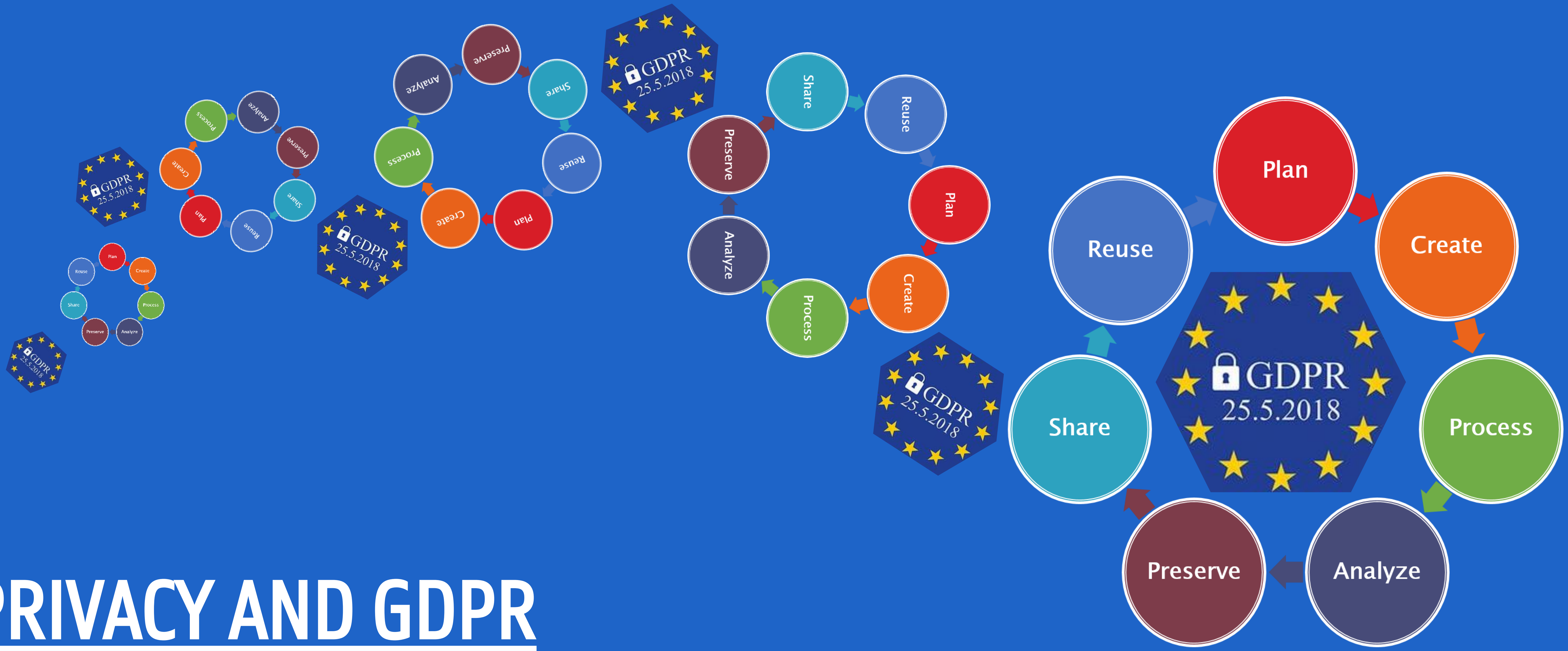


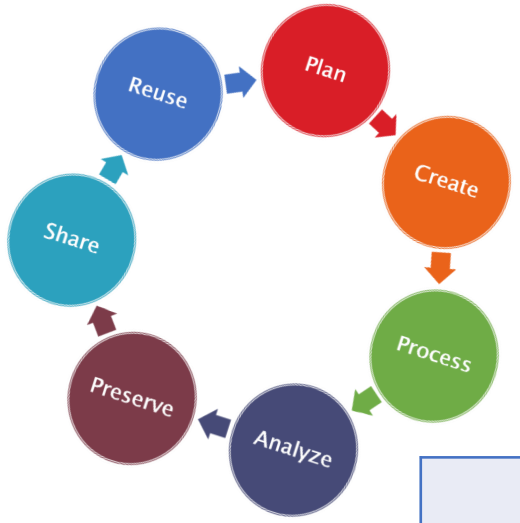
PRIVACY AND GDPR

IN THE RESEARCH LIFE CYCLE

GHENT UNIVERSITY

The information provided in this presentation is based on a **current interpretation of the GDPR,** check the research tips and website for **updates**

This presentation **should not be seen as legal advice**



CONTENT

0. The basics

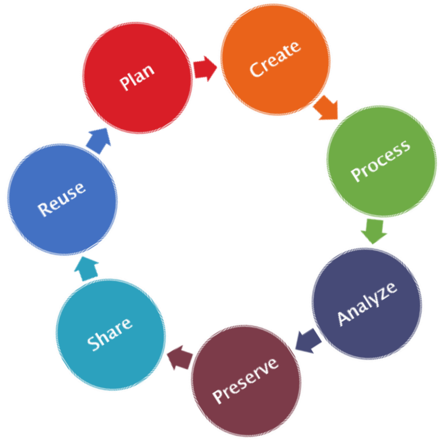
1. Planning your research from a GDPR point of view

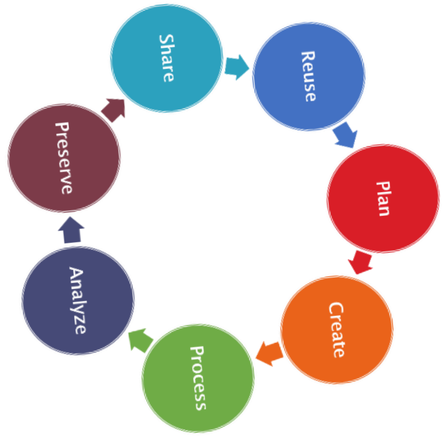
2. From planning to collecting your data

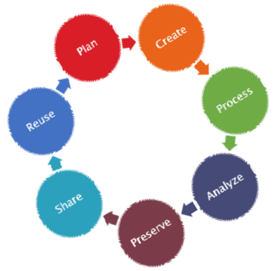
3. Structuring and analyzing your data

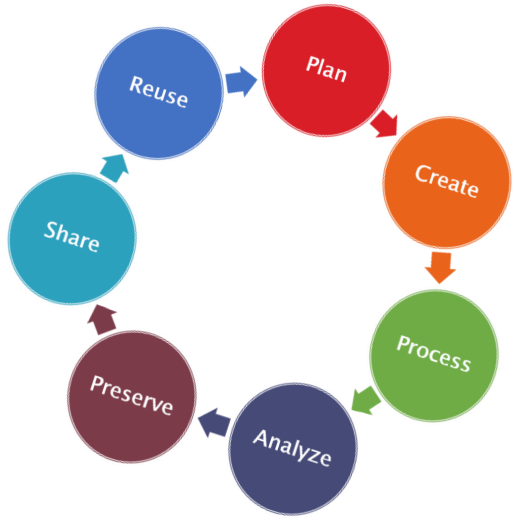
4. Sharing, publishing, archiving and destroying your data

5. Wrap up & questions









0.

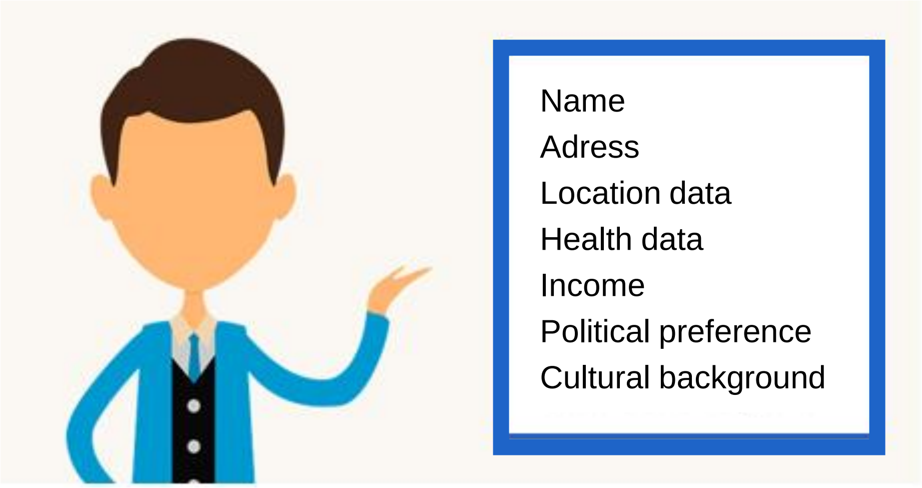
THE BASICS

WHAT ARE PERSONAL DATA? (1)

Personal data about a data subject

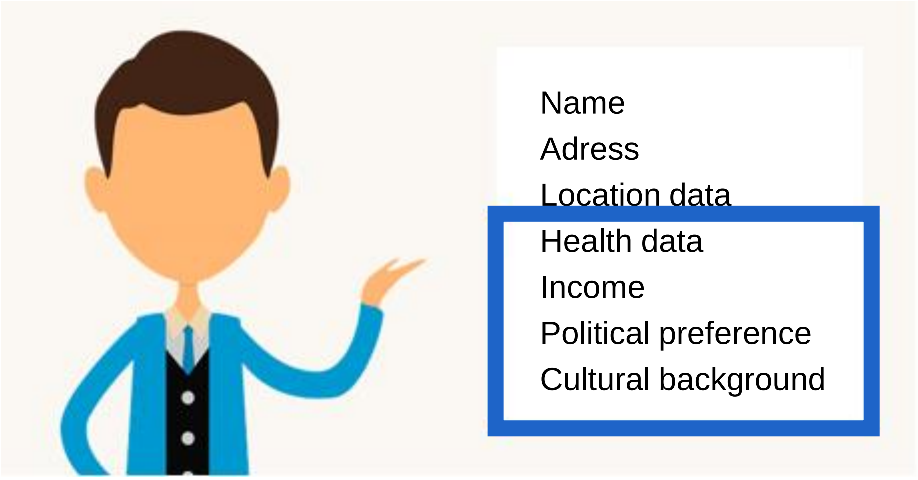
→ Data about **natural living persons** from which they can be **directly or indirectly identified** (name, identification number, location data, online identifier, factors specific to the physical, psychological, genetic, mental, economic, cultural, social,… identity of a natural person)

→ (**combinations** of) **indirect identifiers** can also lead to identification and are therefore also personal data



Special categories of personal data (sensitive data)

→ Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, **biometric data**, health data, data on sex life or sexual orientation



! Confidential data

→ All data, personal data or other that is seen as confidential in a certain context or for specific reasons, e.g. financial data of a company are not personal data, but might be confidential data

GHENT UNIVERSITY

WHAT ARE PERSONAL DATA? (2)

Pseudonymised or ‘coded’ data

⟶ Personal data (sensitive or not) that can only be **associated** with an identified or identifiable person by means of a **non-public (secret) key or additional data (lack of key)**

⟶ Data subject is are **only identifiable** with the use of **additional information/identifiers** that is kept separately

⟶ Pseudonymised data are still **personal data** (even if the identifiers are held by another organisation)

⟶ Pseudonymised data **= GDPR!**

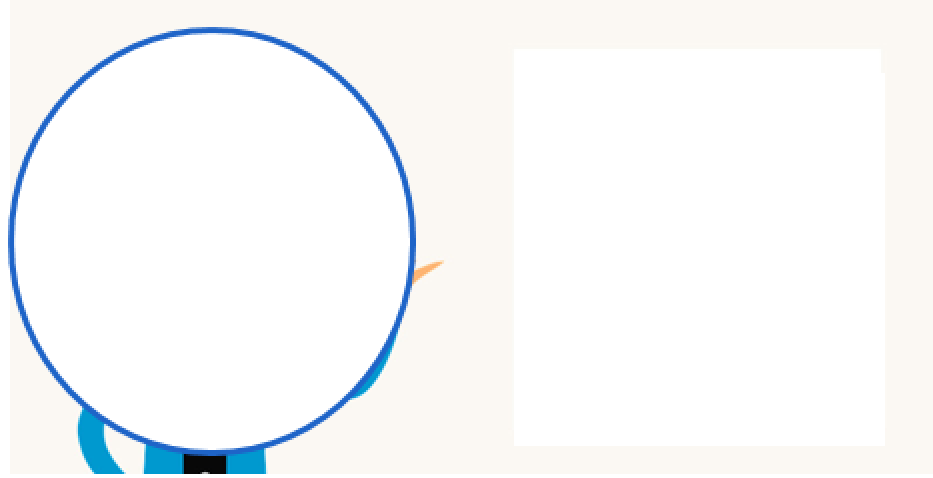
Anonymous data

⟶ Do not relate to an **identified or identifiable** natural person

⟶ Data subject is **not or no longer identifiable** (no person in any way)

⟶ Anonymised data **≠ GDPR**

⟶ The handling (**anonymisation**) **= GDPR!**



WHAT ARE PRIMARY AND SECONDARY PERSONAL DATA?

Primary data

The personal data will be collected **directly from** the data subjects within the research project

→ New dataset created by you

→ I.e. surveys, interviews, observations, …

→ (Extra) ethics issues such as recruitment, risk of stigmatization, unexpected findings, …

→ GDPR applies

Secondary data

The personal data will **NOT be collected directly from** the data subjects within the research project

→ Dataset created in a previous research (project) by the same researcher or another researcher/institution/entity and will be reused

→ I.e. the researcher is using data from a public database such as the national register

→ GDPR also applies!

Combination of primary and secondary data

GHENT UNIVERSITY

WHAT ABOUT PUBLIC AND NON PUBLIC PERSONAL DATA?

Public data or ‘open source’ data

⟶ ≠ always ‘free’ to use

⟶ GDPR might still apply

Using ‘open source’ personal data about <u>identifiable</u> persons to create new records, information or files/profiles

⟶ You are processing personal data

⟶ You must have a lawful/legitimate basis for doing so

⟶ You must ensure that the data processing is fair to the data subject and that their fundamental rights are respected

Using data from social media networks without the data subjects’ explicit consent

⟶ You must assess whether those persons actually intended to make their information public (e.g. in the light of the privacy settings or limited audience to which the data were made available)

⟶ It is not enough that the data are accessible; they must have been made public to the extent that the data subjects do not have any reasonable expectation of privacy

⟶ **privacy & expectations balance**

GHENT UNIVERSITY

WHEN DOES THE GDPR APPLY?

When you are **processing personal data** within your **research**

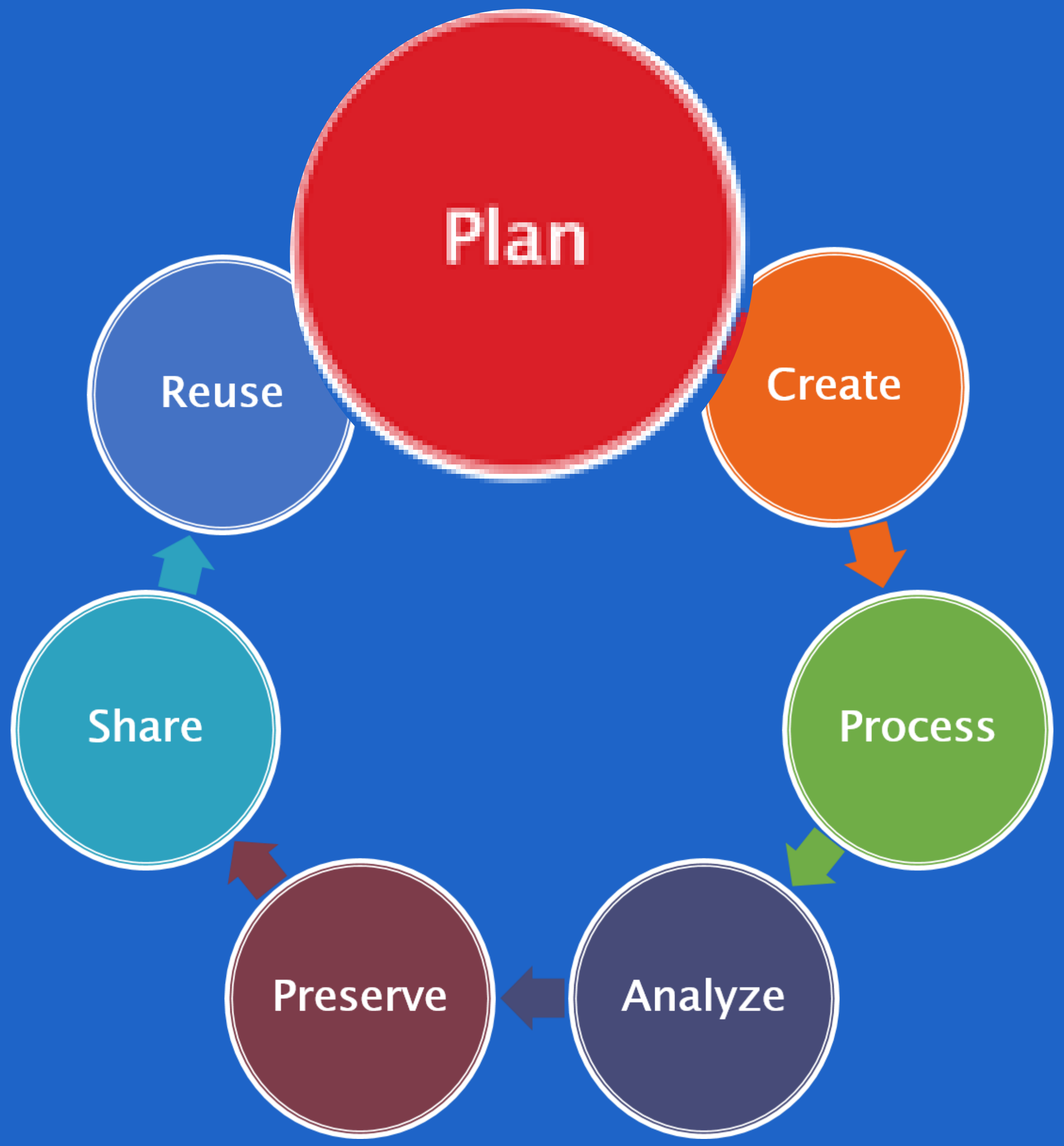
= any operation or set of operations which is performed **on personal data or on sets of personal data**, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

AND WHERE?

A researcher **based within the EU** who processes **personal data of natural persons, from any other country worldwide**

A researcher who is based **outside the EU, but processes data of natural persons in the EU**

GHENT
UNIVERSITY



1.

PLANNING YOUR RESEARCH FROM A GDPR POINT OF VIEW

IS YOUR DATA (COLLECTED) LEGITIMATE AND LAWFUL?

Legitimate, lawful data means defining a legal ground as a condition

- → One legal ground per processing/purpose
- → Must be valid before the processing personal data
- → **6 LIMITED possible legal grounds** for processing personal data (primary AND secondary)

Which possible legal grounds?

- → **Consent: the data subject(s)** has given clear consent for you to process their personal data for a specific purpose
- → **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- → Legal obligation(s): the processing is necessary for you of Ghent University to comply with the law (not including contractual obligations).
- → **Vital interests:** the processing is necessary to protect someone's life.
- → **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- → **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

WHAT ABOUT THE LEGAL GROUND FOR SECONDARY DATA?

Check compatibility (legal ground of primary data collection)

- → If **legal ground primary data collection = consent**:
  - → Did the research participants consent to use their data in a future project?
  - → Does the purpose of your research fall within the **scope** of the given consent?
- → If the **legal ground of the primary data collection ≠ consent**: reuse for scientific purposes is **compatible** with the purposes for which the personal data were initially collected
  - → No 'new' legal basis required
  - → Pseudonymisation is required as a technical and organizational measure
  - → Information obligation remains, unless exception for research can be motivated

STRUGGLING?

- → **Use** the lawful basis interactive guidance **tool** of the ICO: https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/
- → Contact your **DPO (privacy@ugent.be)**

WHO ARE YOUR COLLEAGUES, COLLABORATIONS OR PARTNERS?

Be aware that you 'work' with others in almost every study/research

Inside and outside your institution – other university/ research institution / public - private

→ **Coordination** will be needed on the technologies to be used for, among other things, the storage and analysis of the data

→ Requires **contractual agreements** about the handling of data in all phases of the research

Located in/out the EEA

→ Inside the EEA: GDPR applies

→ Outside the EEA: **adequate transfer mechanism needed!**

What are their **roles and responsibilities?**

→ **Data controller (on behalf of UGent):** the institution / organization that determines the purpose and means of the processing

→ **Joint controller (on behalf of UGent)**: the purpose and means of processing are determined by two or more organizations or institutions

→ **Separate controllers (on behalf of UGent)**: the purpose and means of the processing are determined by two or more organizations or institutions, but these are each separately responsible for processing for 1 specific processing activity

→ **Processor**: the institution, organization or researcher processes personal data on behalf of another institution or organization

→ **Sub processor**: the institution, organization or researcher processes personal data on behalf of another organization and asks another institution, organization or researcher to perform (part of) the processing on his / her behalf

DID YOU REGISTER YOUR PROCESSING ACTIVITY?

Obligation under GDPR

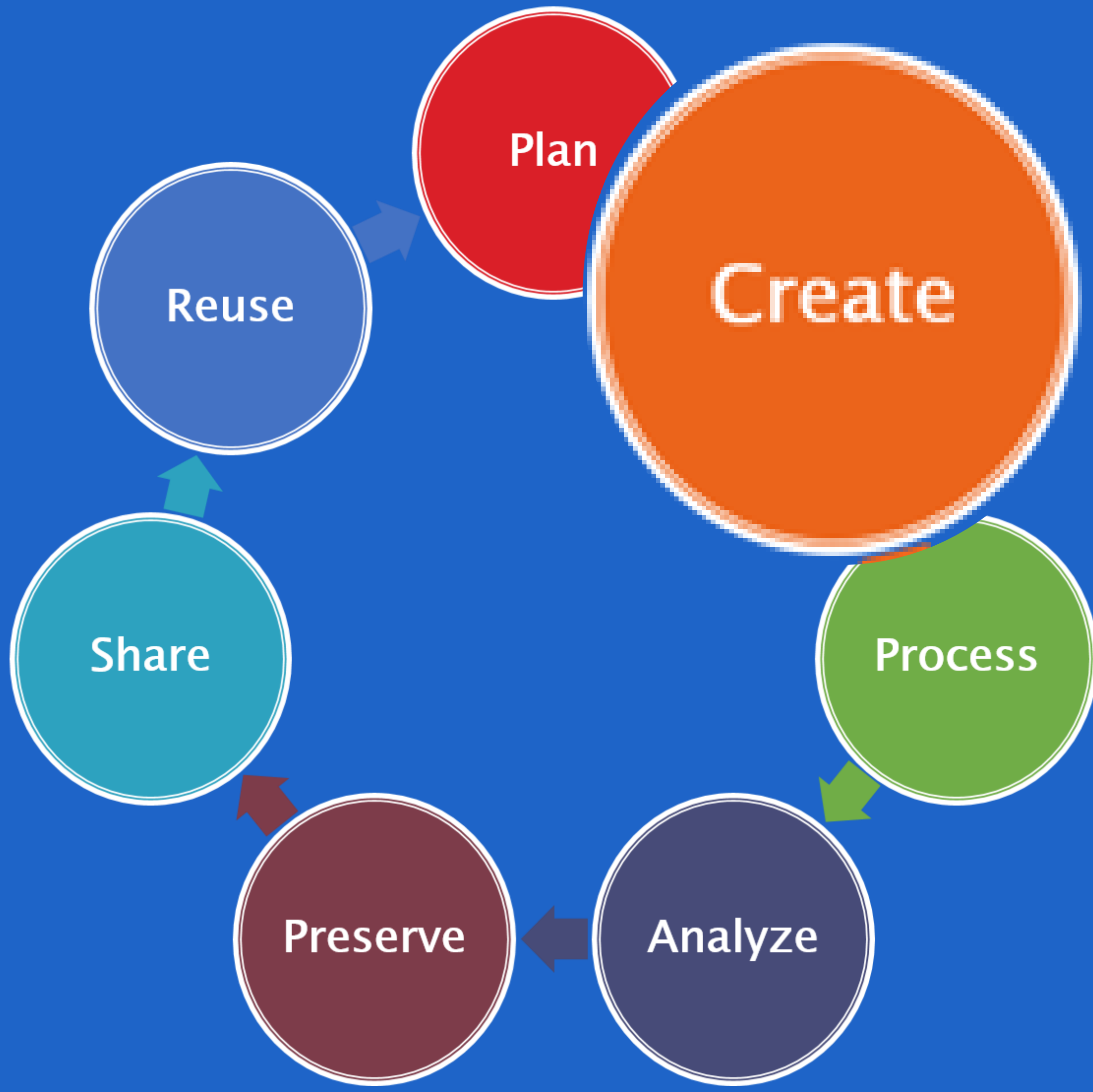
- → Principle of **accountability**
- → **@UGent:** Generic code of conduct for the processing of personal data and confidential information

GDPR register at UGent

- → GDPR record
- → Incorporated in **DMPonline.be** - Data Management Plans tool
- → Complete the **GDPR template** in your role as data controller on behalf of Ghent University or data processor
- → For more information check https://onderzoektips.ugent.be/en/tips/00001795/ or join a workshop

Also embedded in this register: a **Data Protection Impact Assessment**

- → A detailed overview of potential risks related to the data processing in your research
- → Legal obligation if research contains a probably high risk
- → Sometimes also requested by funders



2.

FROM PLANNING TO COLLECTING YOUR DATA

HAVE YOU THOUGHT ABOUT DATA MINIMIZATION?

Don't collect more personal data than you actually need…

- ⟶ Data collection must be adequate, relevant and limited to what is necessary – you do not collect more than you need for your research purpose
- ⟶ E.g. collect 'age categories' if birth dates aren't necessary

HAVE YOU THOUGHT ABOUT YOUR DATA SUBJECTS?

GDPR principle of transparency: obligation to **inform** data subjects

- ⟶ Information should be adjusted to the data subjects & research participants (i.e. children)
- ⟶ For primary & secondary data, whatever the legal ground is!

& data subjects do have rights they can exercise… they have the right:

- ⟶ To be informed about which, how, why and when their personal data is processed
- ⟶ of access to their personal data & rectification of their personal data
- ⟶ to erasure (the 'right to be forgotten')
- ⟶ to data portability of their personal data
- ⟶ to demand a restriction processing of their personal data & to object to (a part of) the processing
- ⟶ not to be subjected tot automatic decision making / profiling

GHENT
UNIVERSITY

WHAT SHOULD YOU INFORM YOUR DATA SUBJECTS ABOUT?

Mandatory information on data protection and privacy when directly collecting information

→ The identity and contact details of the **researcher** and the **DPO**, **legal basis** and **purpose** of the processing of data, period of **retention or criteria** to determine period of retention, information about their **rights** and how to **exercise** their rights, …

→ Usually in **information sheet, website, privacy policy**, …

Mandatory information on data protection and privacy when INdirectly collecting information:

→ The same as for directly collected information, BUT **EXTRA: the categories of personal data concerned, the source of the secondary data and that the data originate from a public source**

→ Usually in **information sheet, website, privacy policy**, …

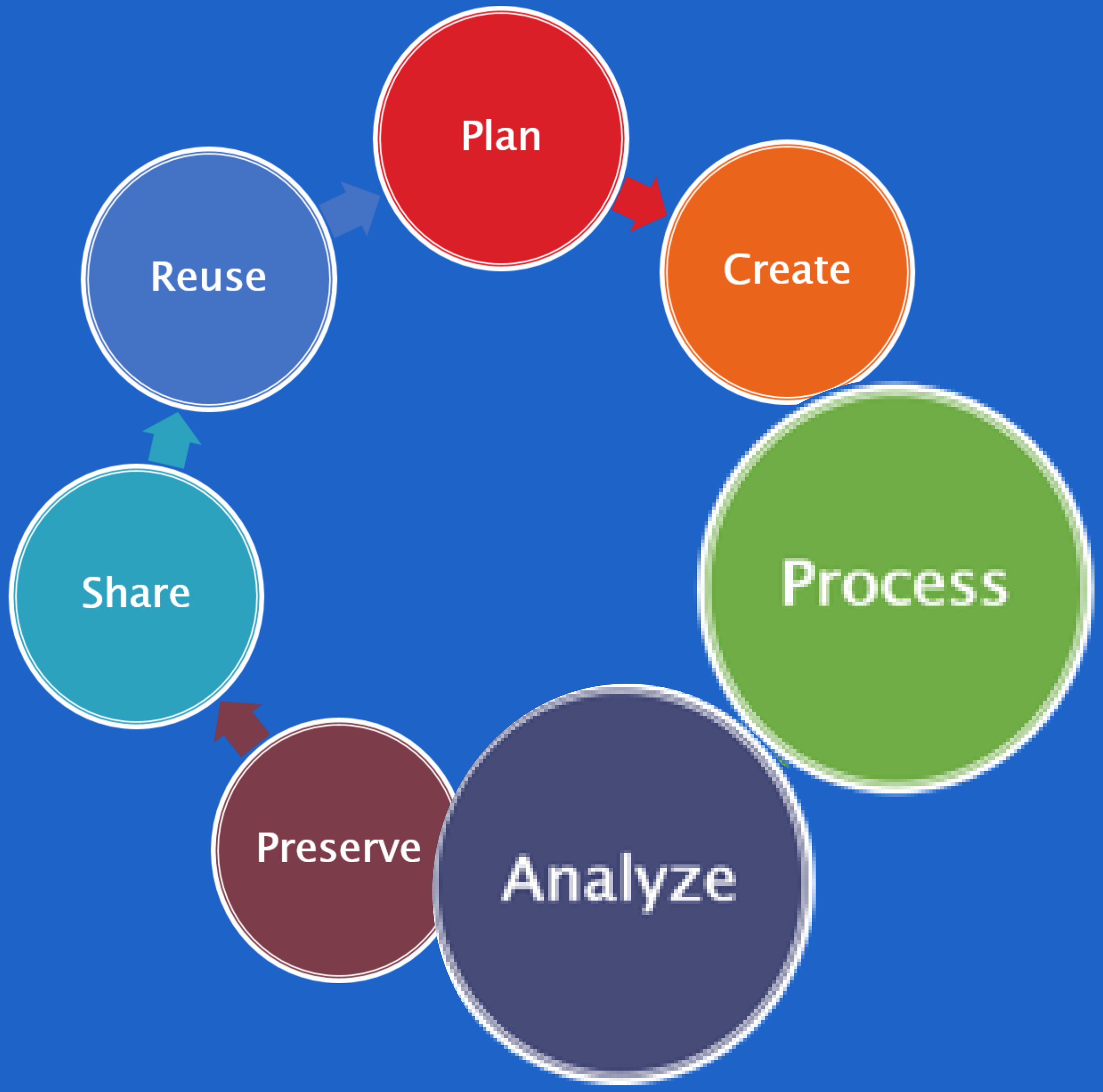
(!) Exception for research (only for the use of secondary data)

→ If providing information is **impossible** or involves a **disproportionate effort**

→ Motivate in the GDPR Register (@UGent: dmponline.be)

→ Other GDPR requirements still apply!

GHENT
UNIVERSITY



3.

STRUCTURING AND ANALYSING YOUR DATA

IS YOUR DATA SAFE AND SECURE?

Basic principle: **do no harm**

→ **Assess the possible risks for the privacy of the data subjects:** sensitivity of the data, possibility for reidentification, consequences of a data breach,...

→ Make the **right decisions and document them (GDPR record)!**

→ **Most important safety measures:** anonymisation, pseudonymisation, encryption

Think about **safe storage & access restrictions**

Be careful when data is "on the move" & during transmission of personal data

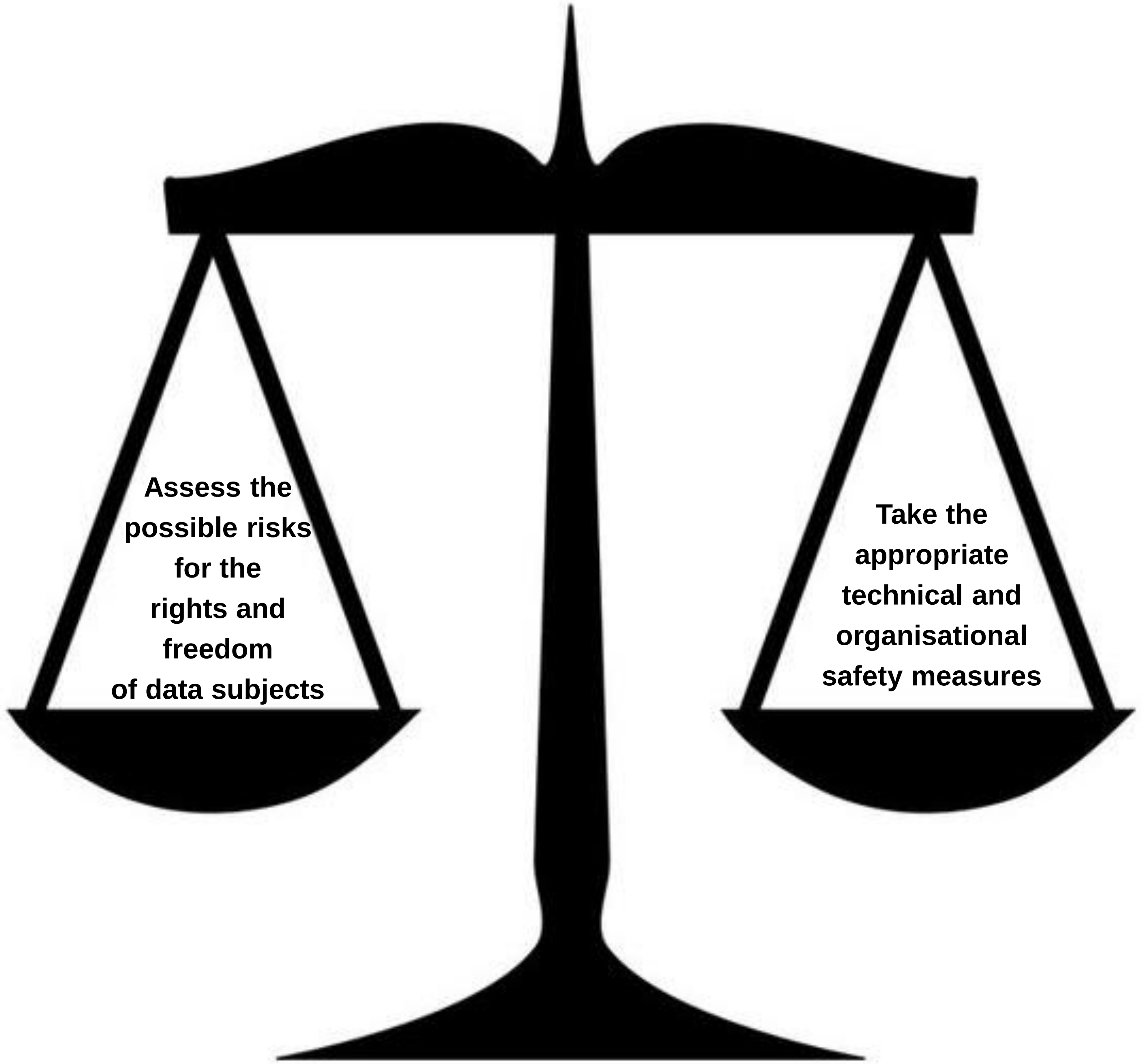
→ Encrypt files with personal data, avoid to transport raw data

Don't forget other (digital) tools

→ When recording interviews: are you using a secure device?

→ Is it encrypted? Does it automatically store in the cloud?

→ Do you have a protocol to transfer it from the device to your hardware?


Assess the possible risks for the rights and freedom of data subjects
Take the appropriate technical and organisational safety measures

THINKING ABOUT ANONYMISATION / PSEUDONYMISATION?

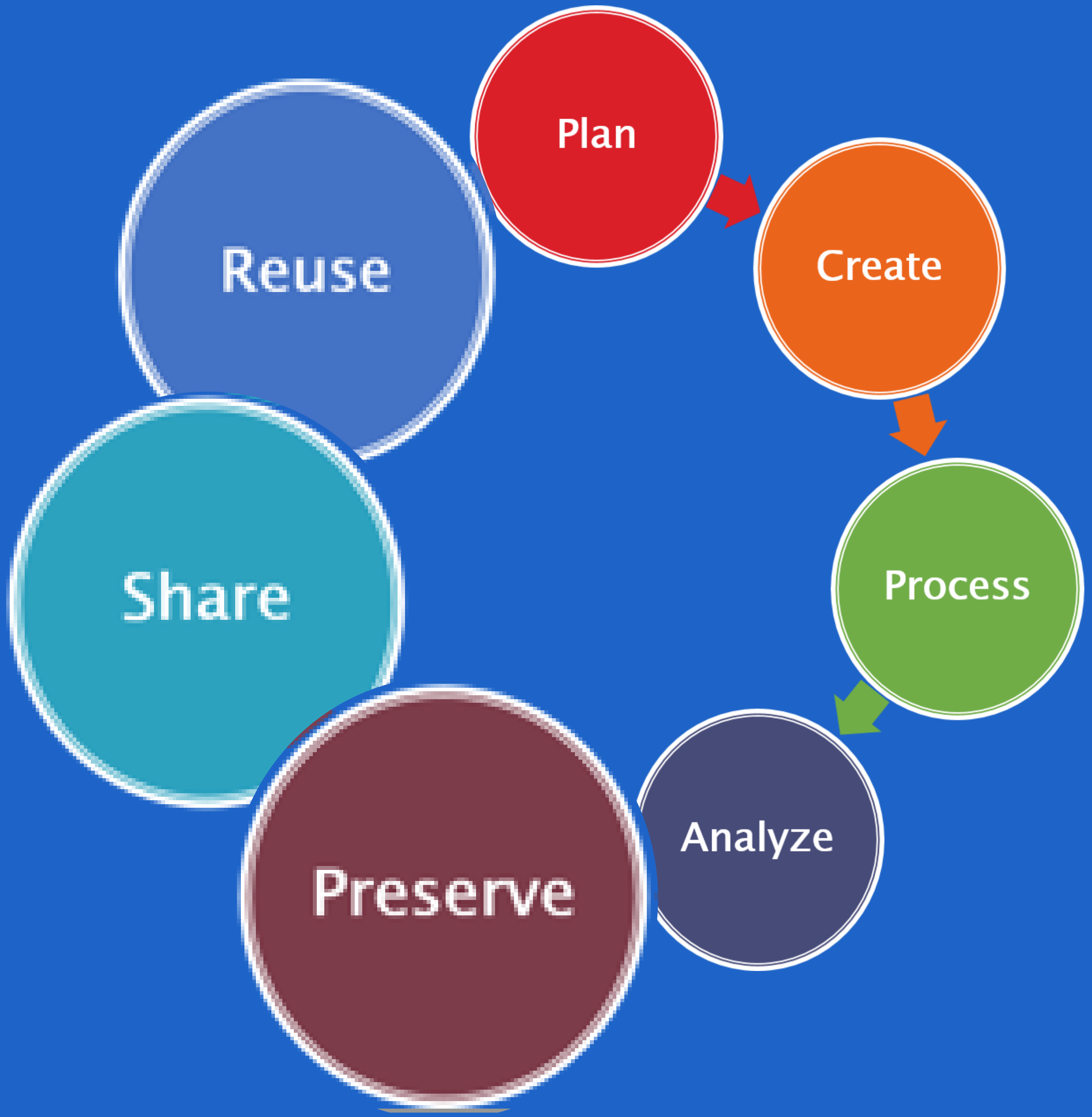
First questions:

- ⟶ Data minimization → Do you need ALL THAT personal data?
- ⟶ Can you truly anonymise?
- ⟶ What are the risks when breached?
  - Sensitivity (i.e. health data – biometric data)? Confidentiality?
  - Higher need for technical & organizational measures!
- ⟶ Information loss?
  - **Trade off**: ↑anonymity ↓utility

Information (name)	Anonymized	Pseudonymized
Peter	*****	4We8Kd
Annabelle	******	L8Fg447bA
Mark	*****	KJDe23
Elizabeth	******	Aq18zRe87
Mark	******	KJDe23
Annabelle	******	L8Fg447bA

GENERAL TIPS

- ✓ **Pseudonymize the data as quickly as possible**
- ✓ Use **different pseudonyms for different datasets**
- ✓ **Access** to the key file is controlled by someone who is not is involved in the investigation
- ✓ Take both **technical and organizational measures** to prevent unauthorized persons from linking the key file and the research data
- ✓ Restrict access to the **key file**



4.

SHARING, PUBLISHING, ARCHIVING AND DESTROYING DATA

HOW LONG CAN YOU KEEP PERSONAL DATA?

Principle of storage limitation in GDPR

→ Only as long as necessary for the data processing

But: exception for research

→ Personal data may be stored for **longer** periods

→ **IF** appropriate **technical and organizational measures** are taken to protect the rights and freedoms of the data subject

→ E.g. pseudonymization and encryption

CAN YOU REUSE IT?

Further processing/ reuse of personal data: check compatibility (lawfulness of primary collection)

→ If **legal ground primary data collection = consent:** did research participants consent to use their data in a future project? Does the purpose of your research fall within the **scope** of the given consent?

→ If **legal ground primary data collection ≠ consent**: reuse for scientific purposes is **compatible** with the purposes for which the personal data were initially collected

→ No legal basis separate from that which allowed the primary collection of the personal data required

→ Information obligation remains, unless exception for research can be motivated

GHENT UNIVERSITY

HOW DOES THIS RELATE TO SHARING YOUR DATA AFTER YOUR RESEARCH?

How to share your data (with researchers, repositories, funders, …)

→ Different access categories

→ Always requires a **balancing of interests** between the need to provide data and the protection of personal data

Central research data management principle: as open as possible as closed as necessary… BUT

→ Only possible if the subjects (research participants) have given **consent for data sharing!**

→ **Safe approach**

→ **Select a trusted repository** with sufficient safeguards for sharing personal data

What to think about when sharing your data?

→ Make **arrangements** on what happens once you no longer need to share the data

→ In some cases, it may be best to **return** the shared data to the partner that supplied it without keeping a copy i.e. governance data

→ In other cases, all of the partners involved should **agree on the retention period(s)**, its purposes and/or delete their copies of the personal data

PUBLISHING PERSONAL DATA

Publishing (personal data) in **articles, papers etc**

⟶ Best practice: research participants should not be identified in published research results unless they have explicitly consented to being identified

Data availability in policy journals

⟶ Journals often require authors to make all data necessary to replicate their study's findings publicly available

⟶ Check if **restricted/controlled access** is possible when sharing personal data

⟶ Make sure you ask for consent & include this in your information sheet (if applicable)

ARCHIVING PERSONAL DATA

⟶ Think about which data could possibly be archived at the start of the research

⟶ Not all personal data should be archived/stored

Main reasons to archive are **(re)use of data**, its **heretical value** and for **verification** reasons

⟶ Consult UGent storage recommendations on https://www.ugent.be/en/research/datamanagement/after-research/preservation.htm

DESTROYING PERSONAL DATA

Delete the personal data you no longer need

⟶ Make sure that they **cannot be recovered**

⟶ Data retained for **auditing processes or scientific integrity** purposes should be **stored securely** and further processed for those purposes only

⟶ If research data are held in the **cloud or by a third-party service provider**, you should ensure that it has securely deleted the data together with any back-ups

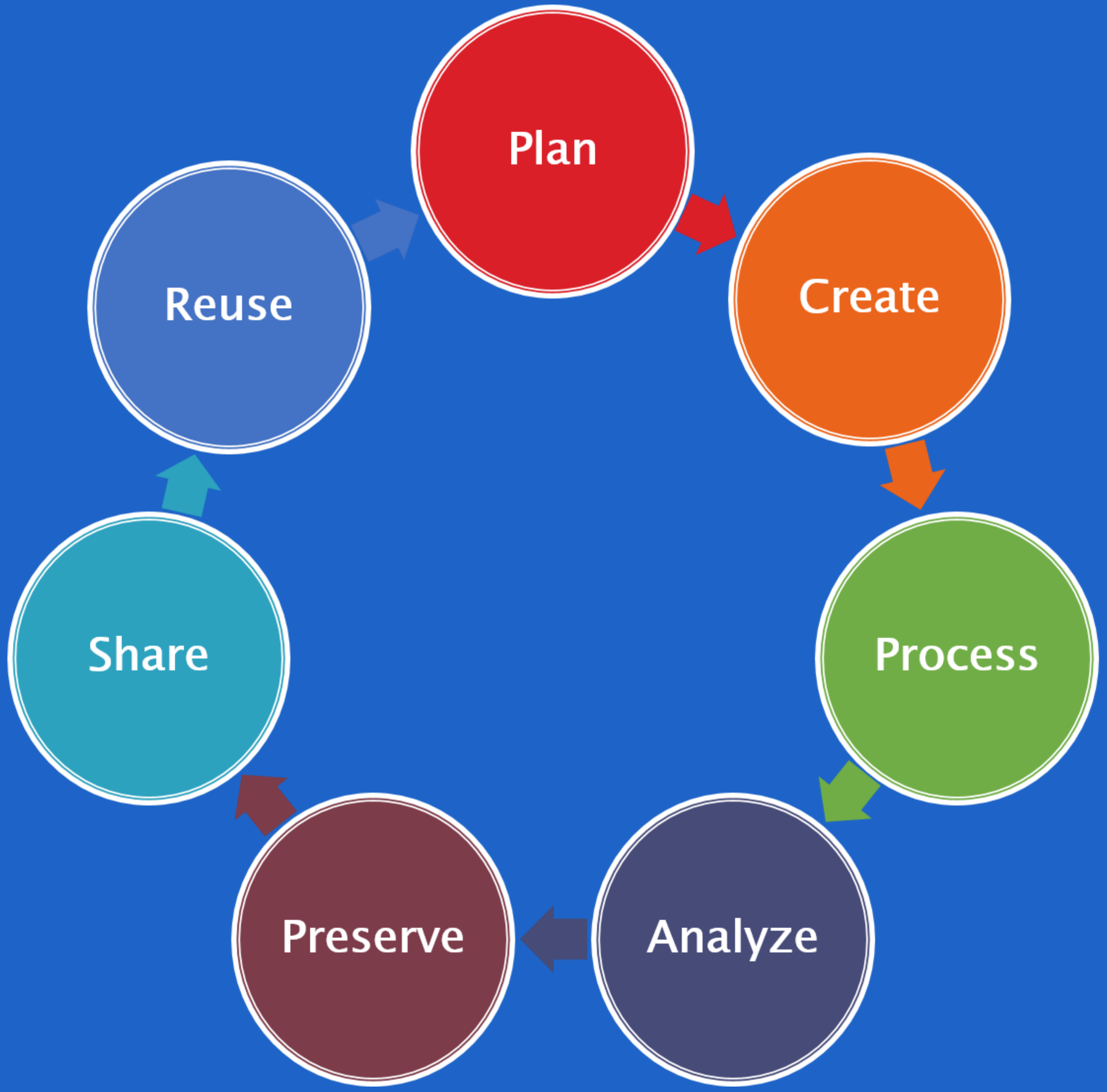
⟶ If data have been shared with **partners or transferred to third parties** in the course of your project, you should ensure that they have deleted the data, unless they have a legitimate basis for retaining them

Destroy data in a **consistent** and **reliable** way

⟶ Deleting files from hard disk -> overwrite the files or use secure erasing software

⟶ USB and CD/DVD -> physical destruction works best

⟶ Data in paper format -> shred the files or treat them as confidential waste



5.

WRAP UP & QUESTIONS

GDPR IN THE RESEARCH LIFE CYCLE

PLANNING Research proposal preparation/ drafting	DATA COLLECTION	DATA STRUCTURING AND ANALYSIS	PUBLICATION AND ARCHIVING
✓ Data ✓ Lawfulness ✓ Collaboration & partners ✓ Responsability ✓ Data transfers ✓ If necessary: processor agreements and/ or agreements for data transfer ✓ Data Protection Impact Assessment (DPIA) ✓ Research Data Management ✓ If necessary: ethical clearance	Transparancy ✓ Primairy vs. secondary data collection ✓ Data subject rights & exceptions	✓ Data protection ✓ Security measures ✓ Data breaches	✓ Retention of personal data for research ✓ Reuse of personal data ✓ Sharing personal data ✓ Publishing personal data ✓ Deleting personal data
✓ Register your processing activity (dmponline.be) in a GDPR record	✓ Update your GDPR record if necessary	✓ Update your GDPR record if necessary	✓ Update your GDPR record if necessary

IMPORTANT DOCUMENTS & LINKS

GDPR

→ https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex%3A32016R0679

Belgian law

→ http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=2018073046

UGent

→ Research tips
https://onderzoektips.ugent.be/en/tips/00001779/

→ Generic code of conduct for the processing of personal data
https://www.ugent.be/intranet/en/regulations/code_of_conduct

→ Policy framework for research data management at Ghent University
https://www.ugent.be/en/research/datamanagement

GHENT
UNIVERSITY

Questions?

Hanne Elsen

Expert gegevensbescherming en informatieveiligheid

Data Protection Officer UGent

Administrative affairs

privacy@ugent.be