POPD – Requirement No. 2

Deliverable D10.2

28 November 2019

Wim Verbeke[1], Lina De Smet[1], Marten Schoonman[2],
James H. Williams[3], Dirk C. de Graaf[1]

1 UGENT, 2 BEEP, 3 AU

B-GOOD

Giving Beekeeping Guidance by cOmputatiOnal-assisted Decision making

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 817622.

Prepared under contract from the European Commission

Grant agreement No. 817622
EU Horizon 2020 Research and Innovation action

Project acronym:	**B-GOOD**
Project full title:	**Giving beekeeping guidance by computational-assisted decision making**
Start of the project:	June 2019
Duration:	48 months
Project coordinator:	Prof. Dirk de Graaf Ghent University www.b-good-project.eu

Deliverable title:	POPD – Requirement No. 2
Deliverable n°:	D10.2
Nature of the deliverable:	Ethics
Dissemination level:	Confidential

WP responsible:	WP10
Lead beneficiary:	UGENT

Citation: Verbeke, W., De Smet, L., Schoonman, M., Williams, J.H.& de Graaf, D.C. (2019). *POPD – Requirement No. 2*. Deliverable D10.2 EU Horizon 2020 B-GOOD, Grant agreement No. 817622.

Due date of deliverable:	Month n°6
Actual submission date:	Month n°6

Deliverable status:

Version	Status	Date	Author(s)
0.1	Draft	26 November 2019	Verbeke, De Smet, Schoonman, Williams, de Graaf UGENT, BEEP, AU
0.2	Review	27 November 2019	Elsen (DPO) UGENT
1.0	Final	28 November 2019	Verbeke, De Smet, Schoonman, Williams, de Graaf UGENT, BEEP, AU

Table of contents

Preface

This deliverable is one out of five related to ethics requirements. It addresses ethics issues with respect to the **protection of personal data** within B-GOOD.

Summary

This deliverable provides further information about the protection of personal data within B-GOOD. Personal data will be collected from human participants by means of personal interviews, surveys, group discussions and participatory workshops within WP4 and WP8. The deliverable addresses the requirement related to Data Protection Officers (DPO) or Data Protection Policies of the involved partners. It includes a description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants, a description of the security measures that will be implemented to prevent unauthorised access to personal data, and a description of the anonymisation/pseudonymisation techniques that will be used. Further details and confirmations with respect to the transfer of personal data between EU and non-EU countries and the use of secondary data are provided.

1. Assessment of ethics issues

One of the key objectives of B-GOOD is to map the business environment and to study the socio-economics of beekeeping. As a result, personal data will be collected from human participants involved in socio-economic research. The socio-economic studies and related data collection are covered in WP4 and WP8 of the project.

The proposed studies and chosen multi-actor approach require the involvement of human participants and the collection of primary personal data from actors directly involved in beekeeping. They participate as individuals in their role as stakeholders and beekeepers and as adult healthy volunteers involved in social sciences research.

As personal data will be collected from human participants (data subjects), ethics issues related to the protection of personal data are raised and addressed.

2. General commitments with respect to data collection and protection

B-GOOD will only collect personal data from the human participants enrolled in the socio-economic studies within WP4 and WP8 that are strictly necessary to achieve the objectives of the research. These objectives concern the performance of social science studies and the implementation of socio-economic statistical analyses such as production and economic efficiency analyses.

The collected personal data will include, depending on the target population: socio-demographic characteristics such as age (years), gender, education, training (necessary for the profiling of aggregated segments) and urban-rural living environment (necessary for linking with environmental and ecological characteristics), as well as attitudinal (attitudes, beliefs, perceptions, opinions and views) and behavioural (management decisions, decision-making processes) characteristics, which will all exclusively relate to beekeeping and its context. All collected socio-economic data are cross-sectional data collected at one point in time.

Sensitive personal information relating e.g. to health, ethnicity, sexual lifestyle, political opinion, religious or philosophical conviction falls beyond the scope of B-GOOD and will not be probed for.

No confidential data, such as information on private businesses, sensitive business practices, finances or income will be collected from stakeholders. In the case of beekeepers, and in line with the objective of performing production and economic efficiency analyses in task 4.2, data relating to business, costs and revenues will be collected. In case these data are seen as and indicated to be confidential by the beekeeper but nevertheless voluntarily provided, they will be strictly treated as data given in confidence or data agreed to be kept confidential between the researchers and the beekeeper. These data will be kept secret and out of the public domain. Any reporting based on these data will be done in aggregated and non-identifiable form only. This will be explained to the beekeepers as part of the informed consent.

The informed consent procedures will also inform all data subjects of the purpose of the data collection, of what will be done with the data and of the processing of the data undertaken accordingly.

Personal interviews and workshops will be audio-taped for the purpose of verbal transcription, which is necessary for later qualitative analysis using NVivo. Transcription will be done within maximum one month following the interview or workshop. As audio-records are considered sensitive personal data because of their biometric nature, these records will be destroyed immediately after transcription. Signed (written or electronic) informed consent forms will be retained for a period of 10 years, which is the recommended retention period for scientific integrity reasons, as proof of completion of the interviews.

All data will be pseudonymised, stored in a de-identified format, kept securely and shared for study purposes and in dissemination activities only in pseudonymised or aggregated form. Transcriptions of interviews and workshops, as well as data records from surveys, will not include the name(s) of the interviewees. Instead, unique personal identifiers will be attributed to participants and used in the transcripts or with the quantitative data records. Personal identifiers and transcripts will be stored and secured separately. These will be retained for a period of 10 years scientific integrity reasons. Access to the personal identifiers will be strictly limited to the principal investigator of the consortium partner who performed the interview.

Detailed information about the planned data collection methods and types of data within WP4 and WP8 is provided in Appendix 1.

3. Data Protection Officers / Data Protection Policies

Requirement: The beneficiary must confirm that it has appointed a Data Protection Officer (DPO) and the contact details of the DPO are made available to all data subjects involved in the research. For beneficiaries not required to appoint a DPO under the General Data Protection Regulation (GDPR) a detailed data protection policy for the project must be kept on file (to be specified in the grant agreement) and submitted to the Agency upon request. The confirmation for each beneficiary must be submitted as a deliverable.

Each of the partners involved in the B-GOOD research activities within WP4 and WP8 and who have access to personal data, either through its collection, processing or storage, have either appointed a Data Protection Officer (DPO) or they have adopted a data protection policy for the project.

Informed consent forms will refer to the principal investigator and the DPO of the B-GOOD partner that performs the data collection or interview.

The confirmation of the concerned partners (UGENT, AU, UCOI and WR) are enclosed in Appendix 2. In case additional B-GOOD partners become involved in the collection, processing or storage of personal data during later stages of the B-GOOD project, their data protection policies for the project and/or their confirmations (similar to the ones provided in Appendix 2) will be collected prior to the start of these activities, and kept on file.

4. Technical and organisational measures to safeguard the rights and freedoms of study participants

Requirement: A description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants must be submitted as a deliverable.

The principle of transparency will be adhered to during all collection of personal data within B-GOOD. This implies that data subjects/research participants will be properly informed and asked to provide informed consent. This will be done in a concise, transparent, intelligible and easily accessible format using clear and plain language, and using study-specific informed consent forms. Data subjects will be informed about the purpose of the research, what is expected from them, eventual benefits and risks involved, and steps taken to safeguard their anonymity and confidentiality. They will be informed that their participation is voluntary and that refusal to participate will involve no penalty or loss of benefits. They will also be informed about the plans with their contribution in terms of analysis, reporting, future archiving and sharing of their data.

The identity and contact details of the principal researcher and the Data Protection Officer (DPO) of the institution responsible for the data collection will be communicated to the data subjects. Information about the rights of the data subjects and how they can exercise these will be provided, including the right to revise their personal data, request their data to be removed, and to lodge a complaint with the supervisory authority.

Adequate security measures will be implemented to prevent unauthorised access to personal data or the equipment used for processing as described in section 5.

All personal data will be pseudonymised as described in section 6.

As a general guideline, the generic code of conduct for the processing of personal data within UGENT, the institution of the B-GOOD coordinator and the B-GOOD WP4-leader, will be shared with the consortium partners and recommended to be adhered to. This code of conduct is enclosed as Appendix 3.

In a similar vein, the policy framework for research data management (RDM) at UGENT, the institution of the B-GOOD project coordinator, will be shared with the consortium partners and recommended to be adhered to. This policy framework is available at: https://www.ugent.be/en/research/datamanagement

5. Security measures to prevent unauthorised access to data or equipment

Requirement: A description of the security measures that will be implemented to prevent unauthorised access to personal data or the equipment used for processing must be submitted as a deliverable.

B-GOOD research activities involving human participants and personal data have been designed following a risk-based approach. Taking into account appropriate technical and organisational measures to safeguard the rights and freedoms of the study participants (as described in Section 4) and to protect the data, the activities have been defined as low-risk.

Based on general principles within UGENT that will be shared with all other B-GOOD partners, all researchers involved in B-GOOD are asked to commit to work on trusted networks, to use trustworthy devices, and to protect their institutional accounts and associated login data in line with their institutional guidelines and data protection policies.

Data will be stored on safe places only, i.e. on password-protected central disk spaces/storage (such as personal disk space and shares at institutional level), which are backed-up automatically and protected by institutional security systems.

The use of external cloud services to store personal data or confidential information will be avoided, unless this data or information is encrypted. Personal data in paper or any other physical form (e.g. non-digital audio- or video-recordings) will be kept in a secured area of a locked filing cabinet.

Access to personal data will be strictly limited to the researchers who are directly involved in the analysis of the concerned data. The principal researcher will ensure this data is password-protected and communicate passwords in person or in encrypted format (not in written). Passwords will be changed at regular intervals. Access conditions will be arranged and agreed upon during project meetings and decisions included in the minutes of the meeting. In case of encrypted data, files containing the encrypted data and the encryption keys will be kept and/or sent separately from the data.

B-GOOD will make use of the encryption functionalities of SPSS (in case of survey data collected from stakeholders and beekeepers, which will also be analysed using SPSS) and of Microsoft Office (in case of the interview and workshop transcripts as text files). In case the specific analysis software used does not provide encryption possibilities, 7-zip compression software will be used where needed.

6. Anonymisation/pseudonymisation techniques

Requirement: Description of the anonymization/pseudonymisation techniques that will be implemented must be submitted as a deliverable.

All data will be pseudonymised, stored in a de-identified format, kept securely and shared for study purposes and in dissemination activities only in pseudonymised or aggregated form. Transcriptions of interviews and workshops, as well as data records from surveys, will not include the name(s) of the interviewees. Instead, unique personal identifiers will be attributed to participants and used in the transcripts or with the quantitative data records. Personal identifiers and transcripts will be stored and secured separately.

7. Transfer of personal data between EU and Non-EU countries

Requirement: In case personal data are transferred from the EU to a non-EU country or international organisation, confirmation that such transfers are in accordance with Chapter V of the General Data Protection Regulation 2016/679 must be submitted as a deliverable.

There will be no transfer of personal data from the EU to a non-EU country within B-GOOD.

Requirement: In case personal data are transferred from a non-EU country to the EU (or another third state), confirmation that such transfers comply with the laws of the country in which the data was collected must be submitted as a deliverable.

Personal data from stakeholders and beekeepers as described above and in Appendix 1 will be exchanged between the EU and Switzerland (UBERN). No personal data within B-GOOD will be exchanged with any other non-EU country than Switzerland. On the basis of article 45 of Regulation (EU) 2016/679, the European Commission has adopted an Adequacy Decision recognising Switzerland as providing adequate protection. A copy of the Directives on Data Protection in the IT Domain at the University of Bern is provided in Appendix 4.

8. Secondary data

Requirement: An explicit confirmation that the data used in the project is publicly available and can be freely used for the purposes of the project must be submitted as a deliverable.

B-GOOD will make use of the secondary data sets such as weather service data, LoRa message data, national georeference data, FADN data, and statistical information on the general characteristics of the beekeeping sector. From these, only the FADN data may eventually contain personal data.

The **F**arm **A**ccountancy **D**ata **N**etwork (FADN) (https://ec.europa.eu/agriculture/rica/) is an instrument for evaluating the income of agricultural holdings and the impacts of the Common Agricultural Policy. The data stem from an annual survey carried out by the Member States of the European Union. The services responsible in the Union for the operation of the FADN collect every year accountancy data from a sample of the agricultural holdings in the European Union. Derived from national surveys, the FADN is the only source of microeconomic data that is harmonised, i.e. the bookkeeping principles are the same in all countries. Holdings are selected to take part in the survey on the basis of sampling plans established at the level of each region in the Union. The survey does not cover all the agricultural holdings in the Union but only those which due to their size could be considered commercial. The methodology applied aims to provide representative data along three dimensions: region, economic size and type of farming. While the European Commission is the primary user of analyses based on FADN-data, aggregated data can be found in the Standard Results database.

The aim of the FADN network is to gather accountancy data from farms for the determination of incomes and business analysis of agricultural holdings. Currently, the annual sample covers approximately 80.000 holdings. They represent a population of about 5.000.000 farms in the EU, which covers approximately 90% of the total utilised agricultural area (UAA) and account for about 90% of the total agricultural production. The information collected, for each sample farm, concerns approximately 1000 variables and is transmitted by Liaison Agencies. These variables described in a specific questionnaire called Farm Return refer to:

- Physical and structural data, such as location, crop areas, livestock numbers, labour force, etc.
- Economic and financial data, such as the value of production of the different crops, stocks, sales and purchases, production costs, assets, liabilities, production quotas and subsidies, including those connected with the application of CAP measures.

The legislation establishing FADN is Council Regulation 79/65/EEC of 15 June 1965. This legislation has since been modified and expanded; the basic act currently into force is Council Regulation (EC) No 1217/2009 of 30 November 2009 setting up a network for the collection of accountancy data on the incomes and business operation of agricultural holdings in the European Community. https://europa.eu/legislation_summaries/agriculture/general_framework/ag0008_en.htm

Incorporated into the founding legislation of FADN is a stipulation that all data relating to individual farms received by the Commission are to be treated with utmost confidentiality. Consequently, data at the level of individual farms are normally not released outside the Directorate General for Agriculture of the Commission. Only aggregated results for a group of farms and for farms within regions and Member States are published since, at this level of aggregation, information relating to individual farms cannot be discerned.

The interest of B-GOOD pertains to FADN data relating to “843 – Apiculture” and “SE251 – Other livestock and products (incl. honey)”. The use of FADN data is conditional upon a formal agreement between the “EC – Directorate-General for Agriculture and Rural Development – E.3 Economic analysis of EU agriculture (DG AGRI-E.3)” and DG RTD and the involved B-

GOOD partner as Beneficiaries. This agreement will stipulate the terms and conditions for use of the data. This will include, amongst others:

- The guarantee that the data will not be used for any other purpose;
- Observation of the rules on non-disclosure of the data and the secrecy of statistics;
- Not to publish a result when it is based on less than 15 observations (holdings);
- The specification of the only authorized persons to handle the FADN farm level data;
- The commitment to erase all FADN data once the project is completed;
- The commitment to take all necessary actions to protect the data.

In case information on individual farms (i.e. commercial beekeepers in our case) is obtained for the specific research purposes of B-GOOD, it will be ensured that data records are pseudonymised and protected in line with the procedures described in Sections 4, 5 and 6, and with the terms and conditions for its use as agreed with DG AGRI-E.3.

9. Appendices

Appendix 1. Details on data collection methods within WP4 and WP8

Task 4.1

Data collection from stakeholders within task 4.1 will be done by means of personal (face-to-face or online) interviews (n=40 stakeholders) (Study 1a), personal feedback interviews and surveys (n=25 stakeholders) (Study 1b), and a quantitative online survey (n=200 stakeholders) (Study 2). Stakeholders will be interviewed/surveyed by B-GOOD researchers in English or in their native language in case English is not feasible and as far as the linguistic skills of the interviewers enable us to do so. The types and contents of data/information that will be collected are detailed below. Issues and procedures related to the protection of personal data are addressed in "D10.2 POPD – Requirement no. 2".

Study 1a - The personal interviews (n=40 stakeholders) will collect textual data from narratives covering the following topics:

1. SWOT of beekeeping in the EU: views and opinions on internal strengths (S) and weaknesses (W) of the beekeeping sector in the EU in general, in specific countries and regions; views and opinions on external opportunities (O) and threats (T) facing the beekeeping sector in the EU in general, in specific countries and regions;
2. Bee health: views and opinions on what constitutes and characterises a healthy bee colony; the threats to bee colony health; future perspectives and challenges related to bee colony health;
3. Business models: views and opinions on current and future beekeeping business models; identification and profiling of beekeeping business models; forecast on future business models for healthy and sustainable beekeeping in the EU.

Study 1b – The feedback interviews combined with a survey (n=25 stakeholders who already participated in Study 1a) will provide participants with a synthesis of the outcomes of Study 1a and will collect textual data from narratives and quantitative scoring data covering the following topics:

1. Feedback, discussion and consensus-seeking on the identified SWOT-components, their grouping or classification, and meaning;
2. Quantitative scoring following the Strategic-Orientation-Round (SOR) procedure in which stakeholders are asked to provide a score (0-1-2-3) to each combination of S/W and O/T components.

All personal interviews will be audio-taped in order to allow for complete transcription of the narratives, i.e. converting audio-recordings to text for qualitative content analysis using the NVivo software that is designed specifically for gaining insights from qualitative and mixed-methods data. Audio-recordings will be destroyed following transcription. Transcripts will be stored in pseudonymised format on secured institutional servers as text files.

Study 1b is a follow-up to Study 1a. Hence, the 25 stakeholders who take voluntarily part in Study 1b will be recruited from the participants of Study 1a. The study protocol for both parts, including informed consent procedures and the final topic guides, will be submitted for ethics approval from the UZGent-UGent Ethics Committee "Commissie voor Medische Ethiek", or an equivalent competent authority, in December 2019. Data collection is planned during January-March 2020 for Study 1a and during March-April 2020 for Study 1b.

Study 2 – The quantitative survey with stakeholders (n=200) will quantify the views and opinions on each of the topics covered in the previous qualitative studies. The survey will therefore cover largely the same topics but in a closed-ended format (i.e. using concrete statements, items, constructs to be scored with predefined response scales, e.g. Likert interval

response scales) and a more structured format compared to the previous qualitative exploratory studies:

1. SWOT of beekeeping in the EU: views and opinions on internal strengths (S) and weaknesses (W) of the beekeeping sector in the EU in general, in specific countries and regions; views and opinions on external opportunities (O) and threats (T) facing the beekeeping sector in the EU in general, in specific countries and regions;
2. Bee health: views and opinions on what constitutes and characterises a healthy bee colony; the threats to bee colony health; future perspectives and challenges related to bee colony health;
3. Business models: views and opinions on current and future beekeeping business models; identification and profiling of beekeeping business models; forecast on future business models for healthy and sustainable beekeeping in the EU.
4. In addition, this survey will collect information on stakeholders' personal (non-sensitive, non-confidential) characteristics and background, e.g. age (years), education, type of stakeholder, years of experience with the beekeeping sector, in order to assess whether any of these personal characteristics associate with particular views and opinions on beekeeping, and to allow for the profiling of eventual stakeholder segments.

The quantitative survey data will be recorded and stored on secured institutional servers as a SPSS data file for statistical analysis using SPSS (Statistical Package for Social Sciences).

The protocol for Study 2, including informed consent procedures and the final questionnaires, will be submitted for ethics approval from the UZGent-UGent Ethics Committee "Commissie voor Medische Ethiek" ", or an equivalent competent authority, in September 2020. Data collection is planned during November 2020 – January 2021.

Besides being kept on file, the final study protocols and copies of ethics approvals will be submitted as Appendices to D4.1 for Study 1a and Study 1b, and as Appendices to D4.2 for Study 2.

Task 4.2

Data collection from beekeepers within task 4.2 will be done by means of online surveys. Two studies collecting quantitative data from beekeepers are planned. The first study includes the 40 beekeepers who take part in the field study A experiments. The second study concerns a survey with a pan-European sample of 600 beekeepers. Beekeepers will be surveyed online in English or in their native language as they prefer. The types and contents of data/information that will be collected are similar in both studies as detailed below.

Study 3 – The survey with 40 beekeepers involved in field study A experiments (WP1) will collect quantitative data dealing with:

1. Beekeepers' management characteristics: business objectives, plans, activities, bee health-related management decisions, beekeeping practices;
2. Bee colony attributes, characteristics, and output data relating to economic variables (e.g. costs and revenues) and production performance (outputs such as honey, other apiary products, pollination or extension services);
3. Beekeepers' personal characteristics: age, gender, education, living environment, experience with beekeeping, attendance to training activities, membership of beekeeping associations, attitudes, beliefs and perceptions in relation to their beekeeping business environment.

Data will be stored on secured institutional servers. The protocol for Study 3, including informed consent procedures and the final questionnaires, will be submitted for ethics approval from the UZGent-UGent Ethics Committee "Commissie voor Medische Ethiek" ", or an

equivalent a competent authority, in August 2020. Data collection is planned during October-November 2020.

Study 4 – The pan-European survey with 600 beekeepers will collect quantitative data in a similar vein as in Study 3, namely:

1. Beekeepers' management characteristics: business objectives, plans, activities, bee health-related management decisions, beekeeping practices;
2. Bee colony attributes, characteristics, and output data relating to economic variables (e.g. costs and revenues) and production performance (outputs such as honey, other apiary products, pollination or extension services);
3. Beekeepers' personal characteristics: age, gender, education, living environment, experience with beekeeping, attendance to training activities, membership of beekeeping associations, attitudes, beliefs and perceptions in relation to their beekeeping business environment.

In line with the data minimisation principle, we will use Study 3 to identify key variables that matter and limit our data collection to these in Study 4. Therefore, the questionnaire for Study 4 is expected to be shorter and more selective, especially with respect to economic variables and production performance, as compared to Study 3 since the latter will be used as an extended pilot that should allow us to fine tune our larger-scale data collection.

The protocol for Study 4, including informed consent procedures and the final questionnaires, will be submitted for ethics approval from the UZGent-UGent Ethics Committee "Commissie voor Medische Ethiek" ", or an equivalent competent authority, in June 2021. Data collection is planned during September-November 2021.

For both studies involving beekeepers, the quantitative survey data will be recorded and stored on secured institution servers as a SPSS data file for statistical analysis using SPSS (Statistical Package for Social Sciences). Economic performance data will be stored as an Excel data file for economic efficiency analysis using R.

<u>Tasks 4.3 and 8.2</u>

Data collection from stakeholders and beekeepers within tasks 4.3 and 8.2 will be done by means of facilitated participatory workshops. A single study is planned with workshops convened in five EU countries where participants will be recruited from the established list of key stakeholders (milestone 4.1) as well as from the networks of the involved research partners who have established close connections with national and regional beekeeper associations. Trained B-GOOD researchers acting as moderators/facilitators within each country will host the workshops. The workshops will be conducted either in English or in the native language for each country in case English is not feasible. The types and contents of data/information that will be collected are detailed below.

Study 5 – Workshops will comprise of approximately 20 participants per workshop and will collect qualitative data as part of a prototyping and elicitation protocol (PrOACT; a decision-making model referring to the identification of Problems; Objectives; Activities; Consequences and Tradeoffs). This protocol will engage participants in structured activities to:

1. Gain participant views and opinions on beekeeping related issues within each country and the EU in general, identifying collective problems, objectives and alternative solutions;
2. Collect information on participant's personal characteristics will also be gathered as part of setting up the workshops e.g. age, type of stakeholder, years of experience within the beekeeping sector. This information will be used to ensure workshops have a broad representation.

Participatory workshops will require participant involvement in group exercises with written / diagram outputs. Workshops will be audio-recorded in order to allow for transcription of

discussions, i.e. converting audio-recordings to text for further qualitative content analysis using the NVivo software for gaining insights from qualitative and mixed-methods data. Digital images will also be taken and all recordings, images and materials will be electronically stored on secured servers at the relevant institutions of the involved researchers in the study.

The protocol for Study 5, including informed consent procedures and the final workshop format, will be submitted for ethics approval from the UZGent-UGent Ethics Committee "Commissie voor Medische Ethiek", or an equivalent competent authority, and the Aarhus University Ethics Committee.

Task 8.3

Data collection as part of task 8.3 will take the form of two facilitated workshops convened as part of B-GOOD's Multi-Actor Forum. These will take place mid-way and towards the end of the project. Selected participants will be recruited from the established list of key stakeholders and/or people having participated in previous workshops. The types and contents of data/information that will be collected are detailed below.

Study 6 – Workshops will comprise of approximately 20-30 participants per workshop and will collect qualitative data by engaging participants in structured activities to:

1. Gain participant views and opinions on developments within the B-GOOD project and provide feedback / evaluation of the project's progress in delivering stakeholder focused research, collaborations and bee-management outcomes;
2. Collect information on participant's personal characteristics will also be gathered as part of setting up the workshops e.g. age, type of stakeholder, years of experience within the beekeeping sector. This information will be used to ensure workshops have a broad representation.

As with the previous study, Study 6 workshops will be audio-recorded, notes taken and all materials electronically stored on secured institutional servers.

The protocol for study 6, including informed consent procedures and the final workshop format, will be submitted for ethics approval from the Aarhus University Ethics Committee.

Task 8.4

Data collection within task 8.4 will be done via a qualitative interview conducted amongst members of the Multi-Actor Forum and selected influential actors, recruited from the list of key stakeholders. Approximately 40 interviews will be conducted and the types and contents of data/information that will be collected are detailed below.

Study 7 – Semi-structured telephone interviews (using both open and closed questions) will be used to:

1. Gather individuals' perceptions and experiences of B-GOOD's collaborative and learning processes and its outcomes.

Interviews will be audio-recorded in order to allow for transcription of discussions, i.e. converting audio-recordings to text for further qualitative content analysis using the NVivo software for gaining insights from qualitative and mixed-methods data. Data will be stored on secured institutional servers.

The protocol for Study 7, including informed consent procedures and the final workshop format, will be submitted for ethics approval from the Aarhus University Ethics Committee.

Appendix 2. Confirmations of compliance with GDPR and national laws for partners UGENT, AU, UCOI and WR

B-GOOD

Declarations on compliance and/or authorisation

The following declarations of compliance must be signed by the institutional Data Protection Officer and/or a designated representative of each B-GOOD project partner, and a scanned copy must be sent to the project coordinator. Each partner must also keep the original of the signed declarations securely on file, and must submit the declarations to the European Commission on request.

Please note that each partner must complete and sign **TWO** of the following declarations: declaration 1), and either declaration 2) or declaration 3).

Name (and acronym) of the partner institution: Ghent University – UGent

1. **Data protection within the H2020 B-GOOD project** (to be completed and signed by all partners)

   I, Hanne Elsen, hereby state that given the available information and the research design of the project mentioned above, carried out by the researchers of Ghent University, complies with the principles and regulations of the Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and the national legislation of personal data regarding data protection; and that this declaration of compliance and/or authorisation will be kept on file and submitted to the European Commission upon request by the researchers.

   Signed _____ (~~Researcher or~~ Data Protection Officer, ~~delete what does not fit~~)

   Date 26/11/2019

2. **No national requirements** (to be completed and signed by partners from countries without national requirements)
   I, Click or tap here to enter text., hereby state that no declaration of compliance or authorisation for collecting and processing personal data are required under the national laws of Click or tap here to enter text..
   I furthermore declare that this declaration of compliance and/or authorisation will be kept on file and submitted to the European Commission upon request.

   Signed_____(Researcher)

   Date

European Commission | B-GOOD has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 817622.

3. National requirements (to be completed and signed by partners from countries with national requirements)

I, Wim Verbeke, hereby state that given the available information all required declarations of compliance or authorisation for collecting and processing personal data, as required under the national laws of Belgium, have been completed.

I, furthermore declare that this declaration of compliance and/or authorisation will be kept on file and submitted to the European Commission upon request.

Signed  (Researcher)

Date 26/11/2019

European Commission

B-GOOD has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 817622.

Declarations on compliance and/or authorisation

The following declarations of compliance must be signed by the institutional Data Protection Officer and/or a designated representative of each B-GOOD project partner, and a scanned copy must be sent to the project coordinator. Each partner must also keep the original of the signed declarations securely on file, and must submit the declarations to the European Commission on request.

Please note that each partner must complete and sign **TWO** of the following declarations: declaration 1), and either declaration 2) or declaration 3).

Name (and acronym) of the partner institution: **Aarhus University** (AU)

1. **Data protection within the H2020 B-GOOD project** (to be completed and signed by all partners)

   I, James Henty Williams, hereby state that given the available information and the research design of the project mentioned above, carried out by the researchers of Aarhus University, complies with the principles and regulations of the Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and the national legislation of personal data regarding data protection; and that this declaration of compliance and/or authorisation will be kept on file and submitted to the European Commission upon request by the researchers.

   Signed _____(Researcher)

   Date 27/11/2019

2. **No national requirements** (to be completed and signed by partners from countries without national requirements)
   I, Name of Researcher, hereby state that no declaration of compliance or authorisation for collecting and processing personal data are required under the national laws of Country.
   I furthermore declare that this declaration of compliance and/or authorisation will be kept on file and submitted to the European Commission upon request.

   Signed_____(Researcher)

   Date

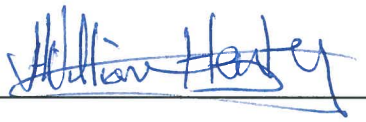
European Commission

B-GOOD has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 817622.

3. **National requirements** (to be completed and signed by partners from countries with national requirements)

I, James Henty Williams, hereby state that given the available information all required declarations of compliance or authorisation for collecting and processing personal data, as required under the national laws of Denmark, have been completed.

I, furthermore declare that this declaration of compliance and/or authorisation will be kept on file and submitted to the European Commission upon request.

Signed  (Researcher)

Date 27/11/2019

European Commission

B-GOOD has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 817622.

Declarations on compliance and/or authorisation

The following declarations of compliance must be signed by the institutional Data Protection Officer and/or a designated representative of each B-GOOD project partner, and a scanned copy must be sent to the project coordinator. Each partner must also keep the original of the signed declarations securely on file, and must submit the declarations to the European Commission on request.

Please note that each partner must complete and sign **TWO** of the following declarations: declaration 1), and either declaration 2) or declaration 3).

Name (and acronym) of the partner institution: University of Coimbra – UCOI

1. **Data protection within the H2020 B-GOOD project** (to be completed and signed by all partners)

   I, Fátima Alves, hereby state that given the available information and the research design of the project mentioned above, carried out by the researchers of University of Coimbra, complies with the principles and regulations of the Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and the national legislation of personal data regarding data protection; and that this declaration of compliance and/or authorisation will be kept on file and submitted to the European Commission upon request by the researchers.

   Signed  (Data Protection Officer)

   Date 27/11/2019

2. **No national requirements** (to be completed and signed by partners from countries without national requirements)
   I, Name of Researcher, hereby state that no declaration of compliance or authorisation for collecting and processing personal data are required under the national laws of Country.
   I furthermore declare that this declaration of compliance and/or authorisation will be kept on file and submitted to the European Commission upon request.

   Signed_____(Researcher)

   Date

B-GOOD has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 817622.

3. **National requirements** (to be completed and signed by partners from countries with national requirements)

I, Fátima Alves, hereby state that given the available information all required declarations of compliance or authorisation for collecting and processing personal data, as required under the national laws of Portugal, have been completed.

I, furthermore declare that this declaration of compliance and/or authorisation will be kept on file and submitted to the European Commission upon request.

Signed  (Researcher)

Date 27/11/2019

B-GOOD has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 817622.

Declarations on compliance and/or authorisation

The following declarations of compliance must be signed by the institutional Data Protection Officer or a designated representative of each B-GOOD project partner, and a scanned copy must be sent to the project coordinator. Each partner must also keep the original of the signed declarations securely on file, and must submit the declarations to the European Commission on request.

Please note that each partner must complete and sign **TWO** of the following declarations: declaration 1), and either declaration 2) or declaration 3).

Name (and acronym) of the partner institution: Wageningen Research (WR)

1. **Data protection within the B-GOOD project** (to be completed and signed by all partners)

   I, **Peter Ras**, hereby state that given the available information all personal data collection and processing in the research design of the project mentioned above will be carried out according to EU and national legislation; and that this declaration of compliance and/or authorisation will be kept on file and submitted to the European Commission upon request.

   Signed _____(Data Protection Officer)

   Date 21 November 2019

2. **No national requirements** (to be completed and signed by partners from countries without national requirements)
   I, Click or tap here to enter text., hereby state that no declaration of compliance or authorisation for collecting and processing personal data are required under the national laws of Click or tap here to enter text..
   I furthermore declare that this declaration of compliance and/or authorisation will be kept on file and submitted to the European Commission upon request.

   Signed _____(data protection officer)

   Date xx/xx/xxxx

European Commission

B-GOOD has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 817622.

3. **National requirements** (to be completed and signed by partners from countries with national requirements)
I, **Peter Ras,** hereby state that all required declarations of compliance or authorisation for collecting and processing personal data, as required under the national laws of the Netherlands, have been completed.

I, furthermore declare that this declaration of compliance and/or authorisation will be kept on file and submitted to the European Commission upon request.

Signed B.A. _____(data protection officer)

Date 21 November 2019

B-GOOD has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 817622.

Appendix 3. UGENT code of conduct for the processing of personal data and confidential information

Generic code of conduct for the processing of personal data and confidential information

Title	Code of conduct for the processing of personal data and confidential information
Reference	ISMS.codeofconduct
Type	Code of conduct
Classification	General
Distribution	All employees and students (via portal, under Information security)

Version	**Date**	**Author (s)**	**Description and history**
1.0.	14 April 2017	Michel Raes	First draft
1.5.	16 November 2017	Michel Raes	After feedback different stakeholders
2.0.	16 April 2018	Kristof De Moor	After informal consultations with the trade unions representatives
2.5.	25 April 2018	Kristof De Moor	After additional first (formal) negotiation with negotiation committee for university staff
3.0.	08 May 2018	Kristof De Moor	After additional second (informal) negotiation with negotiation committee for university staff

1. Objective of this document

This document establishes a generic code of conduct for the processing of personal data at Ghent University through IT applications. By extension, this code of conduct also applies to manual processing operations of personal data at Ghent University, as well as to the processing of confidential information of Ghent University.

This code of conduct includes rules for permitted lawful access to and use of such data in the IT applications of Ghent University. This code of conduct should therefore be read together with the rules for proper use of the ICT infrastructure of Ghent University.

This code of conduct is part of the general data protection policy (i.e. the policy for the legitimate and safe processing of personal data) that is pursued at Ghent University.

Where necessary, this generic code of conduct can be supplemented by codes of conduct that focus on specific applications and processing.

2. Definitions

In this code of conduct, the following terms are used with the following meanings:

1° Processing: any fully or partially automated or manual operation (processing or set of operations) relating to the entire lifecycle of data: collection, recording, organisation, structuring, storage, updating or alteration, retrieval, consultation, use, disclosure by transmission, distribution or otherwise making available, alignment or combination, blocking, deletion or destruction of data, etc. (this is a non-exhaustive list).

2° **Personal data**: any information about an identified or identifiable natural person (the latter will be referred to as the **data subject**). In accordance with European and Belgian privacy legislation, this definition is very broad[1]. This includes medical information, i.e. any information that, directly or indirectly, is related to the health or physical and/or mental state of a natural person.[2]

3° Confidential information: information and data (other than personal data) are considered confidential at Ghent University if there are legal or regulatory grounds for doing so, or after the Application Owner explicitly declares the information to be confidential because the interests of Ghent University are or may be harmed when it is published[3], in particular: (i) information relating to any legal or administrative proceedings or criminal facts to which Ghent University is a party; (ii) information which may harm an economic, financial or commercial interest of Ghent University or the confidential nature of the relationship with another (government) institution or body; (iii) information in connection with Ghent University that is of importance to public order and safety; (iv) a preparatory document for advisory and governing bodies and committees of Ghent University containing information in one of the above categories; (v) administrative or policy information, as well as a preparatory document containing this information, the confidentiality of which is temporary yet necessary in the stage

[1] See the General Data Protection Regulation (GDPR) Art. 4, 1): an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[2] See also the definition of "data on health" in Art. 4,15) of the GDPR: personal data related to the physical or mental health of a natural person, including data on health services provided that provide information on his health status.

[3] See also the policy paper “Guidelines for the classification of information and data" (Executive Board of 10 July 2015), available at https://www.ugent.be/en/facilities/ict/information-security/classification-data.pdf

of conceptual analysis and vision development on institution-wide themes and dossiers (i.e. prior to a possible decision and approval process)[4].

4° Application: An IT system to support processes and activities at Ghent University.

5° Application Owner: this is the person who defines the purpose and means of each Application, and who also decides which users or user roles can access the Application and what information they can access. For the processing of personal data, this is equivalent to a **Processing Controller**, as laid down by law.

6° User[5]: anyone (e.g. student, lecturer, Ghent University employee, external party) who in any way processes personal data and/or confidential information, in particular someone who has access to one or more functionalities within an Application.

3. Legal framework

The legal framework for the processing of personal data and confidential information is determined by:

- the General Data Protection Regulation (GDPR). This new European privacy regulation is directly applicable as of 25 May 2018, without prior transposition into national law.

- Belgian privacy legislation, in particular the Law of 8 December 1992 on the protection of privacy with regard to the processing of personal data, together with all amendments and implementing decrees.

In the event of any conflict between this code of conduct and the aforementioned legislation, legislation will apply, with the European regulation taking precedence over Belgian law.

4. Scope

4.1. Material scope

This code of conduct applies to any fully or partially automated processing of personal data and confidential information.

It also applies to the manual processing of files containing personal data or confidential information.

When the term 'data' is used in this document, it refers to personal data or, by extension and where applicable, to confidential information.

Non-confidential, general and publicly accessible information is disregarded in this code of conduct.

[4] Such as a first draft of university policy vision or a proposal with an administrative position, which then may or may not lead to formal administrative decision-making. In this context, the explicit designation as confidential of this administrative or policy information (carriers) (e.g. by adding the reference 'confidential' to a document) is always temporary in nature. Confidentiality can be lifted by the Application Owner in the course of the concept phase but shall always be lifted before the formal start of the decision process in which the various steps of advice, negotiation and approval are followed successively.

[5] The use of the term "processor" is avoided because "processor" in the context of the privacy legislation has a different, specific meaning.

4.2. Personal scope

This code of conduct shall apply to anyone who processes personal data or confidential information in the context of activities that fall within the scope of Ghent University.

Persons for whom this code of conduct is intended may have various legal statuses:

- Employees who have a **statutory or contractual working relationship with Ghent University** (paid employees) are bound by the labour regulations and this code of conduct to their responsibilities for the lawful and safe processing of personal data and confidential information.
- For **unpaid employees, students** or other persons who have **no contractual working relationship** with Ghent University, the responsibility for the lawful and secure processing of personal data and confidential information shall be laid down in a specific agreement in which the person in question is bound by the present code of conduct. For students, this means that an agreement is concluded together with (or as part of) the entry agreement.

If personal data are processed by external service providers, a processor agreement shall be concluded between this processor and Ghent University as the data controller. In such a processing agreement, the processor shall be required to comply with the information security policy of Ghent University, and in particular with this code of conduct.

Conversely, Ghent University will act as a processor of personal data in certain cases, in which case a processor agreement will have to be concluded with the (external) controller. In that case too, this processor agreement may refer to this code of conduct.

5. Code of conduct

5.1. Principles to be complied with[6]

1° Accountability: Anyone who shares responsibility for the processing of personal data in the context of activities at Ghent University is expected to be able to demonstrate that **responsibility** has **actively** been taken to ensure that the processing takes place in a **lawful and secure** manner. This means, among other things, that it is documented what exact personal data are processed and for what purposes. This should be accomplished in a **record of processing activities**, pragmatically and generating as little administrative burden as possible[7]. If the processing potentially involves a high risk, the risks and foreseen measures shall be assessed and documented prior to the processing[8]. The record of processing activities is the first tool to assess what processing operations may present a high risk. Where necessary, advice will be sought from the Data Protection Officer of Ghent University.

2° Confidentiality and integrity: All users are obliged to treat the personal data and/or confidential information to which they have access as confidential. In addition, each user is

[6] See also Art. 5 and paragraph 39 of the GDPR

[7] General modalities pursuant to article 30 of the GDPR and the explanations of the Privacy Commission on https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_06_2017_0.pdf
The record of processing activities is not necessarily a central record but may also be implemented in a decentralised manner (e.g. per Department and per Faculty). Specific internal Ghent University guidelines are drawn up for this purpose.

[8] In a Data Protection Impact Assessment, in accordance with article 35 of the GDPR.
For more information on this, see guidelines WP 248 of the Working Party 29 (4 April 2017) on http://ec.europa.eu/newsroom/document.cfm?doc_id=47711, as well as the (draft) recommendation of the Privacy Commission on
https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_01_2018.pdf .
Specific internal Ghent University guidelines are also drawn up for this purpose.

expected to take all reasonable steps to ensure the confidentiality and integrity of the data processed. In other words, s/he will help to ensure that the data are adequately protected to prevent unauthorised disclosure. To this end, the information security policy[9] of Ghent University, and in particular the practical guidelines for working safely with IT resources, can be used[10]. Each user also contributes to the integrity of the equipment used for processing (e.g. protection against theft, loss, damage or destruction). If a user detects a data leak (or other related incident), this immediately has to be reported to the Department of Information and Communication Technology, which acts as the central contact point for this purpose.

3° Lawfulness, fairness and transparency: Each user processes personal data and/or confidential information in compliance with all applicable laws, regulations and rules. He or she shall show the necessary ethical integrity in this process. Moreover, it has to be clear to the hierarchical line and to the data subjects that the user collects, uses, consults or otherwise processes these data.

4° Purpose limitation (finality and proportionality): Each user has to respect the specific purposes for which the data are processed. These purposes are clearly defined *and* documented for each application. Processing shall be reasonable and proportionate to the purpose of each application. Any other, additional and therefore improper use of the data is not permitted. This also means that users may only access and/or be given access on a need-to-know basis. If possible, this is also enforced technically. Exceptions for additional processing can only be made within the context of the legislation or regulations established for this purpose (e.g. for scientific or historical research or statistical purposes, for archiving in the public interest, or for further research or control mechanisms for scientific integrity).

5° Data minimisation: Users are not allowed to process (e.g. collect, consult) more data than is necessary for the defined purposes. Personal data may only be processed if the purpose of the processing cannot reasonably be achieved by other means. Wherever possible, anonymised data should be used. If the intended purpose cannot be achieved in this way, pseudonymised (also referred to as 'coded') personal data shall be used. Raw personal data may only be processed if it is correctly justified that the intended purpose cannot be achieved by means of anonymised or pseudonymised data.

6° Accuracy: Users take due care to ensure that the data that they process are correct and up to date. Users shall take all reasonable steps to ensure that inaccurate data is corrected, either on their own initiative or at the request of data subjects[11].

7° Storage limitation: Users shall ensure that the storage period/retention period of personal data and confidential information is determined in accordance with all relevant legal provisions and applicable agreements. In addition, the storage period/retention period should be limited to what is necessary and in accordance with the original purposes. Exceptions for longer retention can only be made within the context of the legislation or regulations established for this purpose (e.g. for scientific or historical research or statistical purposes, for archiving in the public interest, or for further research or control mechanisms for scientific integrity). After the retention period has expired, the data have to be completely and securely deleted, in accordance with the guidelines in the information security policy of Ghent University[12].

[9] See https://www.ugent.be/informationsecurity

[10] See https://www.ugent.be/en/facilities/ict/information-security/data-confidential-information.pdf

[11] The possibility to do so will be disclosed to the data subjects, for example by means of an informed consent form or an online privacy notice.

[12] See https://www.ugent.be/informationsecurity

5.2. Use of IT applications at Ghent University

Any use of IT applications is subject to the Regulations for the correct use of the ICT infrastructure of Ghent University[13].

Access to IT applications is strictly personal through the Ghent University account or through specific accounts for external users.

Each user is responsible for what happens under his or her account (unless the user, despite due care, is himself/herself the victim of abuse of the account in question).

5.3. Registration of users of IT applications

1° Certain users are automatically granted access to an IT application based on their status or the user roles designated by the Application Owner. Within that application, they may only access data relevant to their user role. Wherever possible, this is technically enforced (i.e. role-based access in accordance with the principles of least privilege and separation of duties).

2° Other persons or roles may have access to an application on an individual basis subject to the consent of the Application Owner. The procedures for this are laid down and documented separately for each application.

3° User access as referred to in point 1° shall automatically be adapted or cancelled via an automated process in the event of a change in the user role. User access as referred to in point 2° shall be adjusted or revoked as soon as possible under the responsibility of the Application Owner, in accordance with a procedure laid down for this purpose[14].

4° In order to verify the appropriateness of user management, periodic checks are carried out by or on behalf of the Application Owner and/or the Data Protection Officer of Ghent University.

5° A number of users with multiple roles will have more access to information on the basis of the different roles they take up at Ghent University. For example, a user may have access to the data of one specific department based on his/her user profile. If this user is also a member of the Board of Governors, then his/her user profile will allow university-wide viewing of administrative information. Such users with multiple roles are expected to show the required deontological integrity to use the available information only in accordance with the correct finality and proportionality within their respective roles.

6° Anyone who establishes that s/he has improper access to an IT application as s/he is not one of the authorised users mentioned in point 1° or 2° shall immediately report this to the helpdesk of the Department of Information and Communication Technology, copying in the Application Owner if applicable. Similarly, a lawful user who discovers that s/he has access to broader functionalities than those normally foreseen for his/her respective role shall report this to the Department of Information and Communication Technology, copying in the Application Owner if applicable.

[13] Laid down by decision of the Executive Board of 19 May 2017; see https://www.ugent.be/en/facilities/ict/policy-usage-ict.pdf

[14] The Application Owner is responsible for establishing and (allowing) compliance with this procedure.

5.4. Transfer of personal data or confidential information

1° Third parties – including governments, public and semi-public bodies and organisations – are not entitled to inspect personal data or confidential information of Ghent University unless there is a legal or administrative framework[15] for doing so.

When personal data are systematically transferred to third parties, the Application Owner will ensure that the privacy notice of the application in question specifies the personal data involved and the processing to which they will be subjected by those third parties.

Personal data may never be passed on for commercial or advertising purposes, nor may they be passed on to third parties who would use these data for such purposes.

2° With the explicit consent of the data subject, Ghent University is allowed to pass on or publish data. This is only possible if the data subject himself/herself has given permission to pass on or disclose his/her personal data in a certain way, permission has to be in writing or electronically and on the basis of specific and correct information. Only the data subject is able to grant this permission.

3° In order to prevent intentional and unintentional data leaks, access to or the communication of personal data or confidential information from Ghent University to third parties shall only be granted by means of official procedures provided for that purpose (e.g. in the context of a transparent administration).

5.5. (ICT) employees

For technical reasons, some employees[16] may have very extensive possibilities to know the internal operation of applications and the data associated with it. They are therefore required to comply with this code of conduct at all times, with the necessary ethical integrity. Special points of interest:

- Employees are forbidden to read the electronic mail in the personal mailbox or the unshared files (in particular those on the personal disk space or home drive) of another user without his/her explicit permission.
- Employees are not allowed to work on the personal account of another user, unless exceptionally and very temporarily for maintenance or support activities:
  - either locally, in the presence of that user (with the user himself/herself entering the username and password on the system)
  - or remotely, after the user has given permission for the screen to be taken over, with the start and end of the takeover clearly indicated by a message on the user's screen[17].

[15] Such a framework exists, for example, for (this is a non-exhaustive list):

- requesting administrative documents for the benefit of public access to government (Decree of 26 March 2004 about the publicity of the administration, Executive Board of 1 July 2004)
- requesting archival documents (Archives Decree: Decree of 9 July 2010 about the management of public archival records, Executive Board of 5 August 2010 and the provisions with regard to accessibility, public access and availability contained in the internal rules and regulations for the archival service of Ghent University).
- requesting information on the basis of a court order in the light of a police or legal investigation
- requesting data by the State Security Service (Federal Public Service Justice).

[16] These may include all kinds of employees, but in particular ICT employees such as system administrators, helpdesk employees, developers & application administrators (this is a non-exhaustive list).

[17] See https://helpdesk.ugent.be/help/en/

- If data of a particular user are to be available for other people, these should be on a shared disk space or in a shared mailbox, or a different proxy functionality has to be used.
- Accessing or granting access to private data is only permitted in individual exceptional cases on a court order or at the request of the State Security Service.
- Exceptional access to data of people who are temporarily or definitively incapacitated (e.g. in the event of a major accident, coma, or death) can only be granted in accordance with a specific procedure which will be laid down for this purpose.
- In applications where this is deemed necessary (e.g. as a conclusion of a Data Protection Impact Assessment), the Application Owner has to have additional technical measures in place (e.g. encryption) to increase the confidentiality of the data also towards the ICT staff.
- The ICT infrastructure of Ghent University is monitored by ICT system administrators (logging and monitoring) to ensure its proper functioning and to detect and prevent abuse. Storage of and access to the accompanying data can only take place in accordance with the principles of this code of conduct. This means, inter alia, that the level of detail of those data and the retention period should not exceed what is necessary to achieve the objective.

5.6. Administrative applications

All employees of Ghent University who work with personal data in administrative applications are expected to take note of and comply with this code of conduct.

Typical central examples are personnel administration, the student administration, the administration of student facilities, etc. Typical examples in a decentralised context are the administration of departments and faculties.

For certain administrative applications, it may be useful (e.g. to clarify for the concrete application) to draw up specific additional policy documents or codes of conduct[18].

5.7. Administrative and policy information

Administrative and policy information is all information that is collected, recorded and processed for the purpose of managing, operating and overseeing the organisation, as well as for the purpose of accountability.

UGI is the Ghent University Integrated (Policy) Information System to support policy and decision-making processes. Each individual UGI application provides a defined set of policy information, aimed at a specific administrative objective through specific visualisation (e.g. educational quality assurance, interfaculty staff allocation key).

To this end, UGI processes and collects basic data from one or more databases, both inside and outside Ghent University (e.g. OASIS (education administration and student information system), SAP (accounting, human resources, buildings and facilities management, etc.), and public databases).

Each UGI application has an Application Owner (e.g. administrator, director or head of office) who decides which policy information is required within a UGI application (finality and

[18] As an example, reference is made to the existing "Code of Conduct for the Use of the Education Administration and Student Information System (OASIS)" and the "Good practices of dealing with requests for personal data (in the context of student administration)".
See (in Dutch): http://www.ugent.be/intranet/nl/onderwijs/intern/oasis (Established by the decision of the Executive Board on 5 September 2013; this existing code of conduct for OASIS will be revised to harmonise it with the present code of conduct).

proportionality of the UGI application) and which user roles (can) gain access to the application in what way and what policy information they can consult.

Every user of a UGI application is expected to take note of and comply with this code of conduct.

5.8. Research activities

All researchers (both staff members and Master's dissertation students and doctoral students) who work with personal data or confidential information of Ghent University are expected to take note of and comply with this code of conduct.

As an institution, Ghent University in principle bears the liability and ultimate responsibility for the lawful and secure processing of personal data. However, based on the principle of **empowerment**, this responsibility is shared with the **person(s) responsible for the research, i.e. the supervisor** and/or leader of the research group and the other participants in the research (possibly also students)[19].

Specific reference is made to the accountability for the processing of personal data, which actually includes a comprehensive documentation requirement (see point 5.1 1°). **Research data management**[20] or good, efficient use of research data is an essential part of the research process. When personal data are processed, privacy protection and secure processing are important considerations in data management. This can be adopted into the **data management plan** (as is already required for some research funding).

With regard to data protection and information security, data management involves thinking about and/or implementing (this is a non-exhaustive list):

- risk management: what are the privacy and information security risks related to the data?
- transparency: how are data subjects correctly informed about the processing of their personal data? How is consent obtained?
- data minimisation (i.e. only collecting and/or processing those personal data that are necessary for the research purposes)
- anonymisation or pseudonymisation (also referred to as 'coding') of personal data
- a safe storage strategy (including the establishment of a suitable storage period)
- a secure processing strategy (e.g. with centrally provided applications on central infrastructure)
- a safe disposal strategy (after expiry of the predetermined retention period)

For the handling of medical (personal) data in the context of research activities, reference is made to the protocol for research and valorisation with the Ghent University Hospital and the agreements contained therein concerning cooperation in the field of clinical scientific research[21], without prejudice to the specific regulations that apply to the lawful and safe processing of medical data[22].

Wherever necessary, the researcher takes the initiative to obtain additional information and advice on the aforementioned aspects of data protection and information security, for example via the faculty or central support offices for research data management, and/or from the Data

[19] There is joint responsibility, as provided for in Art. 26 of the GDPR.

[20] See https://www.ugent.be/en/research/datamanagement

[21] As approved by the Board of Governors on 22 December 2017

[22] See also, for example, the law of 22 August 2002 on patient rights (as amended), the criminal law provisions on (medical) confidentiality and the code of medical ethics (art. 55 - 70).

Protection Officer of Ghent University, if necessary in collaboration with the Data Protection Officer of the Ghent University Hospital (e.g. for the processing of medical data).

6. Compliance

Each user is obliged to comply with this code of conduct, without prejudice to generally applicable regulations.

The management of Ghent University will provide appropriate awareness-raising and accountability actions within the context of this code of conduct, to communicate and disseminate the principles and information contained therein, to further translate them into practical guidelines and procedures, and to support all users in complying with them.

In the first place, Ghent University relies on each user's own sense of responsibility in complying with this code of conduct.

If, after having been sufficiently informed, users nevertheless deviate from this code of conduct, this can give rise to formal (re)actions if the behaviour, after verification, is considered to be compellable.

If the user is a contractual or statutory employee, s/he may be asked to explain their behaviour during performance and evaluation interviews.

Possible measures and sanctions to be taken against individuals for establishing active, deliberate and repeated violations of this code of conduct and taking into account the seriousness of the violation:

- Disciplinary measures by the rector: the temporary suspension of an account or the temporary restriction of access to (parts of) the ICT infrastructure (striking a balance between the interests of the service, the protection of the systems and the rights of the data subject, as the account is often necessary for the performance of the job or studies in question);
- Measures and sanctions as provided for in the applicable (e.g. labour law) regulations and in the internal regulations of Ghent University, including the disciplinary regulations.

7. Data Protection Officer

7.1. Support

The Data Protection Officer of Ghent University is the single point of contact for interpreting this code of conduct, for questions and comments, for solving problems and for special situations in the context of this code of conduct.

7.2. Monitoring

The Data Protection Officer of Ghent University is authorised to supervise the lawful and secure processing of personal data at Ghent University. For example, random audits of personal data processed at Ghent University can be organised by the Data Protection Officer.

This is a translation. The original policy text in Dutch was approved by the management of Ghent University (Executive Board of 18 May 2018). In case of discrepancies or doubts about the interpretation of this text, the original Dutch version prevails.

Appendix 4. Directives on Data Protection in the IT Domain at the UBERN (CH)

UNIVERSITÄT
BERN

Directives

Data protection in the IT domain at the University of Bern

Distributor	Administrative Director's Office, IT Manager, IT Services Office
Class	For internal use
Document status	Approved

Table of contents

1. Basic information

1.1 Aim

These directives are designed to enable the more effective classification of data in the IT domain according to level of responsibility and sensitivity. They provide some basic guidelines as to which technical tools are best suited to which level of protection.

The directives are divided into legal and technical sections.

2. Data protection

Everybody affiliated with the university occasionally comes into contact with "data", including:

- students, e.g. during their enrollment;
- examination officers, e.g. when announcing and archiving exam results;
- researchers, e.g. when dealing with survey findings or empirically obtained data relating to individuals;
- service providers, e.g. when consulting medical histories;
- IT officers, e.g. when handling data access requests and securing physical data.

As a public-law entity, the university is subject to the **cantonal data protection legislation** of the Canton of Bern, specifically the Cantonal Data Protection Law of February 19, 1986 (KDSG; BSG 152.04). [1]

Data protection is the implementation of constitutional laws that safeguard personal rights, privacy and confidentiality. Article 13, paragraph 2 of the Federal Constitution of April 18, 1999 states: *"Every person has the right to be protected against the misuse of their personal data."*

3. Data

Within the meaning of data protection legislation, "data" always signifies all **personal data**, i.e. "information about an identified or identifiable natural or legal person" (Art. 2, para. 1 KDSG). This includes:

- personal data;
- enrollment documents;
- exam papers;
- personal files such as correspondence, appeals, notes, reports and evaluations;
- personal research data such as completed questionnaires and interview transcripts.

3.1 Highly sensitive data

Highly sensitive data is subject to particular restrictions in terms of its security and distribution. Under Art. 3 KDSG, highly sensitive data is specifically that which concerns:

- a person's religious, ideological or political beliefs, affiliations or activities, and ethnicity;
- personal privacy, in particular a person's physical, mental or psychological condition;
- social care or welfare support arrangements;
- police investigations, criminal proceedings, offenses and any punishments or other measures subsequently imposed.

4. Information security and data protection plan

If it is known or suspected that data is processed in an organizational unit within the meaning of data protection legislation, an information security and data protection (ISDP) analysis or plan must be established according to the instructions of the Department of Informatics and Organization (KAIO).

If you have any questions in this regard, please contact the IT Services Office [2].

If a new database containing personal data is created, the owner of that database is obliged to register it with the supervisory authority for data protection of the canton of Bern [3].

5. Handling data

Personal data may only be processed (i.e. collected, modified, distributed, etc.) where and to the extent that a **legal mandate** provides a sufficient legal basis to do so (Art. 5 KDSG). For highly sensitive data, the legal basis must be particularly clear and the need to process that data compelling (Art. 6 KDSG). For the processing of all other personal data, on the other hand, an implicit basis – e.g. one derived from the institutional purpose and functions of the university – is sufficient.

Where data is processed for **research purposes**, personal data must be redacted such that no conclusions can be drawn about the person in question (Art. 15 KDSG).

The university is itself **accountable** for the processing of its data (Art. 8 KDSG) and must take responsibility for misuse, including the payment of any damages. The university could face significant costs if those affiliated with it fail to comply with data protection legislation.

Individuals about whom data exists have the **right to access** their file on completion of any processes (e.g. assessments of academic achievement, doctoral or post-doctoral processes) (Art. 21 KDSG; for restrictions of this principle see Art. 22 KDSG).

However, during ongoing processes, the provisions of the Administrative Justice Law of May 23, 1989 (VRPG; BSG 155.21) apply.

6. General technical principles for IT

The general technical principles set out below are rules, which must consistently be applied, regardless of data protection level:

- no unsecured (unencrypted) transmission;
- no access to IT resources without appropriate protection (password, certificate, etc.);
- clear rules on the right to access IT resources, restrictions where necessary/feasible, periodic checks;
- shutdown, deactivation, uninstallation of any devices, services, etc. not being used (any longer);
- compliance with the Richtlinien der Informatikdienste für die sichere Entsorgung von IT-Datenträgern (IT Services Office guidelines on the secure disposal of electronic data carriers) [4].
- files which are stored on externally controlled media/services (clouds) must be encrypted;
- maintenance of IT resources: patch management, updates, malware protection, etc.;
- secure and restricted physical access to IT resources;
- production and distribution of user directives (for subjects not already covered by existing university directives);
- development of a backup strategy (including for data confidentiality/integrity);

6.1 Transporting data on mobile data carriers

Having personal data on mobile data carriers shall be reduced to a minimum and be understood to be an exception. In case of transportation, data must be protected from unauthorized read, copy, modify and/or delete. (cf. Art. 5 Abs. 1 Bst. c Datenschutzverordnung, DSV; BSG 152.040.1)

6.2 Data protection on the university network

Where a user group uses an additionally secured local network in parallel to the university network, the two connections must be kept physically separate. Users may directly connect to either the university network or a secure network segment, but not both at the same time.

6.3 Highly sensitive data

- Highly sensitive data used for research, services and administration, in particular highly sensitive personal data within the meaning of Art. 3 KDSG, must not be transferred unencrypted via the university network.
- Terminal devices holding unencrypted highly sensitive data must not be directly connected to the open university network.
- Highly sensitive data is subject to additional technical protective measures in the IT domain. While those measures may suffice individually, they are generally combined. Specifically, they include:
  a) protection of the local network with a suitable filter (firewall, packet filter);
  b) protection of data confidentiality/integrity on data carriers through encryption;
  c) protection of data confidentiality/integrity during transmission through encryption.

6.4 Telecommunications confidentiality

Information transmitted via the university network is protected under telecommunications confidentiality. In particular:

- information acquired incidentally or in the course of one's work, including mere awareness of that information, is to remain confidential;
- it is forbidden to access the university network with the intention of acquiring or manipulating transmitted information, introducing false information or interfering with transmission.
- it is forbidden to access the university network with the intention of gaining unauthorized access to or deliberately interfering with terminal devices on the university network or connected networks, or attempting to do so;

7. Contacts

The legal bases mentioned above can be found in the link directory of the university's Legal Services Office. If you have any questions about data protection, please contact the university's

Legal Services Office
Hochschulstrasse 6
3012 Bern

info@rechtsdienst.unibe.ch

Extensive technical information is available via the link directory of the IT Services Office. If you have any questions about IT security or ISDP, please contact the

IT Services Office
Hochschulstrasse 6
3012 Bern

security@id.unibe.ch

8. Links

[1] https://www.belex.sites.be.ch/frontend/versions/1028

[2] http://id.unibe.ch

[3] https://www.jgk.be.ch/jgk/de/index/direktion/organisation/dsa/formulare_bewilligungen.html

[4] http://id.unibe.ch/rechtssammlung

9. Final provisions

9.1 Conflicting provisions

Any existing provisions which conflict with these directives are hereby repealed.

9.2 Entry into force

The present directives enter into force upon approval.

Bern, 20/08/2019

For the Executive Board of the University of Bern

The Rector:

Prof. Dr. Christian Leumann