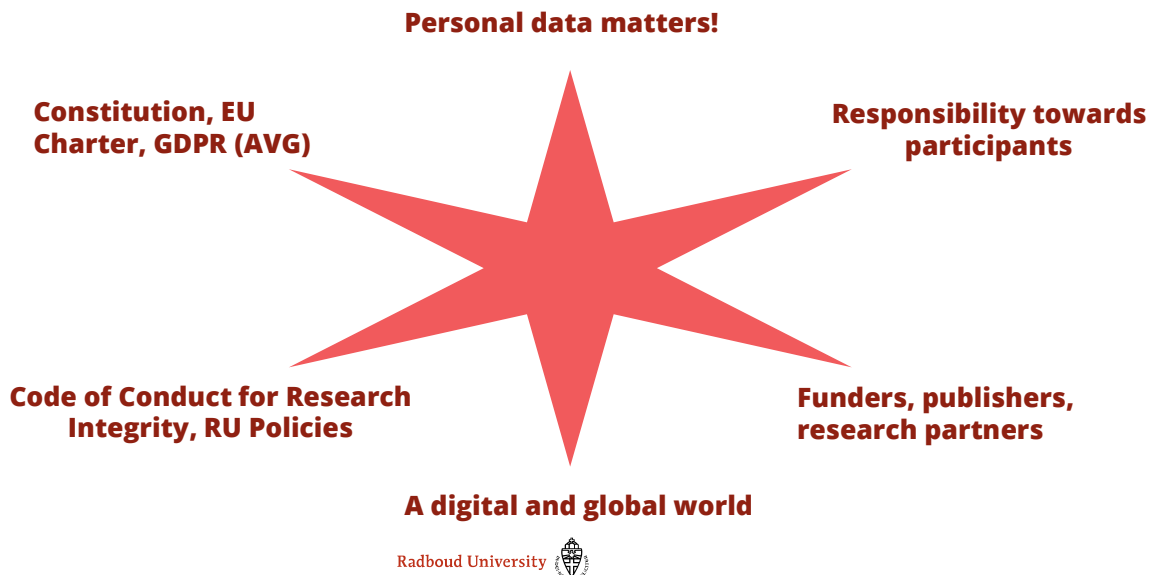


We are the ***Research Data Management (RDM) Support Team***. We function as the central hub for research data on the Radboud University. We assist researchers with everything related to research data, whether it is the research design, the collecting of data, the processing or the archiving.

We are supported by ***datastewards*** in each institute. They have specialized knowledge of your field and are usually based within your department.

We are based at the University Library and act as a central knowledge hub for researchers and datastewards.

Why care about personal data?



INTERACTION: LET RESEARCHERS EXPLAIN WHY THEY CARE ABOUT PERSONAL DATA, SINCE THEY DECIDED TO SHOW UP FOR THIS COURSE

There are indeed many different reasons why personal data matters (or should matter) to people involved with academic research. There are various reasons why.

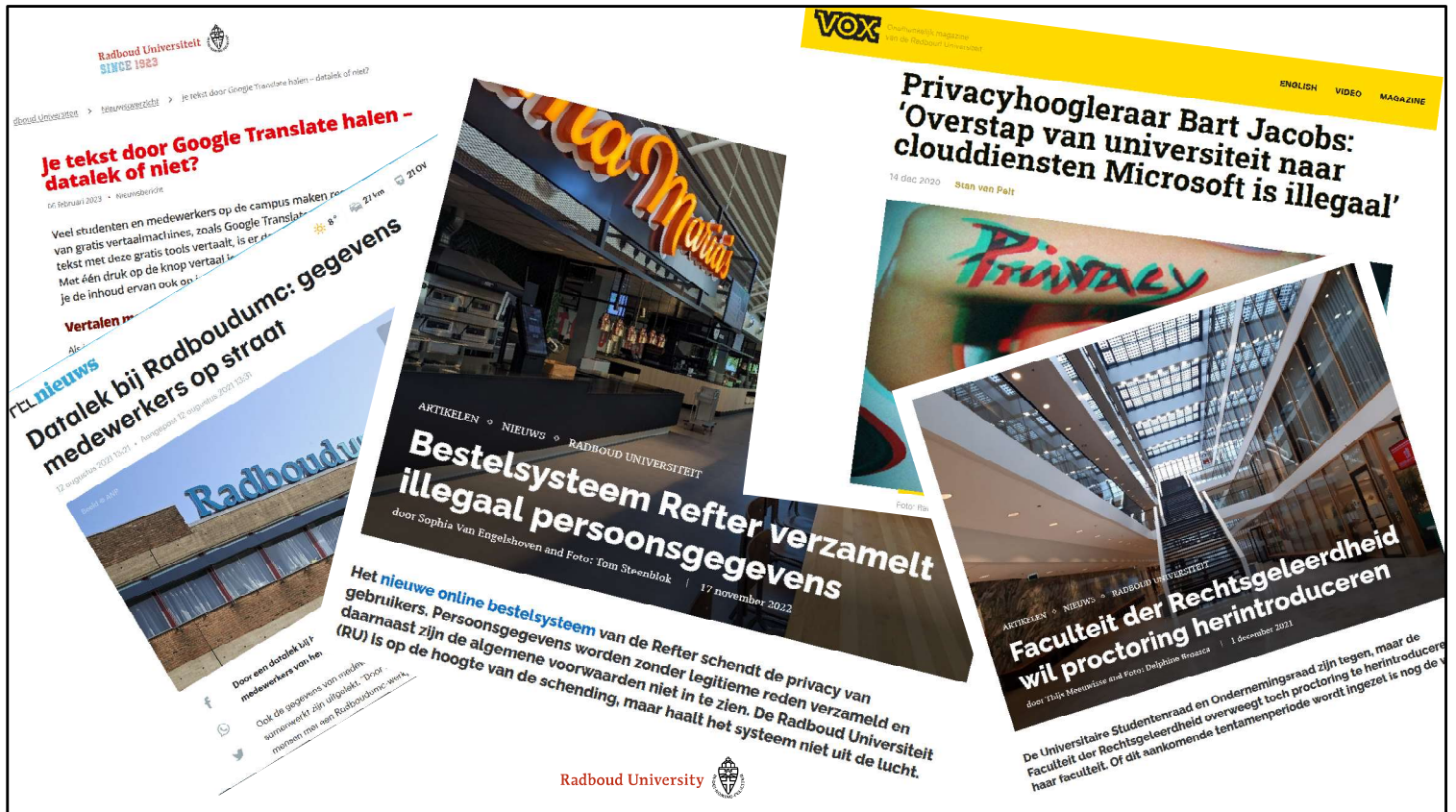
- ❖ **Personal data matters to all of us:** personal data should be important to you, even if you are not at work. Data itself has increasingly more value and problems such as a data breach can cause a lot of problems.
- ❖ **Scientists have a responsibility towards participants:** the trust and confidence of your participants and society at large is the number one resource of the university. Losing this trust impacts future research and academia as a whole.
- ❖ **Funders, publishers, research institutes and research partners:** the institutions you work with are increasingly aware of personal data, which means you have to be aware as well. Knowing your way around personal data increases your chances at funding and research opportunities.
- ❖ **The (academic) world is (more and more) digital and global:** the field of academia is rapidly changing, and a lot happens online and between different countries. This raises the complexity of the personal data that you handle.
- ❖ **The GDPR, the Code of Conduct for Research Integrity and RU policies:** laws and regulations regarding science expect you to handle personal data responsibly.
- ❖ **The right to privacy in the Dutch Constitution and EU Charter of Fundamental Rights:** as inhabitants of the Netherlands and the EU we have a right to privacy.

Personal data + Research = Complex



Before we start it is probably good to make one thing clear: personal data and research = complex.

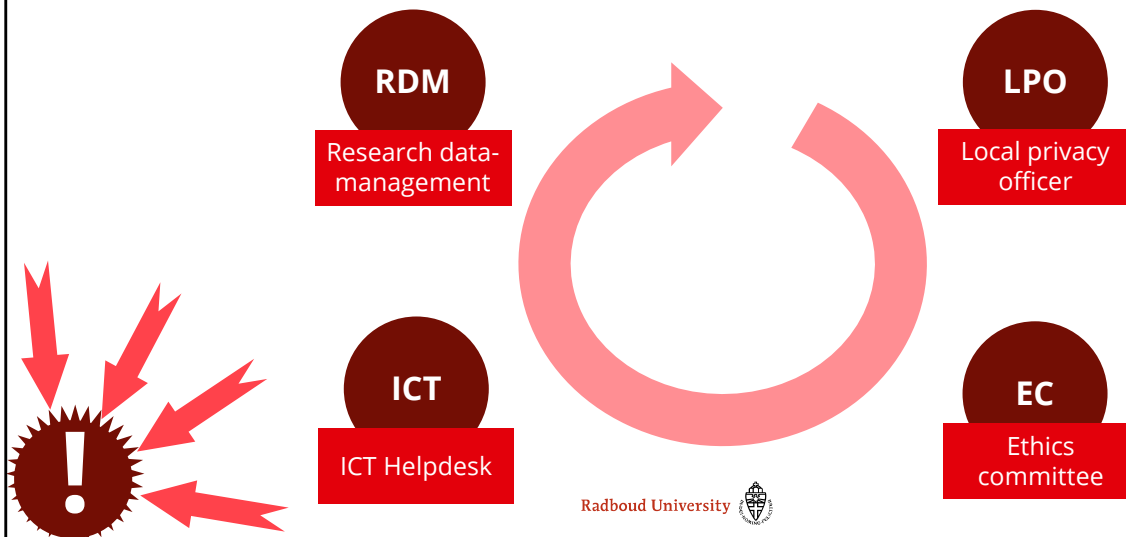
- ❖ ***There is no one-size-fits-all approach:*** You will make different choices depending on your research design.
- ❖ ***Many areas are still in development:*** Technology and privacy concern develop rapidly, and policy is slow to catch up.
- ❖ ***Not everything is covered by guidelines:*** The GDPR is only five years old, its implications are still being investigated.
- ❖ ***Research institutes have their own policies:*** What we tell here today is the general story, always check your local policies.
- ❖ ***Disciplines have their own practices:*** Even within research institutes different academic disciplines can have their own practices and traditions.



To show how complex personal data can be, even our own university is often struggling “to do it right”. Here too there are data breaches, debates about the legality of personal data collection and the limitations of privacy.

When in doubt, scream and shout

Do not hesitate to ask for assistance when something is not clear.



To alleviate at least some of that complexity the single most important message that I would like to give to you today is the following “when in doubt, scream and shout”.

If you have questions with regards to personal data at any point during your academic career, don’t hesitate to contact the responsible support organization.

- ❖ This can be us, ***the research datamanagement support group***, who specialize in the best way to handle research data.
- ❖ For a more specialized opinion on personal data you can go to ***the local privacy officers***.
- ❖ For technical and computer-related topics you can rely on ***the ICT Helpdesk***.
- ❖ For the ethically complex decisions you can also turn to the ***ethics committees***.

While it might seem that these are 4 separated islands, the truth is that we often work together or talk to each other when there is overlap.

For you this might raise the question who you should contact in case of questions. To make this decision easier we have added a ***“help me” button*** in the bottom left of many PowerPoint slides. This will tell you who to turn to if you have questions on that particular topic.

On some slides you will also find ***spiked buttons***. This means that you are dealing with a complex or high-risk topic for which it is pretty much mandatory to contact the responsible support organisation.

We provide ***contact information*** for each of these support organisations at the end of the PowerPoint.

Goal of today's session

Approximately 120 minutes from now:

- ❖ You will have a basic understanding of the GDPR (in Dutch: AVG)
- ❖ You will be aware of the role of personal data in each phase of your research cycle
- ❖ You can reach out for assistance when needed, and know who to contact

The goal of this lecture is three-fold.

1. We will teach a little bit of ***theory about the GDPR (in Dutch: AVG)***. This will help you understand why your research needs to follow certain practices.
2. Secondly we will take you ***through the research cycle and explain where and when personal data matters*** for your research.
3. Lastly, as mentioned before, we provide you with the means receive ***additional assistance*** when you need it.

Table of Content

General Data Protection Regulation

- ❖ **Where does it apply**
- ❖ **What does it encompass**
- ❖ **Terminology**



How to apply the GDPR during

- ❖ **Research planning**
- ❖ **Data collecting**
- ❖ **Data processing and analyzing**
- ❖ **Data publishing & sharing**
- ❖ **Preserving and re-using**

When it comes to the General Date Protection Regulation this lecture will discuss various aspects:

- ❖ **Where** does it apply?
- ❖ **What** does it encompass?
- ❖ **Terminology:** What keywords do you need to know?

After that we will discuss how you can apply the GDPR in each phase of your research. Here we take the research cycle as our starting point. We'll go through each of the following phases of the research cycle:

- ❖ **Research planning**
- ❖ **Data collecting**
- ❖ **Data processing and analyzing**
- ❖ **Data publishing & sharing**
- ❖ **Preserving and re-using**

Because this is quite a lot of information we will take a break in the middle during which coffee and tea will be served.

Table of Missing Content

Some important topics cannot be discussed in detail today:



Anonymisation and pseudonymisation



Data security



Informed consent

Feel free to contact us at rdmsupport@ubn.ru.nl or wait for future courses!

Radboud University 

Besides a table of content there is also a table of missing content.

This is because there are some topics which we can only discuss at a surface level today. These are

- ❖ **Anonymisation and pseudonymisation.**
- ❖ **Data security**
- ❖ **Informed consent**

In the future these topics will be part of different training courses. In the meantime people can direct their questions on these topics to our e-mailaddress.

GDPR

GDPR in a nutshell

- ❖ **The GDPR is not an obstacle but an opportunity for research**

- ❖ **Protect and empower EU citizens.**
- ❖ **Encourage the sharing of (personal) data.**

- ❖ **The GDPR is designed with the future in mind**



Generic language



Neutral towards technology



Supplemented by national law (UAVG)

- ❖ **The GDPR gives the Dutch Data Protection Authority the authority to enforce**

The GDPR is not an obstacle but an opportunity for research:

It united and updated the numerous privacy laws that existed in Europe.

The GDPR has two intertwined objectives:

The first might be well-known, which is to protect and empower EU citizens with regards to their personal data. However, because all European countries follow the same GDPR framework an added benefit is that it is much easier to share personal data between countries. It is much easier to do research involving personal data across borders than it used to be in the past.

The GDPR is designed to be open:

It uses generic terms and is neutral towards technological developments, making it essentially “future-proof”. It also gives each country the freedom to set country-specific regulations and enforce the rules. In the Netherlands this is done via the GDPR Implementation Act, but also national and RU-specific policies concerning personal data. One example of this is the BSN, which was included as personal data and can only be processed in highly specific cases.

The GDPR gives the Dutch Data Protection Authority the authority to fine GDPR breaches:

The AP can fine organisations who breach GDPR standards for a maximum of 20 million euros or 4 percent of their annual worldwide profit. So we better take this serious!

GDPR Enforcement Tracker

tracked by **CMS**
law-tax-future

The CMS.Law GDPR Enforcement Tracker is an overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO). Our aim is to keep this list as up-to-date as possible. Since not all fines are made public, this list can of course never be complete, which is why we appreciate any [indication of further GDPR fines and penalties](#). Please note that we do not list any fines imposed under national / non-European laws, under non-data protection laws (e.g. competition laws / electronic communication laws) and under "old" pre-GDPR-laws. We have, however, included a limited number of essential ePrivacy fines under national member state laws.

New features: "ETid" and "Direct URL"!

We have assigned a unique and permanent ID to each fine in our database, which makes it possible to precisely address fines, e.g. in publications. Once an "ETid" has been assigned to a fine, it remains the same, even if the fine is overturned or amended by courts at a later date, or if we add fines that were issued chronologically before. The "Direct URL" (click "*" or on a specific ETid to view details of a fine) can be used to share fines online, e.g. on Twitter or other media.

Show entries

Search:

ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
ETid-648	CZECH REPUBLIC	2020	Unknown	Public university	Art. 6 (1) GDPR, Art. 13 GDPR	Insufficient legal basis for data processing	link
ETid-449	IRELAND	2020-08-18	65,000	Cork University Maternity Hospital	Art. 5 GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	link
ETid-392	POLAND	2020-09-08	11,200	Warsaw University of Life Sciences	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	link
ETid-472	SWEDEN	2020-12-03	390,100	Karolinska University Hospital of Solna	Art. 5 (1) f) GDPR, Art. 5 (2) GDPR, Art. 32 (1) GDPR, Art. 32 (2) GDPR	Insufficient technical and organisational measures to ensure information security	link
ETid-471	SWEDEN	2020-12-03	341,300	Sahlgrenska University Hospital	Art. 5 (1) f) GDPR, Art. 5 (2) GDPR, Art. 32 (1) GDPR, Art. 32 (2) GDPR	Insufficient technical and organisational measures to ensure information security	link
ETid-569	HUNGARY	2020-12-10	22,200	Budapesti Műszaki és Gazdaságtudományi Egyetem (Budapest University of Technology and Economics)	Art. 5 (1) a), b), c) GDPR, Art. 6 (1) GDPR, Art. 9 (2) GDPR, Art. 12 GDPR, Art. 13 GDPR	Insufficient legal basis for data processing	link
ETid-482	SWEDEN	2020-12-11	54,000	Umeå University	Art. 5 (1) f) GDPR, Art. 32 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security	link
ETid-552	IRELAND	2020-12-17	70,000	University College Dublin	Art. 5 (1) e), f) GDPR, Art. 32 (1) GDPR, Art. 33 (1) GDPR	Insufficient technical and organisational measures to ensure information security	link

If you want to see why it is best to take the GDPR serious, it can help to take a look at the GDPR Enforcement Tracker (www.enforcementtracker.com). Here you can see every fine that was ever handed out because of a breach of the GDPR.

As you can see universities are not immune to this, which sometimes results in pretty steep fines.

One consolation might be that it is ***the university that pays these fines, not the researcher.***

Case: Digital data donation

Raw DDP

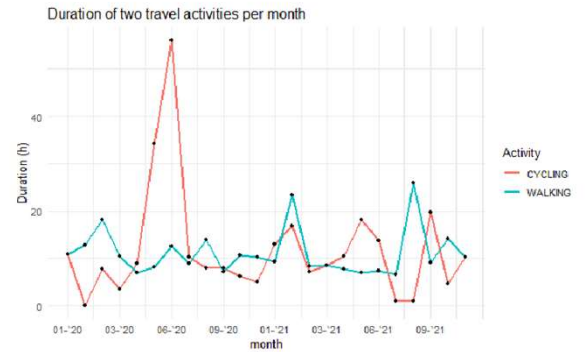
```
"location": {  
  "latitudeE7": 520844770,  
  "longitudeE7": 51716420,  
  "placeId": "ChI33ySEd3toxkcR3o5101qqC1Y",  
  "address": "Heidelberglaan 1\\n3584 CS Utrecht\\nNederland",  
  "name": "Faculteit Sociale Wetenschappen",  
  "sourceInfo": {  
    "deviceTag": 1769097206  
  },  
  "locationConfidence": 47.502987  
},  
"duration": {  
  "startTimestampMs": "1551970749819",  
  "endTimestampMs": "1551976816602"  
},  
"placeConfidence": "MEDIUM_CONFIDENCE",  
"centerLatE7": 520845963,
```

Extracted data

Cycling

		Duration (hours)	Distance (km)
2016	11	5.32	91.49
	12	12.98	199.51
2017	1	8.60	121.26
	2	13.40	308.93
	3	12.43	198.12

Processed data



Langedijk, Annette, Huijser, Dorien, Zundert, Joris van, Bron, Esther, Kesteren, Erik-Jan van, Boeschoten, Laura, & Dijkstra, Freek. (2023, March 28). Your secrets are safe with us: Tools for research with sensitive data. Zenodo. <https://doi.org/10.5281/zenodo.7778159>

There are however also positive outcomes of the GDPR. One example of this is the Digital Data Donation program. This allowed researchers to access data that would otherwise never have been available to them.

1. Participants request raw personal data from government services or companies
2. Participants can analyze their own raw data locally
3. Participants can consent when they share the results of that analysis with the researcher
4. The researcher only ever sees the processed data

Where does the GDPR apply?

❖ **The European Economic Area**

❖ **The United Kingdom***

❖ **But also:**

- ❖ **If your RU research takes place outside the EEA**
- ❖ **If a non-EEA organisation uses personal data inside the EEA**

Radboud University



Right now the GDPR applies ***to 27 countries***. Most of them are located in the ***European Union***, but some countries of ***the EEA***, such as Iceland and Norway, are also included.

The ***United Kingdom*** has its own version of the GDPR, which is nearly identical to the European one, but since they have left the EU this is something which can change in the future.

A consequence of this is that it can be quite challenging ***to transfer personal data from the EEA to a non-EEA country***. This is often a complex process involving legal documents.

Besides these geographic boundaries there are also legal boundaries. The GDPR also applies when:

- ❖ If your research as a RU researcher ***takes place outside of this region***. For example if your study takes place abroad.
- ❖ When an organization outside this region ***uses personal data from citizens in this region***. For example if you send personal data to an organisation in the US or China.

What counts as processing?

Any action performed with personal data, whether automated or manual, on paper or digital.



Radboud University 

Pretty much any imaginable action you perform with personal data counts as processing. It doesn't matter if it is automated or manual, on paper or digital. Even making a dataset anonymous counts as processing, or storing personal data in a box in a closet.

INTERACTION: LET RESEARCHERS MENTION THE MOMENTS DURING RESEARCH WHEN THEY ARE PROCESSING PERSONAL DATA

When can you process personal data?

- ❖ You can only ever process personal data if you have a legal basis.
- ❖ This means you can only process personal data for a specific purpose.
- ❖ The GDPR provides exceptions for scientific purposes.
- ❖ A legal basis ≠ an ethical basis

LPO

Radboud University 

To process personal data ***you need to have a legal basis***. This is the justification on which the GDPR allows you to process personal data.

This also means that you can only process personal data for ***a specific purpose***. If you process personal data for research you cannot continue to process the same data to sell a product. You can also only process personal data for a specific purpose ***as long as it is necessary to complete that purpose***.

There are exceptions that allow further processing of previously collected personal data for research (GDPR article 5(1)(b)). This means that you can reuse personal data, that were previously collected for other purposes, for scientific research purposes. This is only allowed if you put in place sufficient safeguards to protect the personal data, inform data subjects, and allow them to exercise their rights.

Besides a legal basis it is also important that you consider the broad ethical effects of processing: ***avoid deception*** in your communication and ***avoid disproportionate negative, unlawful, discriminating or misleading effects***.

When can you process personal data?

❖ There are six legal bases, but research only uses three.



Informed consent: a person agrees to the processing.



Public interest: the research benefits the public good and consent is not possible.



Legitimate interest: processing without research purpose.

LPO

Radboud University 

While there are six legal bases on which you could collect personal data, in practice research ***almost always works on the basis of informed consent***. This type of informed consent differs from the one requested by ethics committees, although they can often be combined in the same documents.

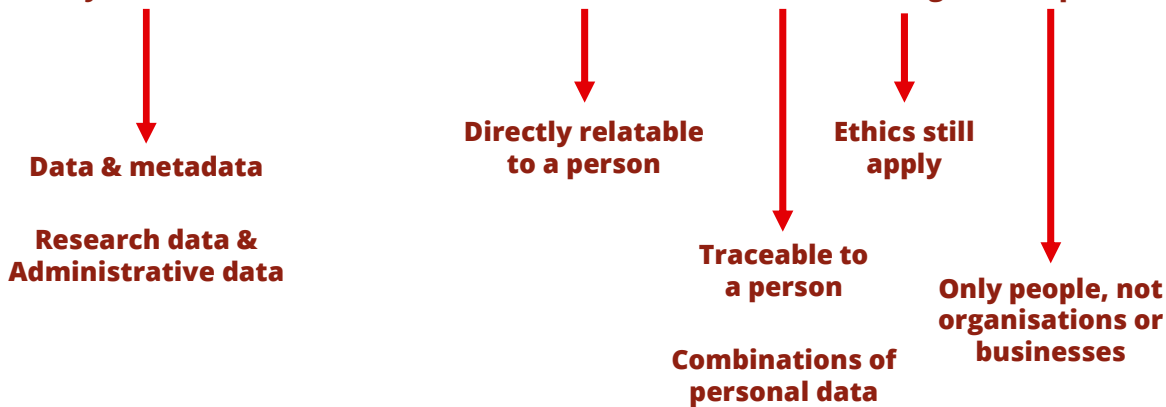
Public interest is sometimes used in research ***when the research is shown to clearly benefit the public good and when informed consent is not an option***. The purpose of the processing must be recognized by an authority and the necessity and proportionality of the research needs to be assessed, for which it is best to contact the LPO. It is a particularly useful legal basis in cases ***where obtaining consent may be impractical***, e.g., when performing public observations or when scraping the web. Or when consent is impossible to obtain because ***data subjects do not have a free choice***, such as when performing research among the university's own employees or students, or among pupils in a school. In some cases consent might still be required, even if you rely on this legal basis, e.g., when this is ethically required or when you want to process special categories of personal data.

Legitimate interest: this can be a basis that is sometimes used for research, for example when you contact participants before you obtain their consent. ***Since contacting participants is a prerequisite to perform research, it can be in the university's legitimate (research) interest*** to process their contact information. This legal basis requires a careful assessment of interests for which it is best to contact the LPO.

What does the GDPR encompass?

Personal data

= any information that relates to an identified or identifiable living natural person.



Radboud University 

Personal data has a technical definition in the GDPR. It is easiest to understand if we break it down into parts:

1. Any information:

Meaning data and metadata (= data about the data itself). But also for example research data and administrative data.

2. Identified

This involves data that is directly relatable to a person, for example a name or photo. Researchers handle these direct identifiers most commonly for administrative purposes.

3. Identifiable

This is concerned with data that combines enough "anonymous" characteristics of someone can still make them identifiable. Within a small population or through the combination of sufficient personal data you can identify someone even without any direct identifiers.

4. Living

Even though a person that passed away does not have personal data, there can be ethical considerations when processing the personal data of a deceased person. It is also possible data reflects on family members and thus is personal data.

F.e. historical medical data with implications for later generations or when diaries with personal data reflect on living family members. It is generally not recommended to process personal data that might negatively impact living family members.

5. Natural person

The GDPR is *only* concerned with human individuals, not companies or organisations. There can be exceptions however, f.e. when a company is named after an individual.

Where can you encounter personal data?



Research data



Administrative data



Informed consent

Based on the previous definition a researcher will generally encounter personal data in three areas.

1. **Research data:** This is the information what you actually want to find out and that you need need to answer your research questions.
2. **Administrative data:** This is the information required to stay in touch with your participants, contact information, payment details.
3. **Informed consent:** The personal data that you record for your informed consen, such as names and signatures.

QUIZ

IS IT PERSONAL DATA?



INTERACTION: This quiz is meant to engage the researchers and to bolster their confidence about their understanding of personal data thus far. It presents a rich variety of examples of ***what could potentially*** be personal data. While examples include definitive yes or no answers, the goal is to raise discussions on what is or is not personal data, or under what circumstances data could be personal data.

Quiz: could it be personal data?

A handwritten signature in black ink that reads "P. Smith". The signature is stylized with a large, sweeping initial "P" and a long, horizontal flourish at the end.

Yes

No

Signatures are by definition personal data, since they allow you identify someone.

Quiz: could it be personal data?

www.leyla.bruijnen.com
@FunnyLeyla

Yes

No

Personal websites and social media handles could potentially be personal data. In this example it is made obvious because the example contains clear personal names, but this can be true for any website or social media handle.

Students might disagree on whether or not this is personal data, since a person has chosen to make it public. This could be an interesting ethical question, just because the information is “public”, does not mean that the person expects it to be spread to a worldwide audience. Unless a person explicitly indicates that they want their information to be processed further it should still be considered personal data and thus requires a legal basis such as informed consent.

Quiz: could it be personal data?

*Stadsplateau 31-32
McDonald's Nederland B.V.
3521 AZ Utrecht*

Yes

No

This is a trick question designed to emphasize the “natural persons” part of the personal data definition. This address, being a business and being publicly available sets it apart from an address of a private individual.

Quiz: could it be personal data?



Yes

No

This question is designed to emphasize that personal data is not just textual but can also be contained in images, audio or video.

Quiz: could it be personal data?

73 kg
Brown eyes
Lefthanded
Black hair
183 cm

Yes

No

This question introduces the potential personal data that is present in particular combinations of data, even when they are seemingly anonymous by themselves. However because of their combination it would be quite possible to identify someone in a group based on the above data.

Quiz: could it be personal data?

*Married
Accountant
Born: 19-07-1984
Died: 05-11-2003
Female*

Yes

No



This is a trick question that follows on the previous one. While this too acts as a combination of various data points that when combined would make it possible to identify someone, the data also suggests that this person has passed away. This means that strictly speaking it would not be personal data, even though it once would have been.

Quiz: could it be personal data?

*Favourites:
Elvis Presley
Shawshank Redemption
Strawberry icecream
Badminton
Ferrari*

Yes

No

This question is meant to introduce the way in which opinions can also be considered personal data under certain circumstances. This is relevant because a lot of human-related research data is essentially made up of opinions, but this is rarely associated with the possibility that someone can be identified. The point of this question is to illustrate that asking someone about their political opinions, religious views, etc. could also increase the chance that they would be identified, even though these are by themselves just anonymous opinions.

Quiz: could it be personal data?

174 cm
174 cm
172 cm
176 cm
182 cm
242 cm
180 cm
180 cm
172 cm
178 cm
174 cm

Yes

No

This question aims to highlight the possibility of an outlier in the data being personal data. If there is one data point which is radically different from all the others it does not take much to identify a person.

Quiz: could it be personal data?

Diary of Queen Elizabeth II

Yes

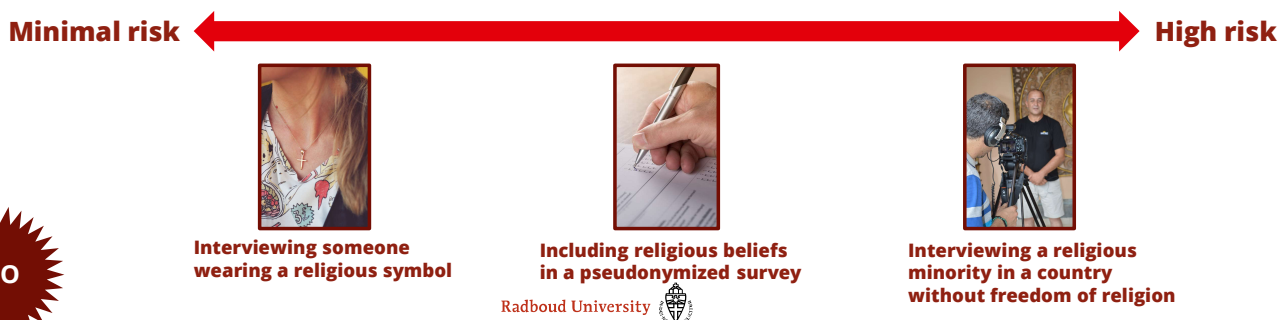


No

This is a trick question, leaving room for debate and if anything emphasizing how complicated personal data can sometimes be. Considering that the Queen passed away technically her diary could not contain personal data about the Queen. However, given the intense personal nature of a diary and the high chance that it contains personal data about other members of the royal family there is still a significant chance that it would in fact contain personal data. Moreover there could be ethical concerns that prevent the use of this data that remain even when there are no GDPR-limitations.

Special categories of personal data

- ❖ When personal data creates risks for the rights and freedoms of a person.
- ❖ Processing of these special categories is **prohibited**, except with **consent**.
- ❖ It is a risk-assessment: leading principle is the risk for your participants.



LPO

- ❖ **Special categories of personal data:** When personal data creates risks for the rights and freedoms of a person: processing this data can seriously infringe on someone's privacy or result in discrimination or prosecution.
- ❖ Processing of these special categories is **prohibited**, except for specific purposes. **Informed consent** is the most common one, however the UAVG also introduces other exceptions (UAVG article 24).
- ❖ It is important that researchers understand that **it is risk-assessment, not a checkbox**. The question is not if a special category of personal data is included in the dataset but how big the overall risk for the participant is when that personal data is included or combined with other personal data in the same or linked databases.
- ❖ If researchers want to work with this kind of data, their goal should be to minimize the risk for their participant by asking themselves:
 - ❖ Are there **less invasive ways** of doing research with the same outcome?
 - ❖ How can this data be collected in the **least risk-introducing manner**?
 - ❖ Do you have **explicit consent** for the collection of these special categories?
- ❖ When researchers suspect there is any risk involved with the processing of special categories of personal data, **they should contact the LPO**.

Special categories of personal data



Racial or ethnic origin



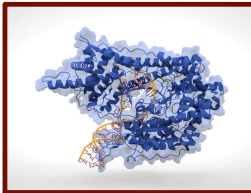
Political opinions



Religious / philosophical beliefs



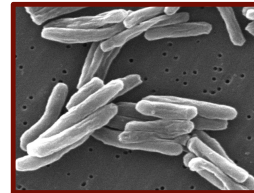
Trade union membership



Genetic data



Biometric data



Health-related data



Sex life or sexual orientation

LPO

This slide provides a short overview of the various special categories of personal data mentioned in the GDPR. This is just to give a brief impression, since the categories are very generic and are very context-dependent.

Sensitive personal data



BSN numbers



Confidential business data



Confidential state security data



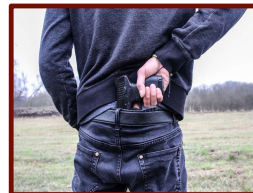
Work performance data



Financial information



Criminal convictions



Punishable offences



Illegal acts

LPO

This is an addition to the previous slide, which explains that there also exists a ***third category of sensitive personal data***.

This involved data which are not subject to the additional rules of the special categories of personal data, but who are ***by their very nature sensitive and high-risk***.

Whenever researchers want to process this type of personal data, ***they should always contact the LPO***.

Audio, photo and video data

❖ Identifiable photo, audio and video recordings are always personal data.

... and sometimes capture special categories of personal data.

❖ Consider de-identifying (parts of) the data:



Deleting after transcription



Record only what you need



Blur or transform the recording

LPO

EC

Radboud University 

- ❖ This slide makes researchers aware that personal data is not just contained in text-form, but can also be present in any ***photos, audio or video recordings*** that they make. If a person is identifiable on these media then ***by definition personal data is collected***. Because of its information density these media also make it relatively ***easy to capture special categories of personal data***.
- ❖ If researchers want to work with this kind of data, their goal should be to minimize the risk for their participant by asking themselves:
 - ❖ Are there other ways to answer your research question?
 - ❖ Is video absolutely necessary or will audio suffice?
 - ❖ Do you have ***explicit consent*** for this photo, audio or video recording?
- ❖ Moreover researchers should consider ways in which they can de-identify (parts of) the data:
 - ❖ Deleting the audio recording after transcription reduces the sensitivity of the personal data.
 - ❖ If researchers are only interested in handwashing practices it is probably not necessary to record faces.
 - ❖ In some cases it might be possible to blur or transform the recordings, however only if sufficient research data remains.

Social media

- ❖ **Social media contains a lot of personal data, but using it is not without problems:**



No informed consent



Possibly unethical



Breach of Terms of Service

- ❖ **Generally treat social media data as you would any other personal data**
- ❖ **Alternatively: Faculty of Arts has more elaborate guidelines**

LPO

Radboud University 

- ❖ Social media are used more often as research data, since they are readily available in large quantities and easily scraped from websites.
- ❖ This is not without problems however
 - ❖ **No informed consent of users:** making public on social media does not mean that someone gives consent to use their data for research purposes
 - ❖ **Possibly unethical:** users might never have intended that their post would reach a worldwide audience.
 - ❖ **Conflict with Terms of Service:** there are different requirements for each social media platform, but these often include rules against unauthorized automated data collection (web scraping).
- ❖ Generally try to **treat social media data as you would any other personal data:** anonymize or pseudonymize when needed, try to get informed consent, consider copyrighted material, etc.
- ❖ **Take this in consideration in your research approach:** if informed consent is not possible (f.e. due to the quantity of personal data involved) one alternative is to only link to social media posts instead of copying them directly. That way the participant stays in control of their own data and can delete their post at any time. This does result in a dead link for the researcher, but that is cost of doing business in this case.
- ❖ The Faculty of Arts has produced clear guidelines on how to work with social media data:
https://www.radboudnet.nl/publish/pages/1048023/guidelines_20for_20collecting_20social_20media_20and_20online_20news_20data-v7.pdf

Misleading or deceptive research

- ❖ **Misleading or deceptive research is possible with the GDPR when informed consent would influence the responses of participant.**



**Strict ethical
and privacy
review**



**Participants are
informed that
they are being
deceived but do
not know how**



**Participants are
fully informed
(debriefed) after
participating**



Deception is when a researcher ***gives false information to subjects or intentionally misleads participants*** about some key aspect of the research. This is most sometimes done when knowing all the information that would normally be presented in an informed consent would change the outcome of the study in a debilitating manner. Instead of a full informed consent researcher tend to do a full debrief after the study is concluded to clarify the deception.

The starting point for this type of research should always be “do no harm”

- ❖ Justify why covert research is required
- ❖ Establish very safe procedures for data processing
- ❖ The identity of participants should be kept anonymous at all cost
- ❖ Ideally participants are informed afterwards, but only if this does not increase risks

To facilitate this the study must be proceeded by a ***strict ethical and privacy review***, and participants are commonly ***informed (debriefed) after participating***.

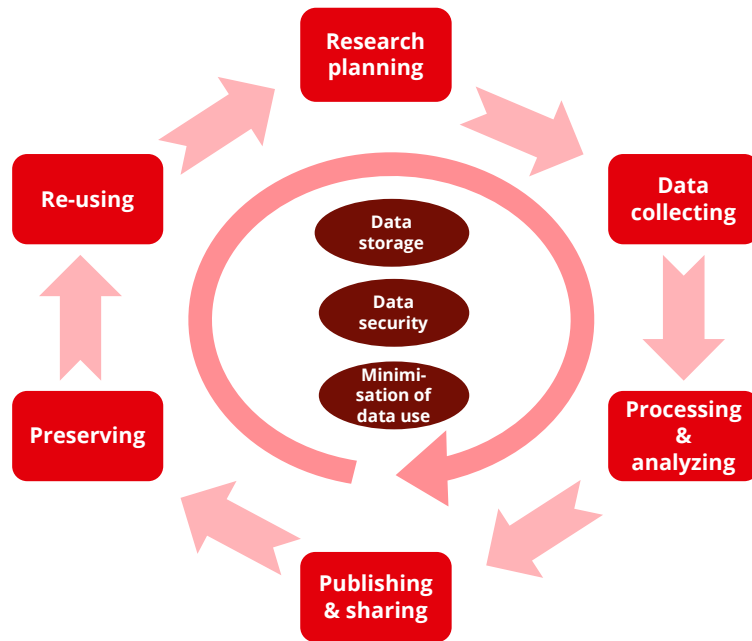
Whenever a research considers this approach ***they must contact the LPO and the EC*** to assess what risks are involved and what steps must be taken to mitigate these.

Deception is when a researcher gives false information to subjects or intentionally misleads them about some key aspect of the research. Examples include:

- ❖ Subjects complete a quiz, and are falsely told that they did very poorly, regardless of their actual performance.
- ❖ In order to induce stress, study personnel tell subjects that they will give a speech that evaluators will observe on video, when the subjects' speeches will not actually be recorded or observed.
- ❖ The study includes a researcher's “confederate” (an individual who poses as a subject) but whose behavior in the study is actually part of the researcher's experimental design.
- ❖ Unnoticed video registration of participants in a waiting room;
- ❖ Subjects are asked to take a quiz for research but they are not told that the research question involves how background noise affects their ability to concentrate.
- ❖ Participants are asked to answer questions, but are not aware that the influence of time pressure is also measured.
- ❖ Participants are asked to read a text, but are not informed that, apart from reading time, their emotional responses to certain words are being measured.

GOOD PRACTICES

General practices



This is the research cycle that researchers are most likely familiar with. It contains every step from research planning to preserving and re-using and is the guiding structure for the remainder of this presentation.

In a first step this presentation will address the general practices that researchers should observe at all times throughout the cycle. These are equally applicable to every phase.

Data storage



Research data:

Minimal 10 years (15 in case of WMO)



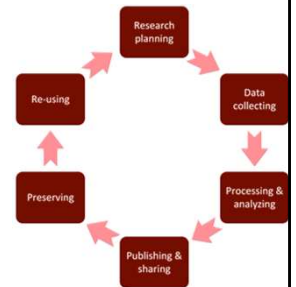
Administrative data:

As long as they serve a purpose



Informed consent:

Institute specific



- ❖ How long personal data can be stored ***depends on the nature of the data containing the personal data.***
- ❖ ***Research data*** follows clear guidelines set by the university: ***at least 10 years***, at least 15 years for WMO research and at least 25 years for pharmaceutical research.
- ❖ ***Administrative data*** only need to be stored for as long as they serve a purpose, for example:
 - ❖ Contact information until it is no longer possible to withdraw
 - ❖ Payment details until the compensation has been paid out
 - ❖ In case of longitudinal research it might be needed to store administrative data for a long time
- ❖ ***Informed consent data*** follows the guidelines set by each research institute or ethics committee.

Data storage

Option	Storing	Sharing	Collaborating	Limitations
Radboud Data Repository	✓	✓	?	Not ideal for work-in-progress
Workgroup folders	✓	?	?	Only with fellow RU-researchers
Personal U-drive	✓	✗	✗	Will be replaced with OneDrive
RU-account on OneDrive	✓	✓	✓	Only if research institute allows it Only with fellow RU-researchers
RU-account on Teams	✓	✓	✓	Only if research institute allows it
SurfDrive	?	?	?	Only encrypted personal data
Surf FileSender	✗	?	✗	Only encrypted personal data
Personal cloud storage	✗	✗	✗	Not allowed
External hard drive / USB	✗	✗	✗	Not allowed



The Radboud University provides various storage services, each with advantages and disadvantages. Some are better suited than others when it comes to personal data.

This presentation cannot go into detail with each storage location, but it is important to be mindful of the locations where you store personal data.

Other storage locations



Audio or video recorders



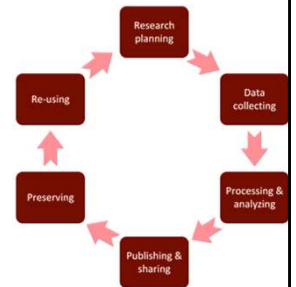
External online services



Software with cloud functionality



E-mail attachments



RDM

Radboud University 

- ❖ Besides the obvious storage locations used for data storage there are also less common ones. In the context of personal data it is however still important to keep these in mind.
 - ❖ Audio or video recorders
 - ❖ Online services such as translation or transcription services
 - ❖ Software with cloud functionalities
 - ❖ E-mail attachments that are send
- ❖ ***Before using these, always verify if you are allowed to use them.*** The only exception are RU-approved services which are available on the Software Center.
- ❖ ***Always choose maximum privacy settings.*** Only lower privacy settings if this is absolutely necessary to retain research value.
- ❖ ***Disable cloud functionalities.*** Non-approved cloud storage is rarely a necessity since the RU provides approved alternatives.

Data security



Organisation

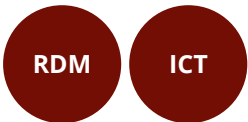
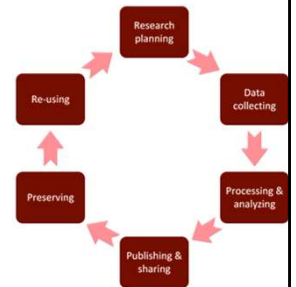


Technological



Project

- ❖ **Encryption: secure access**
- ❖ **Substitution: making paper digital**
- ❖ **Anonymization: re-identification impossible**
- ❖ **Pseudonymization: re-identification with keyfile (= personal data!)**



- ❖ Data security is a complex topic, but in essence occurs at three levels. The first two are relatively easy to implement, the third one places more responsibility with the researcher.
 1. Follow all ***organizational security practices***.
 2. Use only ***university-provided technology and software***.
 3. Ensure that you know ***who is responsible for data security*** within your project.
- ❖ There are guidelines available on encryption, substitution and anonymization & pseudonymization.
- ❖ With personal data especially anonymization and pseudonymisation is relevant:
 - ❖ Anonymization: re-identification is impossible.
 - ❖ Pseudonymization: re-identification is only possible by means of a keyfile.
- ❖ ***Treat pseudonymized data like personal data***. Deleting the keyfile can potentially make an identifiable dataset anonymous, but this is not guaranteed. For example when different datasets are combined.

Minimisation of data use



Limit access



Assign access rights



Remove ex-project members



Get consent for sharing



RDM

Radboud University 

- ❖ One important aspect of the security of personal data is the minimisation of data use. This emphasises that only authorized persons should have access to personal data. The fewer people have access to personal data, the smaller the risk for a security issue to arise.
- ❖ ***Limit access to authorized people*** who need it, for a pre-defined purpose and a limited period of time.
- ❖ ***Define access rights for each user:*** not everyone might need editing rights, or access to all the personal data. Sometimes read-only access to (part of) the personal data is sufficient.
- ❖ ***Revoke access rights when members leave a project***
- ❖ ***Make sure you have consent for sharing.*** This can include project members, other researchers, sharing in a repository but also sharing with RU staff for administrative, ICT and integrity reasons.

Data breaches

❖ Question: what is NOT a data breach?

Storing personal data longer than you have consent for

Sending a letter with personal data to the wrong address

Someone steals your laptop containing personal data

A computer containing personal data is hacked by a hacker

You gain access to personal data which you are not supposed to have access to

Storing personal data on an unprotected location

You lose an unencrypted memory stick containing personal data

You print a document containing personal data and forget to take it out of the office photocopier

You send personal data to the wrong e-mailaddress

You have anonymous survey results which turn out to be identifiable anyway

Accidentally damaging part of a dataset containing personal data

Radboud University



INTERACTION: LET RESEARCHERS THINK ABOUT WHICH OF THESE OPTIONS WOULD NOT BE CONSIDERED A DATA BREACH

By asking for a negative researchers are invited to read all the options, rather than mentioning the first answer that comes to mind. Strictly speaking all of these options could be considered data breaches, however some would be more severe than others. The definition of a data breach is 'a breakdown of security which accidentally or unlawfully (willfully and/or due to gross negligence) results in the destruction, loss, alteration, unauthorised disclosure of or access to personal data that is transmitted, stored or otherwise processed'.

The goal of this exercise is to make researchers aware that there is a large diversity of potential data breaches that could have potentially negative effects.

Data breaches

- ❖ Data breaches are diverse and can occur in different settings
- ❖ The GDPR expects you to report (suspicions of) data breaches
- ❖ Always contact the ICT Helpdesk in case of a data breach
- ❖ ICT Helpdesk: 024 362 22 22 or icthelpdesk@ru.nl



- ❖ ***Data breaches are diverse:*** This builds on the previous slide, emphasizing that data breaches include a wide variety of settings, and not just a hacker or stolen laptop.
- ❖ The rest of this slide contains practical information that refers researchers towards ICT support for any issues they might have with data breaches.

BREAK

Research planning



Privacy by design & privacy by default

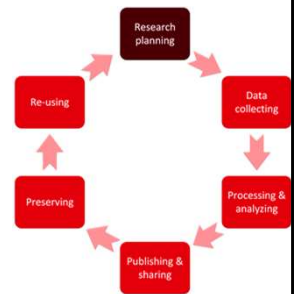


**By design:
start on day 1**



**By default:
aim for maximum
privacy**

- ❖ **Goal setting**
- ❖ **Data management plan**
- ❖ **Data protection impact assessment ?**



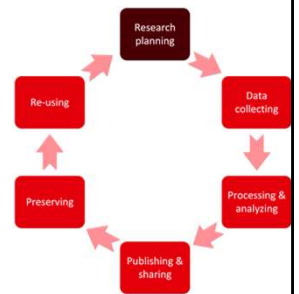
LPO

Radboud University 

- ❖ Privacy by design and privacy by default are two design principles that should underpin any academic study:
 - ❖ ***Privacy by design:*** Start with privacy in mind. It is not an afterthought which can be glued on at the end of a project but should be implemented on day 1.
 - ❖ ***Privacy by default:*** Aim for maximum privacy. Privacy should be the baseline of any study, it should only be compromised when this is essential for the research process.
- ❖ There are three steps which researchers can take to achieve the above design principles:
 - ❖ Determine your ***goal setting:*** This decides what personal data that is required for the study and commits the researcher to a certain approach.
 - ❖ Make a ***data management plan:*** This is always a good practice, but also helps specifically to design a study with privacy in mind.
 - ❖ Sometimes a ***data protection impact assessment*** is needed: this step is only applicable to high-risk studies.

Goal setting

- ❖ **What personal data you are collecting:**
Distinguish research, administrative and informed consent personal data.
- ❖ **What the legal basis is:**
If you have no explicit legal basis, do not process the data (further).
- ❖ **How long you are going to store it:**
Do not store personal data longer than is necessary.
- ❖ **These 3 limits define the space in which you can process personal data.**
But there are exceptions for scientific purposes.



LPO

Radboud University 

- ❖ Goal setting is an aspect of privacy by design. It requires that the research determines upfront how personal data will be handled during the study.
There is no room for vagueness here.

1. ***What personal data*** you are collecting

2. ***What the legal basis*** is under which you collect personal data. The legal basis for research will almost always be informed consent, although public interest and legitimate interest are also possible. If there is no legal basis personal data should not be processed.

3. ***How long*** you are going to store personal data

- ❖ This goal setting is the “framework” in which you can operate in accordance with the GDPR. If the processing of the personal data changes to a point where it is clearly outside of the scope of the original goal then it should not be processed. If the processing stays within the scope of the original goal then processing for another goal is allowed.
There are however exceptions for research that allow further processing for scientific research, meaning that processing personal data further is not an incompatible goal.

Data minimisation



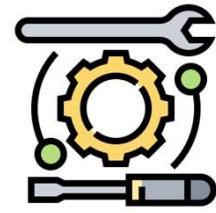
Process for the intended purpose



Process what is needed



Pseudonymize or anonymize as soon as possible



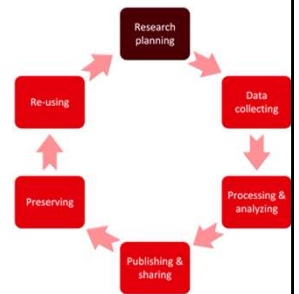
Maximum privacy settings



- ❖ This is different from minimisation of data use, which is concerned with the people who have access to personal data. Data minimisation concerns the personal data itself.
- ❖ **Only process personal data for the intended purposes.** If you don't need a certain personal data, don't process it. If you want to re-use data for a different purpose (f.e. new study or education) you can only do so if prior (or new) consent has been obtained.
- ❖ **Only process as much personal data as is required.** Review regularly if (part of) the collected personal data are still relevant or should be deleted.
- ❖ **Pseudonymise or anonymise your data as soon as you are able to.**
- ❖ **Use all the privacy options available to you in the software you use.** Many survey software allows you to disable IP tracking for example.

Data management plan

- ❖ A DMP helps you think of all research data-related decisions, including personal data
- ❖ The DMP structure follows the research cycle
- ❖ You can save, update and share a DMP as you make decisions along the way
- ❖ You can request feedback from the RDM Support and/or the data steward



RDM

Radboud University 

As RDM Support one of the services which we provide is the data management plan.

- ❖ This is an online tool that allows you to describe how you are using research data throughout your study and what decisions you have made. **Personal data is one of the topics** included in this data management plan.
- ❖ The DMP **mirrors the research cycle**, including data collection, data archiving and data publishing.
- ❖ You can **save, update and share a DMP** as you make decisions over the course of your research.
- ❖ At any time you can **request feedback** from RDM Support and/or the data steward from your institute.

Data protection impact assessment

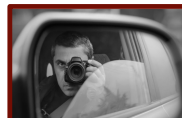
- ❖ The GDPR is based on an “appropriate management of risks”
- ❖ In high-risk cases a data protection impact assessment (DPIA) lets you take appropriate safeguards
- ❖ LPO can provide you with a pre-DPIA to determine if a DPIA is required.



Large scale processing



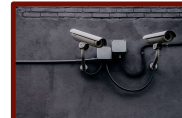
Vulnerable participants



Covert research



Profiling



Public surveillance



Combining datasets



New tools or technologies



Radboud University



In high-risk studies a **data protection impact assessment (DPIA)** makes it possible to assess the risks and to take appropriate safeguards. What determines the risks and thus the necessity of a DPIA is sometimes summarized as collaboration, geography and data.

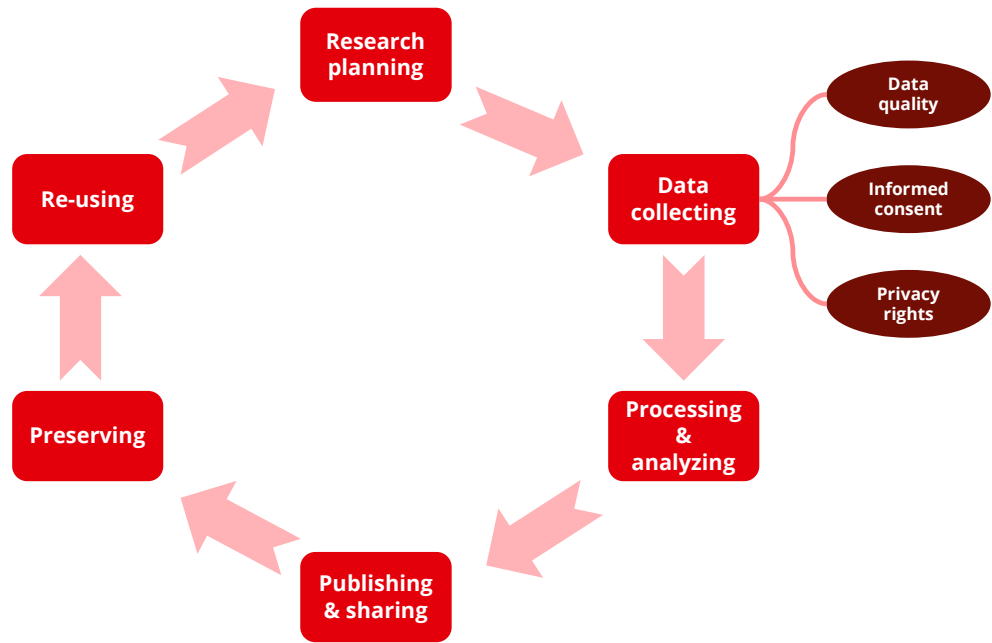
- ❖ What type of collaboration is involved with the study? Just one public institution (the university), multiple public institutions (the university and a government institute), or a public-private partnership (the university and a private company)?
- ❖ Which countries participate in the study? Only EEA countries or other countries as well?
- ❖ What data is used in the study? Publicly available data, a new private dataset, a combination of multiple datasets?

If you suspect there might be risks **you must contact LPO**. They can provide you with a **pre-DPIA**, which is a quick assessment that will determine if a DPIA is required.

High risks might occur in particular settings such as:

- ❖ Large scale processing of sensitive or special categories of personal data
- ❖ Vulnerable participants
- ❖ Covert or misleading research
- ❖ Automated processing (profiling)
- ❖ Systematic monitoring (public surveillance)
- ❖ Combining multiple datasets
- ❖ New tools or technologies

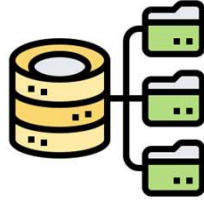
Data collecting



Data quality



Only store accurate and up-to-date personal data



Limit storage locations and sharing



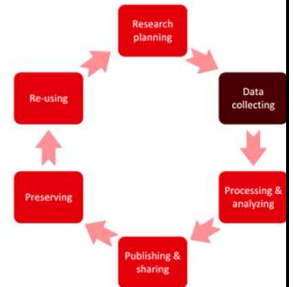
Perform frequent data checks



Use tools or repositories with version history



Provide contact information



- ❖ The GDPR expects you to store personal data that is ***accurate, complete and up-to-date***. It is your responsibility to take action when you find data that does not meet these requirements.
- ❖ Frequent ***data checks*** can be part of your privacy by design decisions. Data you cannot keep accurate should be deleted or updated as needed.
- ❖ ***Limit the number of storage locations*** of personal data, and ***share personal data as little as possible***. This reduces the risk that inaccurate information remains in use.
- ❖ Use dedicated tools or ***repositories*** for data checks or version control.
- ❖ Make sure that your participants know ***how to contact you*** when something changes.

Data quality

❖ Alternatively: include a “date of collection”, making your dataset a historical record.

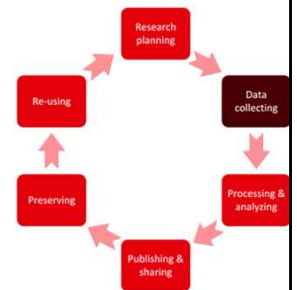


Participant #	Surname	Residence
1	Jansen	Nijmegen
2	Velde, van der	Arnhem

Participant 2 moves to a new city



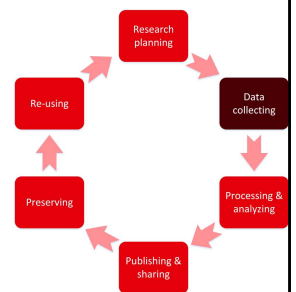
Participant #	Surname	Residence at time of interview	Interview date
1	Jansen	Nijmegen	17-03-2023
2	Velde, van der	Arnhem	09-05-2023



Radboud University 

- ❖ In practice maintaining data quality can be difficult, especially after completion of your research.
- ❖ An alternative approach is to ***include a “date of collection”***, which turns your personal data into a historical record with a fixed date.
- ❖ In the above example the first table would be inaccurate when participant 2 moves to a new city. The second table would not be affected, as it is a record of a certain date and not up-to-date.

Privacy rights



Radboud University

- ❖ **The GDPR provides people with 8 specific privacy rights.** These apply to researchers in their capacity as employees of the university, but also to research participants.
- ❖ While 8 privacy rights exist, in the practice of doing research **only three are really relevant.** This is the **right to be informed, the right to be forgotten** and **the right to object**. The other rights are generally excluded because of research exceptions in the GDPR and UAVG.

Context for the other privacy rights

- ❖ Right to access, Right to rectification & Right to restrict processing: UAVG Article 44 states that this does not apply to scientific research if consent is obtained and there are sufficient safeguards in place.
- ❖ Right to be forgotten, Right to object: GDPR Article 89 states that there can be exceptions for these in case of scientific, historical or statistical research, but this requires consent from your participants.
- ❖ **Right to data portability:** Participants have the right to receive any of their processed (personal) data. This right ends when data is de-identified, and this should be made clear in the information brochure.
- ❖ Rights in relation to automated decision making: In principle, a data subject is entitled not to be required to heed any decision taken by a data processing organisation that is solely based on automated processing, which is deemed to include profiling.

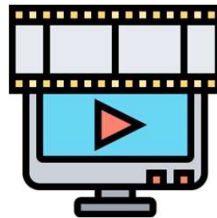
Right to be informed



Participants must be informed



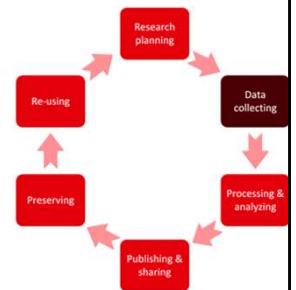
Complete and accurate information



Consider how you inform the participants



Provide contact information



LPO

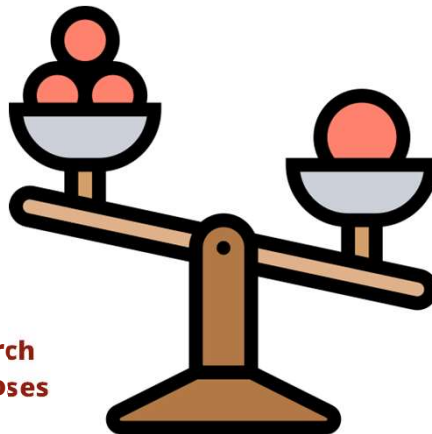
EC

Radboud University 

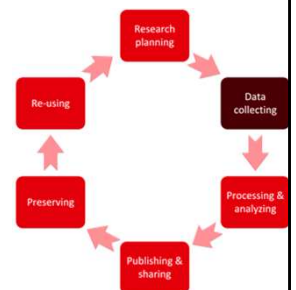
- ❖ Participants ***must be informed*** about the collection and use of their personal data. This means they receive ***complete and accurate information*** about the study
 - ❖ Why, how, how long will you process their personal data?
 - ❖ With whom will you share their personal data?
 - ❖ How will you protect their interests and privacy rights?
 - ❖ How and until when can participants withdraw from the study?
- ❖ Consider ***how you inform the participants***: concise, clear, accessible
 - ❖ Provide the same information in different ways and at different times
 - ❖ If possible, test the information delivery with your audience beforehand
 - ❖ Consider using visuals, videos or other tools
- ❖ Make sure your ***contact details are available*** for the duration of the study

Informed consent

- ❖ Collecting personal data
- ❖ Collecting special categories
- ❖ Recording audio or video
- ❖ Processing with third parties
- ❖ Sharing data with others
- ❖ Sharing data outside of the EEA
- ❖ Facilitating scientific integrity
- ❖ Publishing data for future research
- ❖ Using data for educational purposes



- ❖ Data minimisation
- ❖ Privacy rights of your participants
- ❖ Ethical considerations



LPO

EC

Radboud University 

- ❖ Informed consent means ***finding a balance*** between the things you want to do as a researcher, and the interests that matter for your participants.
- ❖ On ***the left side*** are the things that you might want to include in your informed consent to obtain the maximum scientific value from your data.
- ❖ On ***the right side*** are the limitations, rights and concerns that you need to guard for your participants.
- ❖ Asking consent for personal data ***processing that you do not need*** is problematic, but you also ***cannot be too specific***, since this limits the scientific value of your data
- ❖ Finding a balance between the two is something that can be discussed with the LPO and the EC.

I also agree that:

- the following personal data will be collected, used and stored for this study: [mention the personal data you have indicated in your Data Management Plan and information document].
- the following special personal data will be collected, used and stored for this study: [mention the special personal data you have indicated in your Data Management Plan and information document].
- video recordings/audio recordings/video and audio recordings [delete as appropriate] are made of me for scientific purposes.
- the coded/anonymised [delete as appropriate] research data will be available for at least 10 years for review and reuse in future scientific research.

The box below is optional. Use it only if it is applicable to your study. Remove options that do not apply to your study.

In addition, I give permission to (please check all that apply):

Yes No

- use the [identifiable/de-identified] recordings for scientific purposes (for example a scientific article or a scientific lecture)
- use the [identifiable/de-identified] recordings for educational purposes (for example a lecture class)
- share the [identifiable/de-identified] recordings with other scientists for use in future scientific research
- keep my contact details for a period of [specify period] in order to be contacted for follow-up research

This is a screenshot the informed consent form used in the Faculty of Arts. Other ethics committees have different consent forms.

As you can see the consent form asks explicit consent for **personal, special categories of personal data** and **video/audio data**.

Furthermore it accounts for the possibility that data is **shared with other researchers** or **used for educational purposes**.

Right to be forgotten

- ❖ If a participant withdraws consent, the data controller **must cease processing** that data.
- ❖ **This is not absolute:** the researcher can specify beforehand what is and is not possible.



Before collection:

- ❖ Participant does not participate
- ❖ All personal data is deleted



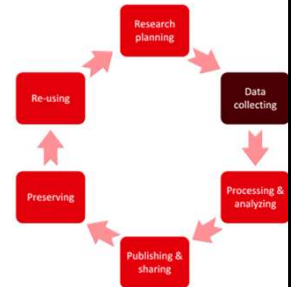
During collection:

- ❖ Same as before
- ❖ Except if data can be made fully anonymous



After publication:

- ❖ Removal is not possible
- ❖ Anonymize or exclude from future studies



LPO

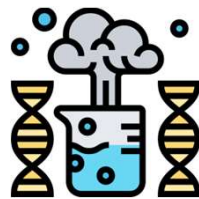
- ❖ General statement: If a participant objects, the data controller **must cease processing** that data.
- ❖ There are exceptions, however. There can be compelling reasons that a researcher can explain beforehand.
- ❖ **Before the data collection has started:** the participant will not participate and all personal data must be deleted.
- ❖ **During the data collection:** the research data must either be deleted or be made fully anonymous.
- ❖ **After publication of the data:** removal of (personal) data is generally not possible. Sometimes data can be anonymized, or at least excluded from future research.

Right to object

- ❖ Participants can object to **legitimate interest** processing.
- ❖ In that case you must either stop processing or motivate why it is justified.



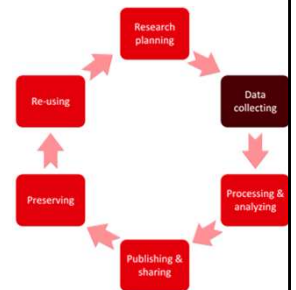
The data is already anonymized and no longer retrievable.



Removing data would introduce substantial bias



The participant made their own personal data publicly available.



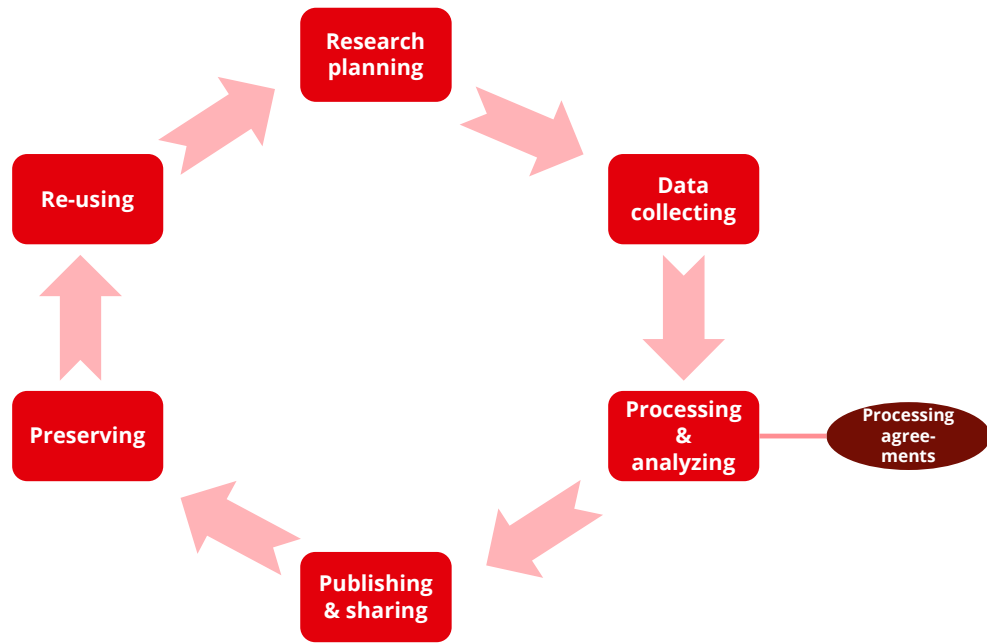
LPO

Radboud University 

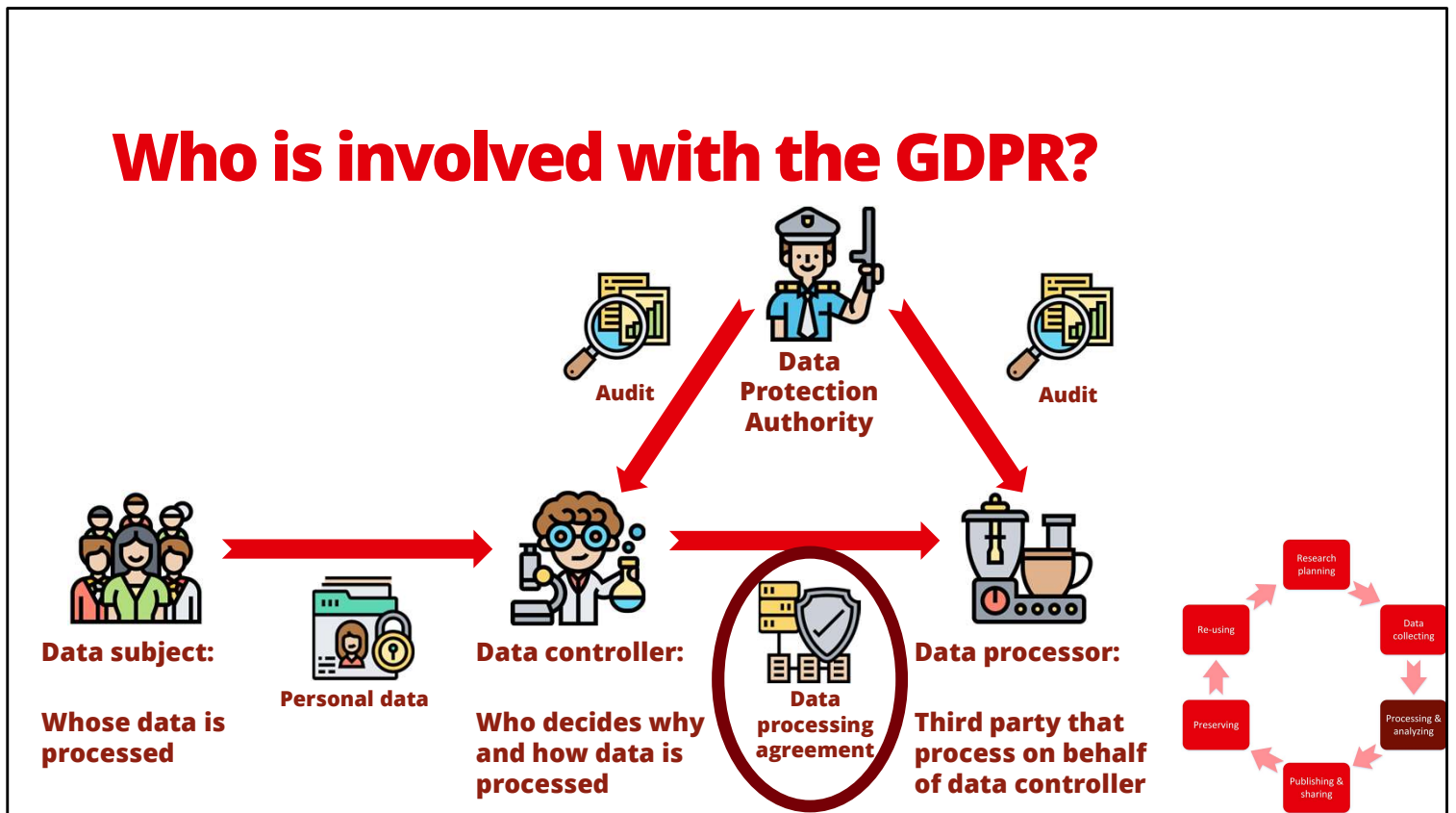
Data subjects have the right to object to what you are doing with their personal data. This right applies when the processing is based on the legal basis of legitimate processing ([art. 21](#)). In case of objection, you have to stop your processing activities and thus delete any data you have from the particular data subject, unless you can demonstrate concrete grounds for overriding the data subject's rights.

This could for example be because the data is already anonymized, because excluding the data subject would substantially bias your results, or because the personal data is already made public by the participant themselves.

Processing & analyzing



Who is involved with the GDPR?



To understand what **data processing agreements** are about, one should first know a bit about the different roles in the GDPR.

Data Subject: A data subject is anyone **whose personal data is being processed**. As such, it is the person to whom the personal data relates, and who can be identified directly or indirectly through personal data. These are the **research participants, patients, informants, test subjects, etc.**

Data controller: A data controller is the person or organisation **that determines the purpose of the personal data processing**. This means that the data controller decides whether personal data will be processed and, if so: what processing will be involved; what personal data will be processed; the purpose for which personal data is processed; and the manner in which the organisation will do that. This is generally the **researcher**.

Data processor: A third party that **processes personal data on behalf of a data controller**. A processor is not responsible for personal data processing, but a processor has a number of derivative duties. A processor must for example secure and refrain from disclosing data. They process personal data at the request of the data controller, and cannot use the personal data for their own purposes. This could be **research partners, repositories, transcription services, cloud storage**.

Data Protection Authority: The authority ensures compliance and can audit both the data controller and the data processor.

Data processing agreement

- ❖ **As data controller you are responsible, even when you give personal data to a data processor.**
- ❖ **Only use data processors that comply with the GDPR.**
- ❖ **A data processing agreement specifies how personal data can be used by the data processor.**



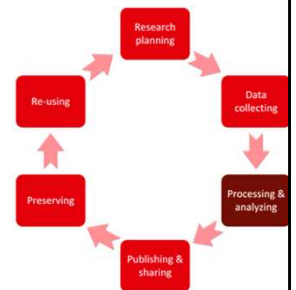
Data will be deleted after processing



Data cannot be used for additional purposes



Data processor participates in audits



LPO

Radboud University 

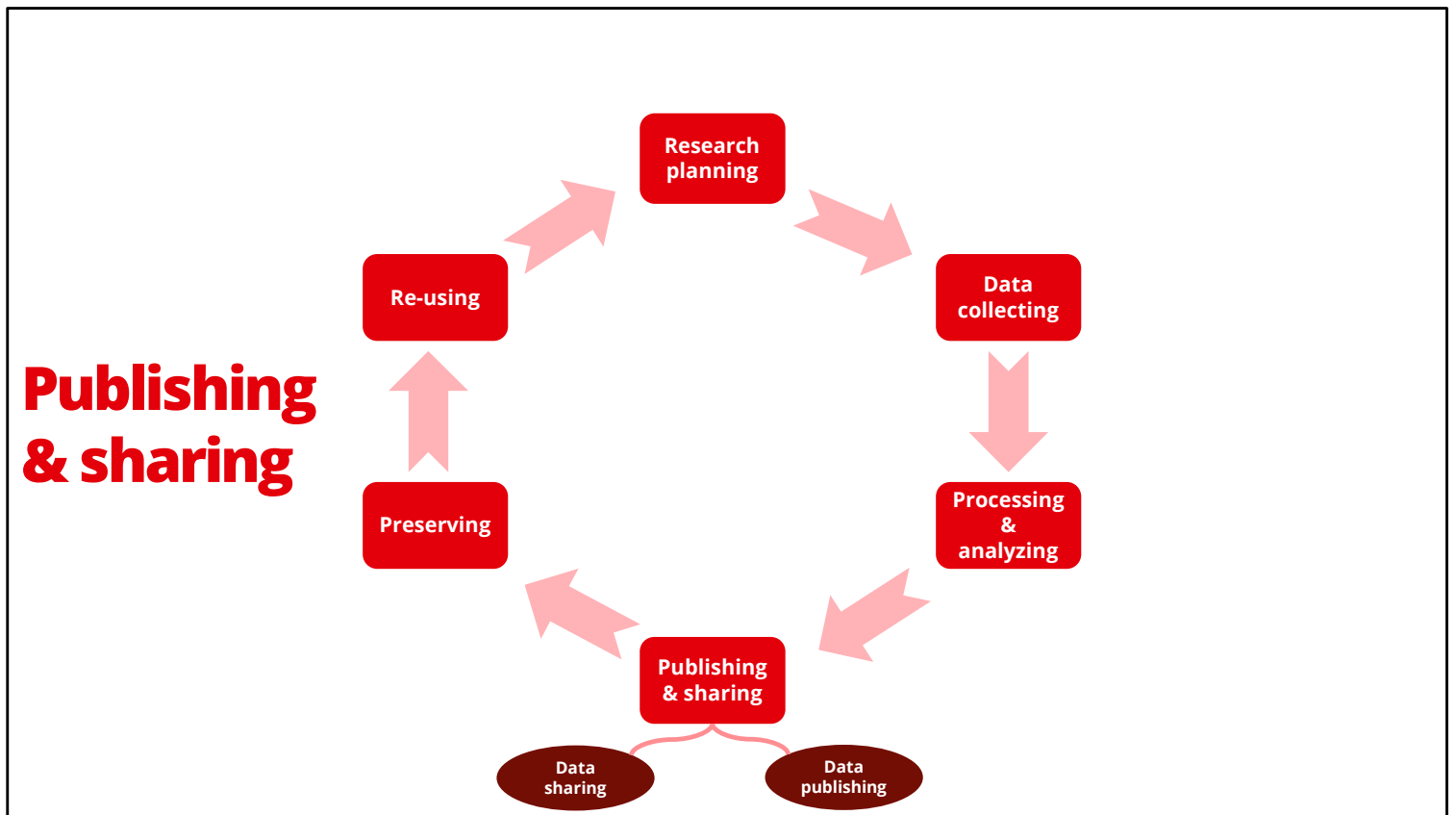
Whenever you as ***data controller*** hand personal data over to a ***data processor***, it is still the data controller that ***remains responsible***.

This means that you should only ever ***use data processors that comply with the GDPR***. You have to be selective where you send personal data.

Moreover, before sending personal data to a data processor it is important to ***have a data processing agreement in place***.

Such an agreement covers various topics that are important to you as a researcher, for example:

1. It guarantees that the data processor will ***delete the data afterwards***.
2. It guarantees that the data processor will ***not use the data for its own purposes*** (f.e. profit)
3. It guarantees that the data processor will ***participate in audits*** from the Data Protection Authority



Data sharing generally refers to the sharing of data during the ongoing research.

After the research is finished it is sometimes possible to ***publish data*** in a way that others can access it.

Sharing personal data



Specify who you share with in the informed consent



Include research support, administration, archive curation



Only share with consent or an agreement



Contact LPO before sharing outside the EEA

RDM

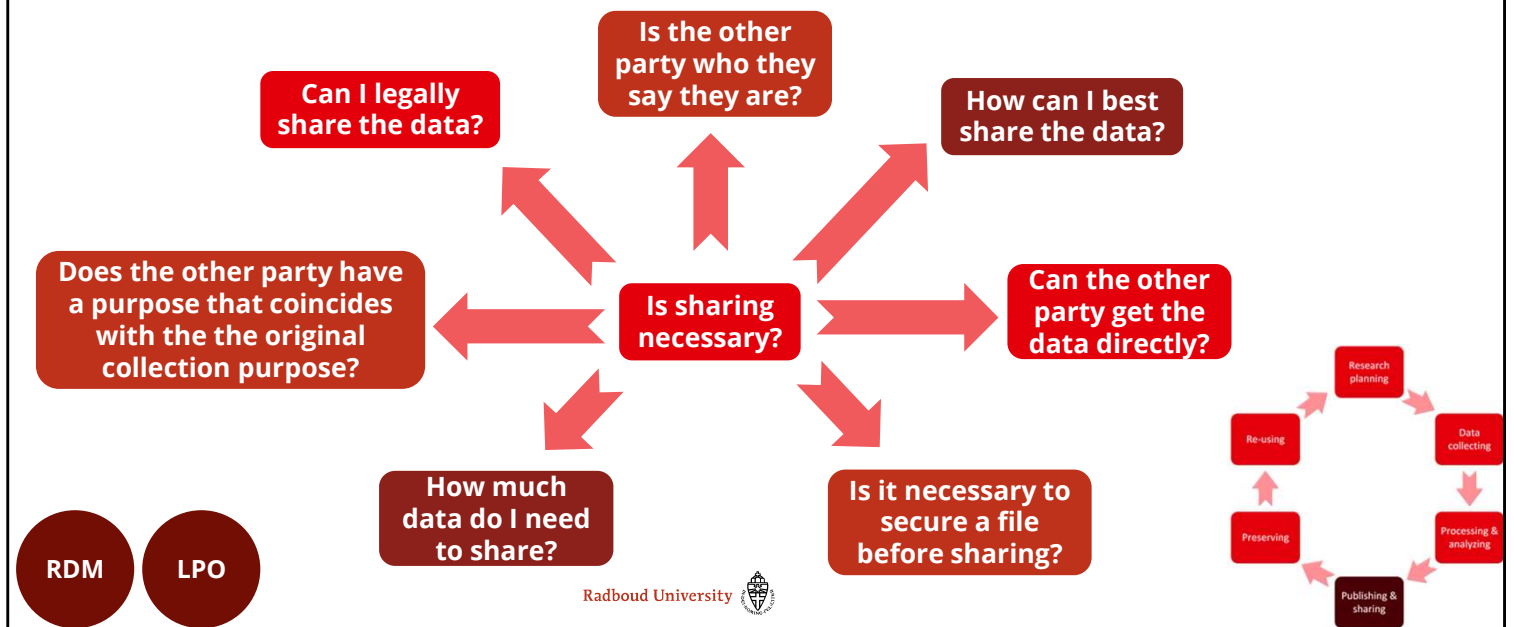
LPO

Radboud University 



- ❖ If you want to share personal data with anyone it is important to **inform your participants about who you will share data with**. It is also important to **get explicit consent** for this.
- ❖ This can include **other researchers**, any **external services** that you need for your research, but also **university staff** such as research support, ICT, archive curation and so on.
- ❖ If you are missing consent but would still like to share, either **contact participants** to get it or see if a **suitable legal agreement** can be made.
- ❖ In essence **you cannot share personal data outside of the EEA**, unless the other party adheres to the GDPR. If this is unavoidable **you must contact the privacy officer** to get a legal agreement set up.

Sharing personal data



- ❖ Make conscious decisions when sharing personal data:
 - ❖ ***Is sharing necessary?*** Does the other party really need the data? Or would it just be convenient for them to have it?
 - ❖ ***Can you legally share the data?*** Do you have consent? Is there an agreement in place? Does the other party adhere to the GDPR?
 - ❖ ***Does the other party have a purpose that coincides with the original collection purpose?*** If the original purpose was research, the other party cannot use the data for commercial purposes.
 - ❖ ***How much data do I need to share?*** Perhaps the other party only needs some of the personal data?
 - ❖ ***Is it necessary to secure a file with a password?*** This can be a good practice regardless of the context.
 - ❖ ***Can the other party get the data directly?*** If possible this is usually a better alternative than sharing the data indirectly.
 - ❖ ***How can I best share the data?*** The RU provides various services (workgroup folder, SURF FileSender, Teams, e-mail). Never use cloud services such as WeTransfer.
 - ❖ ***Is the other party who they say they are?*** This is not just about confirming identities, but for example also about making sure that you e-mail to the right addresses.

Publishing personal data



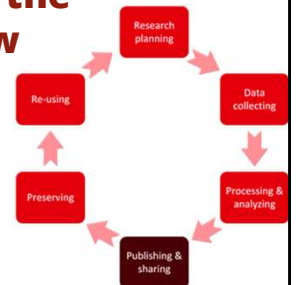
Publish pseudonymized or anonymized data whenever possible



Be mindful of accidental identification



Consider the data exchanged in the peer review

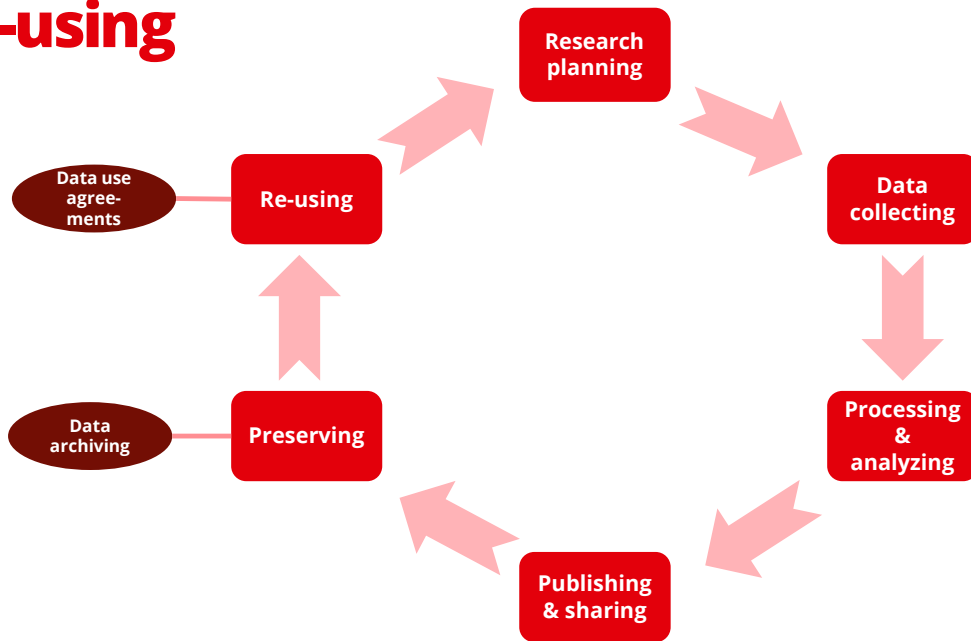


RDM

Radboud University 

- ❖ Whenever possible ***publish only pseudonymized or anonymized personal data***. Whenever possible means as much as is possible ***without losing the scientific value*** of the data.
- ❖ Be sensitive for ***accidental, indirect identification***: this can happen quite easily with certain combinations of personal data.
- ❖ Minimize the personal data you must transfer for ***peer review purposes***: remove non-essential personal data and make sure you get a data processor agreement with the publisher.

Preserving & re-using



Data archiving



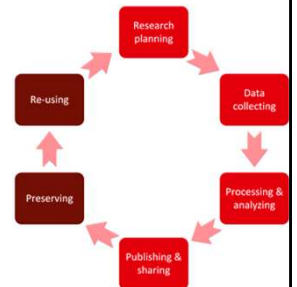
Personal research data can be archived in a repository



Do not include administrative or informed consent personal data



Avoid personal data in metadata, documentation or file or folder names



- ❖ Repositories serve as a safe location in which you ***archive*** research data, including personal data. The Radboud has its own repository: the Radboud Data Repository, but there are many others, ranging from discipline-specific to generalist.
- ❖ Do not include ***administrative*** or ***informed consent*** personal data in the repository.
- ❖ Do not include personal or sensitive data in ***metadata, documentation or file or folder names***

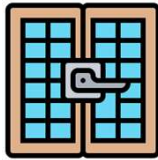
Access levels

If you want to share data in a repository access levels matter:



Open Access

- ❖ Anonymous data
- ❖ Anyone can access unrestricted
- ❖ CC Licence



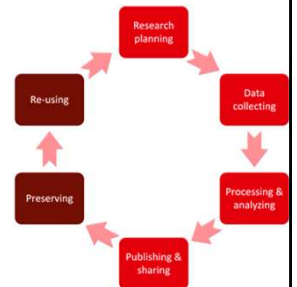
Registered Access

- ❖ Potentially identifiable or pseudonymized data
- ❖ Data use agreement



Restricted Access

- ❖ Sensitive or directly identifiable data
- ❖ Explicit approval from researcher
- ❖ Only shared in consultation with datasteward



❖ If you want to **share** personal research data in a repository this requires **explicit consent** from your participants. Depending on the type of personal data and the informed consent you can choose an appropriate access level. Not every repository offers all access levels. The example used here is based on the Radboud Data Repository.

❖ **Open Access:**

- ❖ Anonymous data with no privacy concerns
- ❖ Anyone can access the data anonymously

❖ **Open Access for Registered Users:**

- ❖ Potentially identifiable or pseudonymized data
- ❖ Users must log in and agree with a data use agreement before they gain access

❖ **Restricted Access:**

- ❖ Sensitive or directly identifiable personal data
- ❖ Users must have explicit approval by a person before they gain access
- ❖ You must consult the datasteward before sharing identifiable personal data

Re-using

❖ Re-using research data with identifiable personal data requires a data use agreement.

❖ This specifies what you can and cannot do with the data:



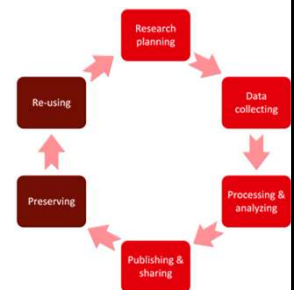
Linking datasets



Redistributing data to others



Acknowledging the use in publications



RDM

Radboud University 

- ❖ Re-using research data with identifiable personal data requires a ***data use agreement***. This sets out certain terms that you have to follow as you re-use the data. It aims to protect the participants and regulate the distributing of the dataset.
- ❖ A data use agreement can specify various things, for example:
 - ❖ ***Linking the dataset*** in a way that could identify participants
 - ❖ ***Redistributing*** the data to others
 - ❖ ***Acknowledging*** the use of the data in publications

Data use agreement for identifiable human data

Version RU-HD-1.1

I request access to the data collected in the digital repository of the Radboud University, established at Nijmegen, the Netherlands (hereinafter referred to as the Radboud University), and I agree to the following:

1. I will comply with all relevant rules and regulations imposed by my institution and my government, including but not limited to the General Data Protection Regulation and other relevant privacy laws. This may mean that I need my research to be approved or declared exempt by a committee that oversees research on human subjects, e.g. my Institutional Review Board or Ethics Committee.
2. I will not attempt to establish the identity of or attempt to contact any of the included human subjects. I will not link this data to any other database in a way that could provide identifying information. I understand that under no circumstances will the code that would link these data to an individual's personal information be given to me, nor will any additional information about individual subjects be released to me under these Data Use Terms.
3. I will not redistribute or share the data with others, including individuals in my research group, unless they have independently applied and been granted access to this data.
4. I will acknowledge the use of the data and data derived from the data when publicly presenting any results or algorithms that benefitted from their use.
 - (a) Papers, book chapters, books, posters, oral presentations, and all other presentations of results derived from the data should acknowledge the origin of the data as follows: "Data were provided (in part) by the Radboud University, Nijmegen, The Netherlands".
 - (b) Authors of publications or presentations using the data should cite relevant publications describing the methods developed and used by the Radboud University to acquire and process the data. The specific publications that are appropriate to cite in any given study will depend on what the data were used and for what purposes. When applicable, a list of publications will be included in the collection.
 - (c) Neither the Radboud University, nor the researchers that provide this data should be included as an author of publications or presentations if this authorship would be based solely on the use of this data.
5. Failure to abide by these guidelines will result in termination of my privileges to access to these data.

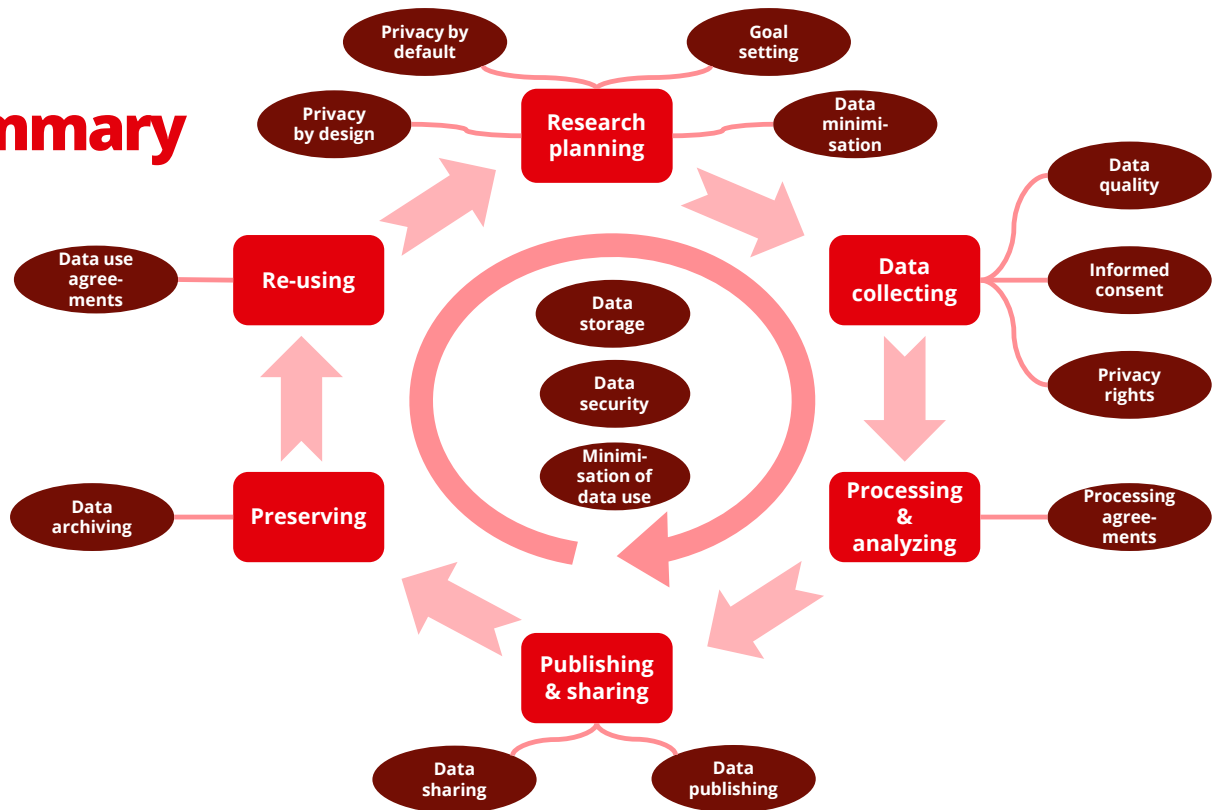
This is the data use agreement signed by researchers when they access a **registered dataset**: <https://data.ru.nl/doc/dua/RU-HD-1.1.html?22>

As you can see it covers various aspects related to the re-use of the data:

1. It expects you to ***follow the rules and regulations***.
2. It expects you ***not to re-identify*** the participants in the dataset.
3. It expects you ***not to redistribute*** or share the data with others.
4. It expects you to ***acknowledge the source of the data*** in any publications.

When you want to access a **restricted dataset** a more elaborate legal document is made up which is about three times as long. This is a legally binding document that is signed by the dean of the faculty.

Summary



This is everything you need to know about working with personal data. What remaining questions are there?

QUIZ

BE A DATA STEWARD



As a final “test” you get to be a data steward and have to advice a researcher that is planning a very elaborate study.

Case example

A researcher wants to collect these data:

- ❖ MRI-research into the brain
- ❖ Blood samples
- ❖ Urine samples
- ❖ Taste test
- ❖ Measurements such as length and weight
- ❖ Survey about food intake and behaviour
- ❖ Tracking participants with a phone app for a week

Participants can not participate if they:

- ❖ Do smoke
- ❖ Had a stomach reduction in the last five years.
- ❖ Had a medical condition such as diabetes, cardiovascular diseases, kidney failure, cancer or a psychiatric condition.
- ❖ Drug use of antidepressants or anti-inflammatories
- ❖ Are pregnant or breastfeeding
- ❖ Have non-removable metals such as a prosthetic.

This is the research brought before you. The researcher wants to **collect various types of personal data**, ranging from MRI-scans to body tissue, body measures, a survey and a phone app.

Moreover the researcher also wants to select a certain category of participants, meaning that **not everyone can participate.**

Case example

A researcher wants to collect these data:

- ❖ MRI-research into the brain
- ❖ Blood samples
- ❖ Urine samples
- ❖ Taste test
- ❖ Measurements such as length and weight
- ❖ Survey about food intake and behaviour
- ❖ Tracking participants with a phone app for a week

Participants can not participate if they:

- ❖ Do smoke
- ❖ Had a stomach reduction in the last five years.
- ❖ Had a medical condition such as diabetes, cardiovascular diseases, kidney failure, cancer or a psychiatric condition.
- ❖ Drug use of antidepressants or anti-inflammatories
- ❖ Are pregnant or breastfeeding
- ❖ Have non-removable metals such as a prosthetic.

Would the researcher need informed consent in order to determine if participants can participate?

Would the researcher need informed consent in order to determine if participants can participate?

Yes, but only for the initial selection procedure. When participants are excluded they are no longer part of the study and any personal data will be destroyed. Alternatively the legal basis of legitimate interest could offer an option to contact participants without informed consent. A LPO could advice how to best approach this.

This could be a tricky question if researchers are not familiar with inclusion/exclusion criteria. Regardless however, what is being collected are still clearly personal data, so informed consent should be obtained before any data can be processed.

Case example

A researcher wants to collect these data:

- ❖ MRI-research into the brain
- ❖ Blood samples
- ❖ Urine samples
- ❖ Taste test
- ❖ Measurements such as length and weight
- ❖ Survey about food intake and behaviour
- ❖ **Tracking participants with a phone app for a week**

Participants can not participate if they:

- ❖ Do smoke
- ❖ Had a stomach reduction in the last five years.
- ❖ Had a medical condition such as diabetes, cardiovascular diseases, kidney failure, cancer or a psychiatric condition.
- ❖ Drug use of antidepressants or anti-inflammatories
- ❖ Are pregnant or breastfeeding
- ❖ Have non-removable metals such as a prosthetic.

Can the researcher go ahead and download a suitable phone app from the App Store?

Can the researcher go ahead and download a suitable phone app from the App Store?

No. ***The phone app company is a data processor*** who will process personal data on behalf of the researcher. As such the researcher can only use an app which is ***approved by their research institute*** or for which there exists a ***data processor agreement***.

Case example

A researcher wants to collect these data:

- ❖ MRI-research into the brain
- ❖ Blood samples
- ❖ Urine samples
- ❖ Taste test
- ❖ Measurements such as length and weight
- ❖ **Survey about food intake and behaviour**
- ❖ Tracking participants with a phone app for a week

Participants can not participate if they:

- ❖ Do smoke
- ❖ Had a stomach reduction in the last five years.
- ❖ Had a medical condition such as diabetes, cardiovascular diseases, kidney failure, cancer or a psychiatric condition.
- ❖ Drug use of antidepressants or anti-inflammatories
- ❖ Are pregnant or breastfeeding
- ❖ Have non-removable metals such as a prosthetic.

Would you recommend open-ended or close-ended questions if the researcher wants to avoid personal data in the survey?

Would you recommend open-ended survey questions if the researcher wants to avoid accidental recording of personal data?

Close-ended survey questions are generally recommended. Open-ended questions always create a risk that personal data is included accidentally.

Case example

A researcher wants to collect these data:

- ❖ MRI-research into the brain
- ❖ Blood samples
- ❖ Urine samples
- ❖ Taste test
- ❖ Measurements such as length and weight
- ❖ Survey about food intake and behaviour
- ❖ Tracking participants with a phone app for a week

Participants can not participate if they:

- ❖ Do smoke
- ❖ Had a stomach reduction in the last five years.
- ❖ Had a medical condition such as diabetes, cardiovascular diseases, kidney failure, cancer or a psychiatric condition.
- ❖ Drug use of antidepressants or anti-inflammatories
- ❖ Are pregnant or breastfeeding
- ❖ Have non-removable metals such as a prosthetic.

Could this study benefit from a visit to the LPO?

Could this study benefit from a visit to the LPO?

Yes. They are collecting ***special categories of personal data*** (related to health), they are ***combining different personal data***, they are using ***potentially new tools*** (phone app) that might require a ***data protection impact assessment (DPIA)***.

It is likely very obvious to researchers that a visit to the LPO is required. More important is the follow-up question, why such a visit would be advisable.

Case example

A researcher wants to collect these data:

- ❖ MRI-research into the brain
- ❖ Blood samples
- ❖ Urine samples
- ❖ Taste test
- ❖ Measurements such as length and weight
- ❖ Survey about food intake and behaviour
- ❖ Tracking participants with a phone app for a week

Participants can not participate if they:

- ❖ Do smoke
- ❖ Had a stomach reduction in the last five years.
- ❖ Had a medical condition such as diabetes, cardiovascular diseases, kidney failure, cancer or a psychiatric condition.
- ❖ Drug use of antidepressants or anti-inflammatories
- ❖ Are pregnant or breastfeeding
- ❖ Have non-removable metals such as a prosthetic.

A colleague asks if she can use the MRI data, would this be acceptable?

A colleague wants to use the MRI data for a separate study, would this be acceptable?

This would depend on various things, for example if there is ***informed consent*** for sharing, if the colleague intends to use the personal data for a ***similar purpose as the original purpose*** of the data collection and ***how much personal data*** the colleagues require for their purposes. In general ***minimisation of data use*** should be the baseline and personal data should not be shared unless there is explicit consent.

Case example

A researcher wants to collect these data:

- ❖ MRI-research into the brain
- ❖ Blood samples
- ❖ Urine samples
- ❖ Taste test
- ❖ Measurements such as length and weight
- ❖ **Survey about food intake and behaviour**
- ❖ Tracking participants with a phone app for a week

Participants can not participate if they:

- ❖ Do smoke
- ❖ Had a stomach reduction in the last five years.
- ❖ Had a medical condition such as diabetes, cardiovascular diseases, kidney failure, cancer or a psychiatric condition.
- ❖ Drug use of antidepressants or anti-inflammatories
- ❖ Are pregnant or breastfeeding
- ❖ Have non-removable metals such as a prosthetic.

For integrity the researcher suggests including the participant's real name instead of a pseudonym in the dataset. Do you agree?

For the purpose of integrity the researcher suggests using the participant's real name instead of a pseudonym. Do you agree?

No. There is no reason to include a direct identifier such as a name in a dataset, doing so would create an ***unnecessary privacy risk*** and make it ***more difficult to share or publish*** the dataset. Using a ***pseudonym linked to a keyfile*** would be the better course of action in this case.

Case example

A researcher wants to collect these data:

- ❖ MRI-research into the brain
- ❖ Blood samples
- ❖ Urine samples
- ❖ Taste test
- ❖ Measurements such as length and weight
- ❖ Survey about food intake and behaviour
- ❖ **Tracking participants with a phone app for a week**

Participants can not participate if they:

- ❖ Do smoke
- ❖ Had a stomach reduction in the last five years.
- ❖ Had a medical condition such as diabetes, cardiovascular diseases, kidney failure, cancer or a psychiatric condition.
- ❖ Drug use of antidepressants or anti-inflammatories
- ❖ Are pregnant or breastfeeding
- ❖ Have non-removable metals such as a prosthetic.

The phone app can also record GPS and call history, even though this is not required. Would it be necessary to block these features?

The phone app can also record GPS and call history, even though this is not required. Would it be necessary to block these features?

Yes. This would fit with the principle of **data minimisation** and would greatly **reduce the privacy risks** for the participants.

Case example

A researcher wants to collect these data:

- ❖ MRI-research into the brain
- ❖ **Blood samples**
- ❖ **Urine samples**
- ❖ Taste test
- ❖ Measurements such as length and weight
- ❖ Survey about food intake and behaviour
- ❖ Tracking participants with a phone app for a week

Participants can not participate if they:

- ❖ Do smoke
- ❖ Had a stomach reduction in the last five years.
- ❖ Had a medical condition such as diabetes, cardiovascular diseases, kidney failure, cancer or a psychiatric condition.
- ❖ Drug use of antidepressants or anti-inflammatories
- ❖ Are pregnant or breastfeeding
- ❖ Have non-removable metals such as a prosthetic.

The body tissue is analyzed in a lab with a very good reputation, so the researcher doubts that a processor agreement is necessary. What do you say?

The body tissue is analyzed in a lab with a very good reputation, so the researcher states that a processor agreement won't be necessary. What do you say?

No. A good reputation is no excuse to not ***get a data processor agreement***. It is in everyone's interest to have a clear legal framework for the data transfer in case a ***data breach occurs*** or other issues arise.

Helpful links

- ❖ **General questions:** www.ru.nl/rdm or rdmsupport@ubn.ru.nl
- ❖ **Data management plan: Log in at** www.ru.nl/research-information-services
- ❖ **Radboud Data Repository: Help page on** <https://data.ru.nl>
- ❖ **Data breach: ICT Helpdesk via 024 362 22 22 or** icthelpdesk@ru.nl
- ❖ **Questions related to your own privacy rights:** mijnprivacy@ru.nl

Datastewards (RDM)

Research Institute	Data steward	Research Institute	Data steward
Behavioural Science Institute	Rob Gommans	Radboud Institute for Biological and Environmental Sciences	Eelke Jongejans
Centre for Language Studies	Henk van den Heuvel	Radboud Institute for Culture & History	Henk van den Heuvel
Donders Institute for Brain, Cognition and Behaviour	Bernhard Englitz (DCN) Temporarily vacant (DCCN) Miriam Kos (DCC) Joanes Grandjean (DCMN)	Radboud Institute for Health Sciences	Team Datastewardship IM
Institute for Computing and Information Sciences	Gunes Acar	Radboud Institute for Molecular Life Sciences	Team Datastewardship IM (UMC) Joost Martens (FNWI)
Institute for Management Research	Francie Manhardt	Radboud Social Cultural Research	Bas Hofstra
Institute for Mathematics, Astrophysics and Particle Physics	Andrew Levan	Radboud Teachers Academy	Robin Satter
Institute for Molecules and Materials	Evan Spruijt	Research Centres of the Faculty of Law	Anita Böcker
Institute for Science in Society	Temporarily vacant	Research Institute for Philosophy, Theology and Religious Studies	Sanna van Roosmalen

The datastewards are the first point of contact for researchers at the RU. They are experts on the data management practices in their own field and have the most knowledge of the local policies of their research institute. If datastewards need additional advice, they can fall back to the RDM Support team for additional support.

Local privacy officers (LPO)

Faculty	Privacy officer	Faculty	Privacy officer
Donders Institute for Brain, Cognition and Behaviour	Steven Ligthert	Faculty of Science	Paul Deimann Bjorn Bellink (backup)
Faculty of Arts	Igljka Vassileva-van der Heiden Jelmer Gerritsen	Faculty of Social Sciences	Enna Lujinović
Faculty of Law	Ellen Nieboer	Nijmegen School of Management	Ellen Nieboer
Faculty of Philosophy, Theology and Religious Studies	Igljka Vassileva-van der Heiden Sanne van Roosmalen	Radboud University Medical Centre	privacy@radboudumc.nl

The local privacy officers (sometimes supported by local privacy coordinators) are the first line of inquiry for any questions with regards to personal data or privacy in research. They can fall back on legal and privacy experts that operate university-wide.



Ethics Committees (EC)

Ethics Committees
<u>Ethics Assessment Committee Law and Management</u>
<u>Ethics Committee Faculty of Social Sciences</u>
<u>Ethics Assessment Committee Humanities</u>
<u>Ethics Committee Science</u>
<u>Ethics Committee Radboud Teachers Academy</u>

Sources

Slide	Source
3	https://freerangestock.com/photos/136939/close-up-of-a-question-mark-drawn-with-chalk.html
4	https://www.ru.nl/over-ons/nieuws/je-tekst-door-google-translate-halen-datalek-of-niet https://www.rtnieuws.nl/tech/artikel/5247775/radboudumc-radboud-nijmegen-datalek https://ans-online.nl/artikelen/bestelsysteem-refter-verzamelt-illegaal-persoonsgegevens/ https://www.voxweb.nl/nieuws/privacyhoogleraar-bart-jacobs-overstap-van-universiteit-naar-clouddiensten-microsoft-is-illegaal https://ans-online.nl/artikelen/faculteit-der-rechtsgeleerdheid-wil-proctoring-herintroduceren/
5	Photo by Daniel Roberts via Pixabay via https://pixabay.com/nl/illustrations/doolhof-puzzel-labyrint-uitdaging-5768511/
7	Photo by Leopold Böttcher via Pixabay https://pixabay.com/nl/photos/het-doel-doel-boogschieten-4508412/
8-9	Photo by Pexels via Pixabay https://pixabay.com/nl/photos/stoelen-conferentieruimte-meubilair-2181951/ Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
11	Photo by Chickenonline via Pixabay https://pixabay.com/nl/illustrations/vlag-europese-unie-brexit-europa-1198978/ Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
12	GDPR Enforcement tracker https://www.enforcementtracker.com/
13	Langedijk, Annette, Huijser, Dorien, Zundert, Joris van, Bron, Esther, Kesteren, Erik-Jan van, Boeschoten, Laura, & Dijkstra, Freek. (2023, March 28). Your secrets are safe with us: Tools for research with sensitive data. Zenodo. https://doi.org/10.5281/zenodo.7778159
14	Photo from Wikipedia https://en.wikipedia.org/wiki/European_Economic_Area#/media/File:European_Economic_Area_member_states.svg
16	Photo by Edar via Pixabay https://pixabay.com/nl/photos/bedrijf-handtekening-contract-962359
19	Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp

Sources

Slide	Source
21	Photo by Gerd Altmann on Pixabay https://pixabay.com/nl/illustrations/handtekening-handschrift-523237/
24	Photo by Anastasiya Babienko on Pixabay https://pixabay.com/nl/photos/vrouw-portret-model-glimlach-657753
30	Photo by rhoda_alex on Unsplash https://unsplash.com/photos/4OD7NWwhgi8 Photo by Karolina Grabowska via Pixabay https://pixabay.com/nl/photos/goud-nek-kettingen-stijl-sieraden-792002/ Photo by Andreas Breitling via Pixabay https://pixabay.com/nl/photos/opiniepeiling-enqu%C3%A4te-stemmen-1594962/ Photo by David Waters via Pixabay https://pixabay.com/nl/photos/interview-ontmoeting-zakenman-1389206/
31	Photo by  Use at your Ease  via Pixabay https://pixabay.com/nl/photos/handen-team-verenigde-samen-mensen-1917895/ Screen capture from movie V for Vendetta Afbeelding van Gordon Johnson via Pixabay https://pixabay.com/nl/vectors/gouden-regel-glimmend-metalen-1321410/ https://en.wikipedia.org/wiki/Trade_union#/media/File:Garment Workers on Strike, New York City circa 1913.jpg https://en.wikipedia.org/wiki/DNA#/media/File:T7_RNA_polymerase.jpg https://en.wikipedia.org/wiki/Fingerprint#/media/File:Fingerprint detail on male finger in T%C5%99eb%C3%AD%C4%8D, T%C5%99eb%C3%AD%C4%8D District.jpg https://en.wikipedia.org/wiki/Disease#/media/File:Mycobacterium tuberculosis.jpg Screen capture from Sims 4
32	https://www.rijksoverheid.nl/binaries/large/content/gallery/rijksoverheid/content-afbeeldingen/onderwerpen/paspoort-en-identiteitskaart/bsn-identiteitskaart-2011-voorkant.jpg Photo by Photo Mix via Pixabay https://pixabay.com/nl/photos/digitale-marketing-seo-google-1725340/ Photo by Tayeb MEZAHEDIA via Pixabay https://pixabay.com/nl/photos/stempel-geheim-bovenkant-spion-4299143/ Screen capture from movie Office Space https://cdn.vox-cdn.com/thumbor/9ARTrIE8kSpX4sWPapX_Sj-EDDs=/1400x0/filters:no_upscale()/cdn.vox-cdn.com/uploads/chorus_asset/file/13890766/job_interview_office_space.jpeg Photo by Welcome to All! 🌍 via Pixabay https://pixabay.com/nl/photos/euro-bankbiljetten-munten-1159935/ Photo by Ichigo121212 via Pixabay https://pixabay.com/nl/photos/gevangenis-gevangeniscel-misdrijf-553836/ Photo by un-perfekt via Pixabay https://pixabay.com/nl/photos/wapen-pistool-grijpen-gewapende-3836563/ https://www.theodysseyonline.com/funniest-crimes-reported

Sources

Slide	Source
33	Photo by Vanilla Bear Films on Unsplash https://unsplash.com/photos/IEwNQerg3Hs Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
34	Photo by fekhaf on Wallpapercave https://wallpapercave.com/w/wp6626371
35	Photo by bruce mars on Unsplash https://unsplash.com/photos/xj8qrWvuOEs Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
38	Photo by Reimund Bertrams via Pixabay https://pixabay.com/nl/illustrations/veilig-khuis-stalen-deur-913452/ Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
39	Image by juicy_fish on Freepik https://www.freepik.com/free-vector/check-cross-flat-boxes_35514460.htm Image by Bootstrap on https://seekicon.com/free-icon/question-square_1
40	Photo by Gerd Altmann via Pixabay via https://pixabay.com/nl/illustrations/cloud-computing-gegevensopslag-byte-7433389/ Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
41	Photo by Gerd Altmann via Pixabay via https://pixabay.com/nl/illustrations/veiligheid-professioneel-geheim-5199236/ Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
42	Photo by https://brabantinbeelden.nl/verhalen/klaar-over#&gid=2&pid=9 Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
44	Photo by Jos Speetjens on Unsplash https://unsplash.com/photos/b2P4_I9G_mA
47	Photo by Jason Goodman on Unsplash via https://unsplash.com/photos/Oalh2MojUuk Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
48	Photo by Chaos Soccer Gear on Unsplash via https://unsplash.com/photos/Cjfl8r_eYxY

Sources

Slide	Source
49	Photo by vacdll via Pixabay via https://pixabay.com/nl/photos/bril-notitieboekje-telefoon-muis-2947708/ Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
50	Photo by Arek Socha via Pixabay https://pixabay.com/nl/photos/deuren-keuzes-kiezen-beslissing-1767562/
51	Photo by NASA on Unsplash Photo by Colin Maynard on Unsplash https://dds-detectivesolution.com/some-important-tips-before-hiring-a-private-detective/ https://theracquet.org/wp-content/uploads/2018/04/Racial-Profilng-Pic-1.png Photo by Joseph Mucira via Pixabay Photo by Pete Linforth via Pixabay Photo by Thomas Ehrhardt via Pixabay
53-54	Photo by Gerd Altmann via Pixabay via https://pixabay.com/nl/photos/matrix-communicatie-software-pc-2953869/ Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
55	Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
56-57	Photo by Albrecht Fietz via Pixabay https://pixabay.com/nl/photos/bel-afro-megafoon-scream-symbool-2946023/ Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
58	Screenshot of sample document of Radboud University Faculty of Arts Ethics Assessment Committee https://www.radboudnet.nl/facultyofarts/research/ethics-assessment-committee-humanities/sample-documents/sample-documents/
59-60	Photo by Nadine Shaabana on Unsplash via https://unsplash.com/photos/DRzYMtae-vA Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
62	Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp

Sources

Slide	Source
63	Photo by Scott Graham on Unsplash via https://unsplash.com/photos/OQMZwNd3ThU Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
65	Photo by Gerd Altmann via Pixabay https://pixabay.com/nl/photos/dol-zijn-op-hart-tijd-3365338/
66	Photo by Luiz Jorge de Miranda Neto- Luiz Jorge Artista via Pixabay https://pixabay.com/nl/photos/druk-op-verdichting-samendrukken-1332506/
69-70	Photo by Nino Carè via Pixabay via https://pixabay.com/nl/photos/boeken-planken-deur-ingang-1655783/ Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
71	Photo by Shirley Hirst via Pixabay https://pixabay.com/nl/photos/recyclen-hergebruiken-recyclebaar-57136/ Icons by Eucalyp on Flaticon via https://www.flaticon.com/authors/eucalyp
72	Screenshot from https://data.ru.nl/doc/dua/RU-RA-DUA-1.0.html?23
75-83	Image by juicy_fish on Freepik https://www.freepik.com/free-vector/check-cross-flat-boxes_35514460.htm
84	https://www.pickpick.com/life-saving-swimming-tube-save-me-helping-hands-save-help-symbol-112917