UNIVERSITEIT GENT

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

TABLE OF CONTENTS

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

[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

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 of conceptual analysis and vision development on institution-wide themes and dossiers (i.e. prior to a possible decision and approval process)[1].

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[2]: 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.

[1] 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.

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

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.

4.2 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[1]

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

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

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[1]. If the processing potentially involves a high risk, the risks and foreseen measures shall be assessed and documented prior to the processing[2]. 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 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[3] of Ghent University, and in particular the practical guidelines for working safely with IT resources, can be used[4]. 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).

---

[1] 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.

[2] 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.

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

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

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[1].

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[2].

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[3].

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.

[1] 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.

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

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

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[1].

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.

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[2] 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

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

[2] 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).

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).

6 APPLICATIONS AND EXAMPLES

6.1 (ICT) employees

For technical reasons, some employees[1] 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[2].
- 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.

[1] 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).

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

6.2 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[1].

6.3 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 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.

6.4 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**

[1] 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).

and/or leader of the research group and the other participants in the research (possibly also students)[1].

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**[2] 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[3], without prejudice to the specific regulations that apply to the lawful and safe processing of medical data[4].

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 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).

7 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

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

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

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

[4] 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).

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.

8 DATA PROTECTION OFFICER

8.1 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.

8.2 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.