GHENT
UNIVERSITY

FACULTY OF ECONOMICS AND BUSINESS ADMINISTRATION

HANNE ELSEN
DATA PROTECTION OFFICER

GDPR AND RESEARCH

SSHT 1.04.2019

GHENT UNIVERSITY

DISCLAIMER

The information provided in this presentation is based on our **current interpretation of the GDPR**

Guidelines by the DPO will **follow, keep an eye on** **https://www.ugent.be/en/research/datamanagement/privacy.htm** **(work in progress)**

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

GHENT UNIVERSITY

CONTENT

GDPR

→ What is the GDPR?

→ GDPR concepts and definitions

GDPR in the research life cycle

→ Planning

→ Data collection

→ Data structuring and analysis

→ Publication and archiving

GHENT UNIVERSITY

GDPR

GHENT
UNIVERSITY

WHAT IS THE GDPR?

→ The General Data Protection Regulation
→ Came into force on May 25th 2018
→ ‘New’ EU-wide data protection regulation
→ The general principles remain the same!
→ Goal= modernising and harmonization of European data protection rules

GHENT UNIVERSITY

WHAT IS THE TERRITORIAL SCOPE OF GDPR?

Who needs to comply?

→ A data **controller** or data **processor based within the EU** who processes personal data of natural persons, from any other country worldwide

→ A data **controller** or data **processor** that is **based outside the EU** but processes **data of natural persons in the EU**

GHENT UNIVERSITY

WHY IS IT IMPORTANT TO KEEP TO THE RULES?

Compliance:

→ Sense of **responsibility**

→ **Quality and reliability** of the research and the research results

→ **Confidence of citizens and data subjects** in science

Non compliance:

→ **Reputational damage** and **negative media attention** for the researcher, the research group and for Ghent University

→ **Fines** of up to 20 million euros

→ **Indemnification or compensation** for data subjects

→ **Disciplinary measures** and **sanctions** within Ghent University (Generic code of conduct)

GHENT UNIVERSITY

WHAT ARE PERSONAL DATA?

Personal data

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

Special categories of data (sensitive data)

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

Natural living persons whose personal data are being processed = data subjects

! Always take the appropriate **safety** measures to **protect** the data!

GHENT UNIVERSITY

ANONYMOUS DATA?

Anonymous data

→ Data that does not relate to an identified or identifiable natural person or to personal data that has been made anonymous in such a way that the data subject is not or no longer identifiable (no person in any way)

→ Data subjects are **not identifiable**

→ Anonymised data **no longer** fall under the **GDPR**

→ The handling (**anonymisation**) itself falls under the **GDPR**

Pseudonymised 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**

→ Data subjects 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)

GHENT UNIVERSITY

WHAT IS DATA PROCESSING?

Very **broad** term

→ Collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction,…

Roles and **responsibilities** in **data processing**

→ **Data controller**: the institution/organization who determines the **purpose** and **means** of the processing

! Only providing the funding for research is not sufficient to be controller in the context of research

→ **Joint controllers**: the purpose and means of the processing are determined by two or more organizations or institutions

! Data processing agreement between joint controllers necessary

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

! Data processing agreement between data controller and processor necessary

GHENT UNIVERSITY

ROLES AND RESPONSIBILITIES @ UGENT

Individual researchers

→ Are processing on behalf of UGent

→ Are responsible and should be able to demonstrate compliance

→ Cfr. UGent generic code of conduct for the processing of personal data)

Data controller on behalf of UGent

Joint controller on behalf of UGent

Data processor

GHENT UNIVERSITY

WHAT ARE THE BASIC PRINCIPLES?

Lawfulness, fairness and transparency
Are the data subjects informed of what will be done with the data and is the processing of the data undertaken accordingly?

Purpose limitation
Do you use personal data only for specified and legitimate purposes in your research?

Data minimization
Do you only collect personal data that are necessary to achieve the specified goal of your research?

Accountability
Have you taken your responsibility and are you able to demonstrate compliance with the GDPR?

Accuracy
Are the personal data still correct?

Storage limitation
Do you really need the data after a certain period?

Integrity and confidentiality
Do you process personal data in a manner that ensures appropriate security?

GHENT UNIVERSITY

WHAT IS LAWFULNESS OF PROCESSING?

Defining a legal ground

→ By the data controller

→ Before the processing personal data

→ One legal ground per processing/purpose

6 legal grounds for processing personal data

1. **Consent of the data subjects**
2. Necessary for the performance of a contract
3. Legal obligations placed upon the controller
4. Necessary to protect the vital interests of the data subjects
5. **Carried out in the public interest or in the exercise of official authority**
6. Legitimate interest pursued by the controller

The lawful basis for processing personal data should be **documented** on the **information** sheet for the data subjects and in the **GDPR Register**

GHENT UNIVERSITY

WHAT ARE THE RIGHTS OF THE DATA SUBJECTS?

Data subjects have the right:

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

! Check the **legal** ground to see **which rights** can be exercised

! Inform data subjects **about their rights** and **how they can exercise them**

GHENT UNIVERSITY

EXCEPTIONS ON THE RIGHTS OF THE DATA SUBJECTS

Exception on the right to erasure (the ‘right to be forgotten’)

→ If the exercise of the right is likely to render impossible or seriously impair the achievement of the research objectives

→ Motivate in the GDPR Register

→ GDPR applies

Exception on the right of access, the right to rectification, the right to restriction of processing and the right to data portability

→ If the exercise of the right is likely to render impossible or seriously impair the achievement of the research objectives

→ Motivate in the GDPR Register

→ GDPR and **Belgian law** apply!!!

GHENT UNIVERSITY

GDPR IN RESEARCH LIFE CYCLE

GHENT UNIVERSITY

GDPR IN THE RESEARCH LIFE CYCLE

PLANNING	DATA COLLECTION	DATA STRUCTURING AND ANALYSIS	PUBLICATION AND ARCHIVING
• Collaboration & partners • Geography: cross border? • If necessary: processor agreements and/or agreements for data transfer • If necessary: ethical clearance • DPIA? • Research data management • Complete the register	• Transparancy • Primairy vs. secundary use of data • Informed consent • Update register if necessary	• Data security • Report data breaches	• Publishing personal data • Retention of personal data for research • Sharing personal data

GHENT UNIVERSITY

PLANNING

GHENT
UNIVERSITY

WHICH ASPECTS OF A RESEARCH PROJECT ARE IMPORTANT TO TAKE INTO ACCOUNT?

Collaboration & partners

→ What type of collaboration takes place in your research project (none, public-public, public-private, in/outside UGent)?

Geography

→ Which countries participate in the research and where does the storage of data take place?

Data

→ What kind of personal data do you use (existing dataset, new dataset, acquired dataset, quantitative data, qualitative data, sensitive data, ...)

GHENT UNIVERSITY

CROSS BORDER DATA TRANSFER

Within the EU and EEA (28 EU Member States + Norway, Iceland, Liechtenstein)

→ GDPR = applicable

→ Adequate data transfer mechanism under **GDPR**

→ Data processing agreement necessary

Outside EU and EEA

→ GDPR ≠ applicable

→ **Adequate data transfer mechanism necessary**

→ Data processing agreement necessary

→ DPIA?

GHENT UNIVERSITY

CROSS BORDER DATA TRANSFER

Adequate data transfer mechanism outside EU and EEA

→ '**Adequacy decision'** by EC: 'white list'

Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guersney, Israel, Isle of Man, Japan, Jersey, New Zealand, Switserland, Uruguay and the US (limited to the Privacy Shield framework).

→ Check https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

→ **Standard contractual clauses** made by **EC** (non changeable!)

→ An approved **code of conduct**

→ **Derogations for specific situations**

For research: data subjects have given explicit consent for the transfer of data after having been informed about the possible risks

Data processing agreement

GHENT UNIVERSITY

DATA PROCESSING AGREEMENTS (DPA)

Separate agreement or **annex** to data transfer agreement, consortium agreement or other type of contract

Determines roles & responsibilities, context of the processing, technical & organisational measures,…

Joint data controller:

→ Define the roles and responsibilities of the different controllers towards the data subject (e.g. informing them about the processing and about how they can exercise their rights)

Processor:

→ Choose only processors providing sufficient guarantees for safe processing

Contact contracten@ugent.be or privacy@ugent.be

GHENT UNIVERSITY

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

What?

→ Instrument to identify and assess the risks of a future processing

When necessary?

→ Mandatory if data processing poses a **potentially high privacy risk** for the data subjects

When?

→ At the start of your research

How?

1. Evaluate potential high risk in GDPR Register (www.dmponline.be)
2. French CNIL https://www.cnil.fr/en/privacy-impact-assessment-pia

! DPIA should be documented, continuously reviewed and regularly **reassessed**!

GHENT UNIVERSITY

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Criteria to evaluate a potential high risk (embedded in GDPR Register):

- ❑ **Special categories of personal data** are processed in this research
- ❑ Personal data of **children or other vulnerable persons** are processed in this research
- ❑ Personal data are processed on a **large scale** (please consider the number of data subjects concerned, either as a specific number or as a proportion of the relevant population)
- ❑ Aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements are evaluated or scored, profiled or predicted
- ❑ The data are **transferred beyond the borders of the EU or the EEA**, or to a country not listed on the 'white list'
- ❑ The research involves datasets that have been or will be **matched** or combined
- ❑ The processing aims at taking decisions producing legal effects concerning the data subject or similarly significant effects for the data subject. For example, the processing may lead to exclusion of or discrimination against individuals
- ❑ The processing prevents data subjects from exercising a right or using a service or a contract
- ❑ The research involves the systematic monitoring of persons in one or more publicly accessible areas
- ❑ The research involves innovative use or application of technological or organisational solutions, like combining the use of finger print and face recognition for improved physical access control
- ❑ The research involves the processing of **non-pseudonymised** personal data

! A data processing meeting **two or more criteria** requires a **DPIA !**

GHENT UNIVERSITY

RESEARCH DATA MANAGEMENT

Personal data → research data

RDM policy UGent

Create a DMP before the start of your research

→ Take the basic principles into account (e.g. data minimisation, use pseudonymised/ anonymised data,…)

→ Be sure to **assign responsibilities** (who is authorised & for what)

→ **Define the legal ground** for processing personal data

→ **Document the processing** of personal data in the GDPR Register @ UGent: part of DMP

Privacy by design

GHENT UNIVERSITY

GDPR REGISTER OF PROCESSING ACTIVITIES

Obligation under GDPR

→ Processing of personal data

→ Principle of **accountability**

For research at UGent

→ Incorporated in **DMPonline.be** - Data Management Plans

→ Complete the **GDPR template** in your role as data controller or data processor

→ **Update** the GDPR template if necessary

Information sessions

→ More information very soon…

GHENT UNIVERSITY

DATA COLLECTION

GHENT
UNIVERSITY

TRANSPARANCY

Principle of transparency

→ Obligation to inform data subjects

→ Data subjects should be informed in a concise, **transparent**, intelligible and **easily** accessible form, using **clear** and plain language

Mandatory information for data subjects under GDPR

→ The identity and contact details of the **researcher** and the **DPO** (privacy@UGent.be)

→ The **legal basis** and **purpose** of the processing of data

→ The (categories of) **recipients** of the data

→ If applicable: the fact that the data will be **transferred** to a third country or international organisation

→ The period of **retention**

→ Information about their **rights** and how to **exercise** their rights

→ A reminder that they have the right to lodge a complaint with the supervisory authority

→ The existence of automated decision-making, including profiling

GHENT UNIVERSITY

TRANSPARANCY

Information for data subjects (ethical reasons)

→ The **purpose** of the research
→ What is **involved** in participating in the research
→ Describe the **benefits** and **risks** of participating in the research
→ Indicate steps that will be taken to **safeguard** their anonymity and confidentiality
→ Details of the **research**, e.g. the funding source, institution, name of the project,…
→ Explain that taking part in the study is entirely **voluntary** and that refusal to agree to participate will involve no penalty or loss of benefits
→ Discuss what will happen to their **contribution** (including the future archiving and sharing of their data)

For primary and secondary use of data

Integrated in information form

In line with informed consent form (if applicable)

GHENT
UNIVERSITY

REUSING DATA

Further processing of data

→ Check the **informed consent forms**: 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?

Extra information to be provided to the data subjects

→ The categories of personal data concerned

→ From which source the personal data originate

! Exception on obligation to inform data subjects for research

→ If providing information is impossible of involves a disproportionate effort

→ Motivate in the GDPR Register

→ GDPR applies

GHENT UNIVERSITY

INFORMED CONSENT AS LEGAL GROUND

Informed consent needs to

→ be unambiguous
→ be specific
→ be freely given, by a clear affirmative action
→ Consider specific circumstances and needs of the data subjects (using pictures, translation,…)
→ be documented (written or oral statement)
→ be obtained for each separate processing activity
→ address the possibility of sharing data, future data publication (including storage in a repository) or long-term retention of data for reproducibility
→ outline their right to withdraw their consent, and how to do this

! Consent as **legal basis** for processing personal data vs. **ethical consent** as an extra safeguard

GHENT UNIVERSITY

INFORMED CONSENT AS LEGAL GROUND

Informed consent from children under the age of 18

→ Obtain consent from the person who holds the parental responsibility over the child

Broad consent

→ Data subjects should be able to give their consent to certain areas of research

→ Not to wide, not to narrow

GHENT UNIVERSITY

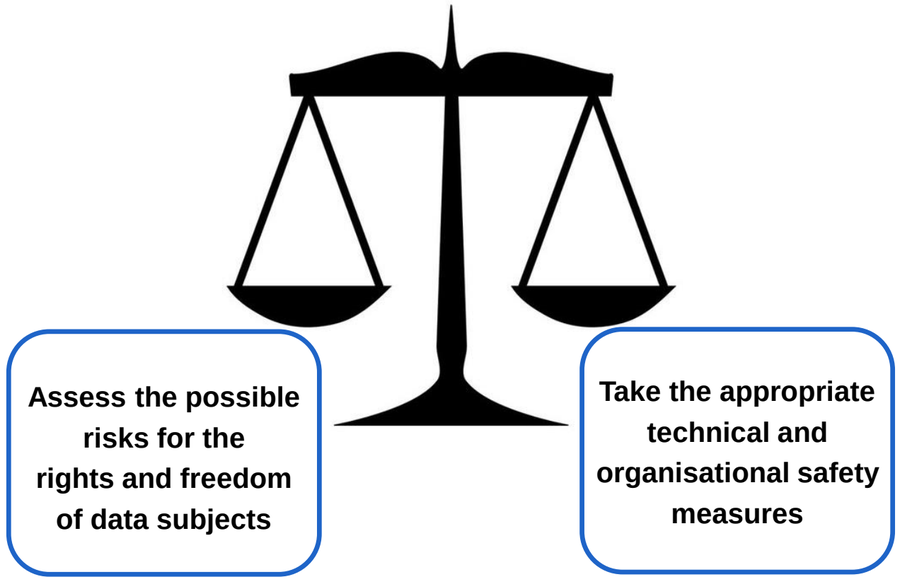
DATA STRUCTURING AND ANALYSIS

GHENT UNIVERSITY

DATA SECURITY

Data security

→ Basic principle of the GDPR!
→ Do no harm
→ Risk based approach



Tips for safely working with IT

→ Work on a trusted network
→ Use a **trustworthy device** (desktop, laptop, notebook, tablet, smartphone,…) which is sufficiently secured
→ Protect your **Ghent University account** and the associated login data
→ Be fully aware of **common risks and hazards** (do not open files that you not trust completely, avoid questionable websites,…)
→ Preferably work with the applications offered on **Athena.UGent.be**
→ Install as few additional applications as possible on your devices
→ https://www.ugent.be/en/facilities/ict/information-security

GHENT UNIVERSITY

DATA SECURITY

Store your personal data on a safe place

→ **Use the central disk space/storage** (personal disk space and shares) offered by DICT instead of storing files locally on your own IT resources (hard disk of desktop or laptop, USB stick, external hard disk,…). The files will also be back-uped automatically and will be protected by the UGent security systems

→ **Do not use external cloud services** to store personal data or confidential information unless you encrypt this data

→ **Regularly back-up data** which is not stored on the UGent shares

→ **Personal data in paper format** (e.g. consent forms signed by research participants) should be kept in a secure area of a locked filing cabinet

Pseudonymise personal data as soon as possible and keep the file with the personal information in a secure place

→ **Access** to the raw data should be restricted

GHENT UNIVERSITY

DATA SECURITY

Arrange access conditions in a consortium agreement, non-disclosure agreements, processor agreements,…

Be careful when data is “on the move”

→ Laptops and storage devices such as USB-sticks, CD’s, DVD’s, portable hard drives are particularly vulnerable for theft or accidental loss

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

Be careful during transmission of personal data

→ Files containing personal data should be encrypted and the encryption keys should be sent separately from the data

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

GHENT UNIVERSITY

DATA BREACH

Data breach

→ A security incident that has affected the **confidentiality**, **integrity** or **availability** of personal data that results in a risk to the rights and freedoms of the data subjects

Inform the DICT Helpdesk as soon as possible helpdesk@ugent.be

Data Protection Officer should notify a data breach to the supervisory authority **within 72 hours**

→ Act fast!

Breach don’t kill my vibe

GHENT UNIVERSITY

PUBLICATION AND ARCHIVING

GHENT UNIVERSITY

PUBLISHING PERSONAL DATA

Research participants should not be identified in published research results unless they have consented to being identified, or the information is already in the public domain

Check **publisher & funder** requirements

Providing research participants with a copy of the final research results or research publications will support openness and transparency

GHENT UNIVERSITY

RETENTION OF PERSONAL DATA FOR RESEARCH

Principle of storage limitation in GDPR

→ Only as long as **necessary** for the data processing

RDM policy Ghent University

→ Data must be kept for up to **five years** after the end of the project (unless contract/law determines otherwise)

→ Storage ≠ reuse

Take the appropriate **security** measures!

GHENT UNIVERSITY

DATA SHARING

Required by some funders and journals

→ Different access categories

→ Open access: data can be used by any user

→ Restricted access: access is limited and can only be granted upon request, data can be shared with a user agreement/license

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**

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

→ **Pseudonymise** personal data as soon as possible

GHENT UNIVERSITY

GDPR IN THE RESEARCH LIFE CYCLE

PLANNING	DATA COLLECTION	DATA STRUCTURING AND ANALYSIS	PUBLICATION AND ARCHIVING
• Collaboration & partners • Geography: cross border? • If necessary: processor agreements and/or agreements for data transfer • If necessary: ethical clearance • DPIA? • Research data management • Complete the register	• Transparancy • Primairy vs. secundary use of data • Informed consent • Update register if necessary	• Data security • Report data breaches	• Publishing personal data • Retention of personal data for research • Sharing personal data

GHENT UNIVERSITY

IMPORTANT DOCUMENTS

GDPR

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

Belgian law

UGent

→ 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

HELP?

Privacy@UGent.be

For general questions, questions about processor agreements, transfer to third contries,…

GHENT UNIVERSITY

QUESTIONS?

GHENT
UNIVERSITY

FACULTY OF ECONOMICS AND BUSINESS ADMINISTRATION

Hanne Elsen

Data Protection Officer

E privacy@ugent.be

T +32 9 264 95 17

www.ugent.be

Ghent University

@ugent

Ghent University

GHENT UNIVERSITY