Safeguarding Privacy Rights in Human Subject Research [Non-Medical], a GDPR* Approach

Right to Privacy
Human beings participating in your research project(s), *research participants,* or *data subjects*, have a right to privacy.

Research participants run potential risks*:
Physical, Psychological, Social/Economic, Privacy and Legal.

Researchers are expected to take steps, during the entire research cycle, to minimise potential risks. This infographic provides practical guidance for doing so.

Privacy Risks for Research Participants:
Loss of Confidentiality*
"In all research involving human subjects, confidentiality of identifiable information is presumed and must be maintained unless the investigator obtains the express permission of the subject to do otherwise.

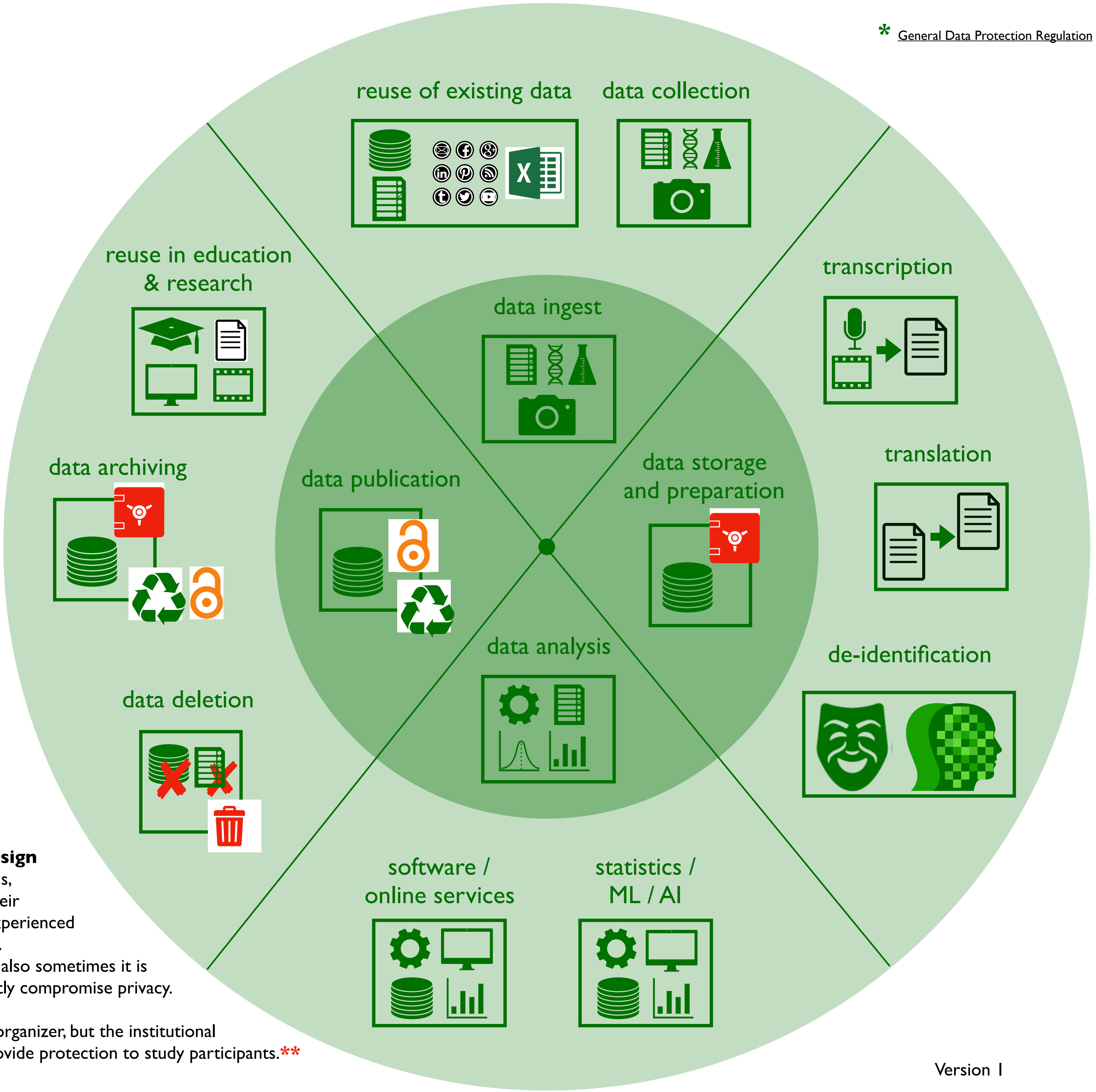
Subjects have the rights to be protected against injury or illegal invasions of their privacy and to preservation of their personal dignity. The more sensitive the research material, the greater the care that must be exercised in obtaining, handling, and storing data. In order to minimise the risk for loss of confidentiality, investigators should only collect personal information that is absolutely essential to the research activity.

If personal data must be collected, it should be coded as early in the activity as possible and securely stored so that only the investigator and authorised staff may access it. Identities of individual subjects must never be released without the express consent of the subject.

In addition, if an investigator wishes to use data for a purpose other than the one for which it was originally collected and the data are still identifiable (e.g. a code list for the data still exists), the investigator may need to obtain consent from the subjects for the new use of the data."

Privacy is best protected when secured in your Research Design
People decide to participate in research for any number of different reasons, such as a personal interest, a desire to promote research which benefits their community, or for other reasons. Many study participants, however, have experienced problems when their privacy was not upheld after participating in research.
Sometimes privacy is not kept because of insufficient study protection, but also sometimes it is because of unanticipated problems with the study design which inadvertently compromise privacy.

The privacy of research participants is typically protected by the research organizer, but the institutional review board is a designated overseer which monitors the organizer to provide protection to study participants.**



* General Data Protection Regulation

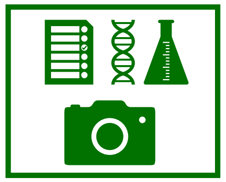
Version 1

Marlon Domingus
Erasmus University Rotterdam
marlon.domingus@eur.nl
November 2019

Credits: Social Media icon made by Sean_Hurley, https://www.needpix.com/photo/927464/
* University of Oregon, *Examples of Potential Risks to Participants*, https://rcs.uoregon.edu/content/examples-potential-risks-subjects
** Wikipedia, *Privacy for research participants*, https://en.wikipedia.org/wiki/Privacy_for_research_participants

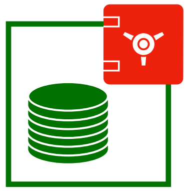
Safeguarding Privacy Rights in Human Subject Research [Non-Medical], a GDPR Approach

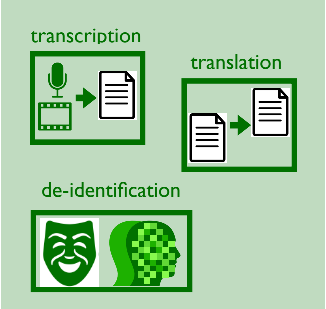
data ingest



Re-use existing data first, then decide which information requires collection
In various data repositories [i.e. DANS EASY, CBS, EU Open Data Portal, Generation R / Next, ODISSEI, Open Data Overheid, etc] and data hubs, datasets are available for research purposes. Note that re-use of existing personal data is less intrusive for research participants. Re-using data available on the internet (web scraping) can violate intellectual property rights or privacy rights (e.g. social media (exceptions exist). For advice, contact your privacy officer*.
Collecting personal data from research participants Make sure the research participants are well informed and free to participate in your research project, and under no obligation to participate. Explicit consideration should be taken with **vulnerable participants** (racial or ethnic minorities, children (different ages of consent within the EU), elderly, socioeconomically disadvantaged, underinsured or those with certain medical conditions). Consideration and documentation is required with regards to: potential negative consequences or lack of personal benefits from their involvement in research; providing appropriate information to elicit freely-given consent for participation, as well as information regarding data deposit and data re-use (where deposit is possible), for instance for education or follow on research. **Surveys** Qualtrics is the Erasmus University's GDPR compliant survey tool, but your settings and questions should also respect the GDPR privacy principles. Don't promise anonymity to research participants if you can't deliver (e.g. sending reminders or an incentive for participation). **Interviews** For audio and/or video recording purposes, don't use devices or services connected to the web, unless you can ensure that the data stored online is encrypted and the communication with the cloud is also encrypted. If you use offline devices, remove the recordings from the devices during travel and keep them secure elsewhere, so the data does not get lost when a device unfortunately gets stolen. **Research project website** Use your secure website for transparency to your research participants, as well as for public outreach; state your project's privacy statement and consent information in clear and understandable language.

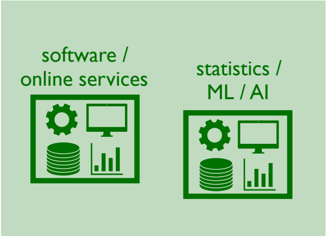
data storage and preparation





Data storage Two files are stored for each dataset: (1) a key file: provided with artificially generated identification codes and identifying information (for example names, birth dates, postal codes, contact details, etc.) on the basis of which personal data is pseudonymised and can be translated back into personal data; (2) a dataset with the artificially generated identification codes and the data points or content data from the research (for example calculated ages, questionnaire scores, etc.). These two files are stored in different protected folders. In addition, the key file itself is encrypted. The principal investigator is responsible for monitoring and keeping the decryption key of the key file secret.
Qualitative material (the original digital audio and video recordings) is stored in password-protected and encrypted folders, [i.e. EUR Document Vault, SURFdrive] using artificially generated identification codes in the document titles. The recordings can be retrieved to the other (identifying or substantive) data with the help of a decryption key, for which the principal investigator is responsible. For de-identification services (pseudonymisation & anonymisation), contact your privacy officer. **Personal data** is stored in encrypted services SURFdrive and only accessible (password protected) to research partners that have an explicit (documented) 'need to know'. Personal data are *not* sent by email, but rather: urls to data in SURFdrive are emailed to the authorised research partners. **Special categories of personal data** are stored in and shared via the EUR Document Vault and never emailed. Only use trusted and secure services and partners for **transcription** and **translations**. Certain agreements (data sharing agreement / data processing agreement / joint controller agreement) and data protection measures have to be in place with regards to your exchange of personal data; contact your privacy officer for advice.

data analysis



Agreements and AIIA Your internal review board, ethical board, and/or supervisor can advise you on methodological matters and relevant datasets for the purpose of your research project. Your privacy officer can support you by making sure that the required agreements (data sharing agreement / data processing agreement / joint controller agreement) and data protection measures are in place with your partners, service providers and software providers. Your privacy officer can also participate in an AI impact assessment with you.
FAIR This is also the phase in which the description of your work, the documentation of your decisions, and used software (and versions), in a codebook is very relevant to be released with your dataset(s) for validation purposes as well as for follow on research, by depositing your datasets in a data repository. This can only be done in case you are given explicit consent to do so by your research participants, for specified purposes. If done correctly you make your datasets 'as open as possible and as closed as necessary', and make the data *Findable, Accessible, Interoperable and Reusable*, following the FAIR principles, after your research project has ended. This may result in data citations to your research projects and further re-use of your datasets in other scientific domains.

data publication

Data publication The datasets supporting your research findings may well be re-used for research questions from other domains. To be able to facilitate this, explicit consent should be asked from your research participants. Also for your further reuse of the data for your follow on research and / or educational purposes. In the Erasmus University standard Consent Form, these topics are addressed. Contact your privacy officer in an early stage of your research design, if you have additional requirements for the data, for instance the **retention period** of your datasets, of to ensure the relevant questions are answered by the research participants. For further re-use of data for **educational purposes**, for instance video recordings of interviews or observations, specific consent is required and standard templates are available. If you agree to certain retention periods, make sure you honour them and **securely wipe** the collected raw datasets containing personal data, if there is no practical use or legitimacy to keep them any longer.

Marlon Domingus
Erasmus University Rotterdam
marlon.domingus@eur.nl
November 2019

* Who is your privacy officer? Check here: https://my.eur.nl/en/eur-employee/work-support-0/privacy-security/who-can-help-you/privacy-officers
Contact them directly or via: privacy@eur.nl What are the *GDPR privacy principles* and what is *personal data* and *special categories of personal data?* Check the Erasmus University Privacy & Security app at the Apple App Store or Google Play Store.