UFSCar
N.º: 116/2025
Processo: 23112.028807/2025-10

Student/Staff Exchange Agreement

between

Universidade Federal de São Carlos

and

Ghent University
Faculty of Arts and Philosophy

In accordance with a mutual desire to promote international academic, cultural and scientific exchange, Ghent University ('UGent'), a public institution with legal personality, duly organised and existing under the special (Flemish) decree of 26 June 1991 on Ghent University and the University Centre of Antwerp (Belgian Official Gazette of 29 June 1991, as amended afterwards), having its registered office at 9000 Ghent, *Sint-Pietersnieuwstraat* 25, with company registration number 248.015.142 (Belgium), represented by prof. dr. Rik Van de Walle, rector, by delegation pursuant to the Board of Governors' decision of June 4, 2021 ('UGent'), and *Universidade Federal de São Carlos* ('UFSCar') enter into this Student/Staff Exchange Agreement ('SEA') Agreement.

Both institutions, for the purpose of furthering cooperation through both educational and academic exchanges, hereby affirm their intent to promote such exchanges as will be of mutual benefit to their institutions. Educational and academic exchanges are considered here to include but not be limited to:

- Development of mutually beneficial academic programmes and courses;
- Exchange of academic staff for the purpose of teaching, training or research;
- Exchange of students for study, internship or research in the framework of a master thesis;
- Reciprocal assistance for visiting academic staff and students;
- Exchange of documentation and pedagogical information

Both parties decide by mutual consent that all possible financial agreements will have to be negotiated and will depend on the availability of funds.

Both parties refer to Annex I (Standard Contractual Clauses and Technical and Organisational Measures). Annex I is incorporated into this agreement and made a part thereof.

A. Student exchange
A.1. Balanced exchange

- Each university may in principle nominate not more than two (2) undergraduate or graduate students for exchange each year. The UGent students going on outbound mobility will originate from the following programmes within the faculty mentioned above: Literature and linguistics. Students going on exchange from UFSCar to UGent will have to choose the majority of courses (ECTS-credits) at the participating faculty in this agreement. A minority of courses (ECTS-credits) can be chosen at any other faculty of UGent[1].

- The Institutions will seek to achieve a fair balance in the number of students exchanged between the two Institutions.

A.2. Screening of the applicants
The home institution will screen applicants according to the admission requirements and language requirements of the host institution. The host institution reserves the right to make a final judgement on the admissibility of each applicant nominated for exchange.

A.3. Nomination and application procedures
Each university will nominate their students in a timely manner, respecting the deadlines of the host institution. At Ghent University, the following nomination and application deadlines apply:

[1] This always needs to be approved by the non-participating faculty(ies).

https://www.ugent.be/prospect/en/administration/application/application-exchange. At UFSCar, the following nomination and application deadlines apply: https://www.srinter.ufscar.br/en/academic-mobility/study-at-ufscar-1/bilateral-agreements.

A.4. Duration of stay
A selected student may study for a period of 1 to 12 months at the host institution.

A.5. Status of exchange students
Each institution shall normally accept incoming exchange students as non-regular students (i.e. students who do not seek to obtain a degree or other formal qualification from the host university).

A.6. Study programme
The following types of mobility are possible under this SEA: study, internship or research in the framework of a master thesis. Each exchange student shall determine the academic activities at the host institution in consultation with academic advisors of both the home institution and the host institution. The academic activities intended will be written down in a Learning Agreement, signed by student, home and host institution before departure. Depending on the study programme, language requirements and/or other prerequisites may be imposed in accordance with the regulations of the host institution. Exchange students will usually be permitted to enter a programme except where such programme is subject to limited enrolments.

A.7. Tuition fees and additional costs
Exchange students participating in the student exchange programme will be exempt from paying tuition and academic fees to the host institution. Exchange students must register/enrol at their home institution and pay the fees required of them by their home institution, if existing, in order to participate in the student exchange programme.

Each exchange student is responsible for the financial costs of the following items during the exchange period:

- costs related to language proficiency testing;
- travel to and from the host institution;
- textbooks, stationery etc.;
- travel documentation, visa requirements etc.;
- accommodation, meals and living expenses;
- applicable student association fees;
- medical/health, personal injury, civil liability, and/or medical and mortal remains repatriation insurance as required by the host institution and country of destination;
- personal travel within the country of destination;
- costs associated with dependents including education and living expenses; and
- all other debts and incidental expenses incurred during the exchange period.

A.8. Recognition of study results
All credits gained during the period of study abroad or during the virtual mobility – as agreed in the Learning Agreement and confirmed by the Transcript of Records – should be transferred without delay and counted towards the student's degree without any additional work by or assessment of the student, in compliance with the rules and procedures in effect at the home institution.

A.9. Visa
The host institution will provide students from the home institution with relevant documentation to assist the exchange students in obtaining a student visa. It remains the individual student's responsibility to obtain visa.

A.10. Accommodation
Both partners will use their best endeavors to assist exchange students in finding accommodation if an exchange student's application is received prior to the relevant application deadline. It remains the responsibility of the individual student to find accommodation.

B. Staff exchange
Both parties hereby agree that:

1. Both parties agree to support the exchange during each academic year of maximum two (2) professors from each university.
2. However, this number may vary in any given year provided a balance of exchanges is attained over the term of the agreement.
3. Each host institution will issue appropriate documents for each visiting staff member for the issuance of a visa, in accordance with current national laws. It is the responsibility of each individual staff member to obtain a visa in their home country in a timely manner.

C. Insurances

Staff and students from UGent going to UFSCar can rely on UGent insurance contracts covering their bodily injury after an accident, covering their liability towards third parties, provided the accident is related to university activities. In the event of a third party claim it is common practice that the third-party liability insurance of the hosting university applies, as during the exchange the student/staff member is under the authority, direction and supervision of the hosting university. The third-party liability insurance of the UGent will therefore only apply provided the relevant insurance of the hosting university does not apply. For accidents in their private life, or if they wish to top up the health insurance of their health fund and/or UGent insurance, staff and students may choose to take out their own insurances.

Staff and students from UFSCar going to UGent should rely on their own insurance contracts, i.e., those put in place by those staff and students themselves, covering their bodily injury after an accident, covering their liability towards third parties, covering medical and mortal remains repatriation. In the event of a third party claim it is common practice that the third-party liability insurance of the hosting university applies, as during the exchange the student/staff member is under the authority, direction and supervision of the hosting university. Although UFSCar cannot put in place insurance contracts for its students and staff members, the liability of UFSCar staff members towards third parties related to university activities is usually covered by UFSCar itself using funds from its own budget. The liability of UFSCar students towards third parties, including related to university activities, will be covered by their own insurances, i.e., those put in place by those students themselves, or by the insurance of the UGent, where the case. For accidents in their private life, or if they wish to top up their health insurance, staff and students may choose to take out their own insurances. There is a legal obligation for all Belgian residents to take out health insurance with one of the Belgian Health funds, if the stay in Belgium is longer than 3 months. In this case staff and students should register with one of the Belgian Health funds upon arrival in Belgium.

D. Academic contact persons

For UGent, Prof. Dr. Renata Enghels (Faculty of Arts and Philosophy) will be the academic contact person responsible for the SEA. For UFSCar, this will be Prof. Dr. Flávia Bezerra de Menezes Hirata-Vale (Department of Language and Literature/Graduate Program on Linguistics).

E. Force Majeure

In this clause a “Force Majeure Event” shall mean circumstances beyond the reasonable control of an institution including, but not limited to, governmental actions, war or national emergency, acts of terrorism, protests, riot, civil commotion, fire, explosion, flood, epidemic, pandemic, lock-outs, strikes or other labour disputes (whether or not relating to either institution’s workforce).

Neither institution will be liable to the other to the extent that it is unable to perform its obligations by reason of a Force Majeure Event, provided the institution so unable to perform promptly notifies the other of the Force Majeure Event and its causes, following which the institutions shall enter into discussions with a view to alleviating its effects or to agree reasonable alternative arrangements.

If a Force Majeure Event continues for more than 30 days, the institution in receipt of such notice may terminate this Agreement by giving 30 days’ notice to the other institution along with return receipt. The institution serving a notice to terminate may withdraw it if the Force Majeure Event ceases during the 30 day notice period.

F. Human rights

The parties guarantee to respect human rights. Each of the parties may terminate this agreement with immediate effect if the other party is involved in a serious or systematic violation of human rights.

G. Intellectual property rights

In case of joint research projects, the intellectual properties generated as a consequence will be subject of a separate agreement between both parties and depending on the material, intellectual and financial contributions of the parties involved.

H. Confidentiality of information

The parties shall take all reasonable steps not to divulge to third parties any confidential data or information acquired in relation to or in the carrying out of the activities foreseen by this agreement.

I. Clause concerning the joint processing of personal data - student exchange

The parties agree that they will act as Joint Controllers for the processing of Personal Data in the context of the implementation of the underlying agreement.

The parties therefore wish to define their rights and obligations with regard to the protection of personal data as established in the European General Data Protection Regulation 2016/679 (hereinafter the "GDPR") of 27 April 2016, as well as in the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (hereinafter the "Personal Data Processing Act");

The terms below are used in the meaning as defined in the GDPR and the Personal Data Processing Act:

1. The parties will process the following Personal Data in the context of the implementation of the underlying agreement: first name – surname – gender – date of birth – nationality – email address – planned start and end date of the mobility – current EQF-level – EQF-level of mobility – area of study – study results.
2. The personal data processed by the parties include the following categories of data subjects: students.
3. The parties undertake to communicate with the Data Subjects in a transparent manner on how they can exercise the rights that are granted to them under the GDPR.

The parties will provide the Data Subjects with the information set out in Articles 13 and 14 of the GDPR by publishing it on an internal platform or website.

4. The parties undertake to respect the confidentiality obligation when processing personal data and to provide each other with the required assistance that is necessary and/or may reasonably be expected to enable them to meet their obligations under the GDPR.
5. In the event that a Data Subject makes any request regarding his or her personal data to a party, the responsibility for the execution of such a request lies with the party receiving the request. The other party shall assist them in this.
6. If the personal data is processed and/or stored outside of the European Economic Area or by an international organisation, and insofar as no adequacy decision applies, the parties must additionally sign the standard clauses drawn up by the European Commission. The processing and storage will always take place in accordance with the GDPR as well as, where applicable, the national legislation of the country where the data is being processed/stored, if that would also apply.
7. The parties shall ensure that appropriate technical and organisational measures are taken to protect the personal data against loss or any form of unlawful processing. The measures to be taken are in line with the available technology.

In the event that there is an infringement with regard to personal data, the party who committed the infringement will be responsible for the communication (if any) to the Data Subject and, if applicable, to the supervisory authority. The party will also notify the other party in writing without unreasonable delay. The party who committed the infringement is obliged to immediately take the appropriate measures at its own expense to stop the infringement and to limit any adverse consequences of the infringement.

8. If a Data Subject or a third party believes to have suffered damage as a result of (unlawful) processing of personal data or failure to fulfil an obligation, the party responsible for processing or complying with the obligation will fully indemnify the other party for this in accordance with the liability rules as established in the GDPR.

If the supervisory authority imposes a fine as a result of an unlawful or negligent act of one party, it will be obliged to indemnify the other party in case they have also been imposed with a fine.

9. Mrs Elisabeth Velle acts as a contact person on behalf of GHENT UNIVERSITY within the context of this Data Processing Agreement.

Mrs Hanne Elsen acts as data protection officer on behalf of GHENT UNIVERSITY in the context of this Data Processing Agreement.

Mrs Andreia Businaro Forim acts as a contact person on behalf of *UNIVERSIDADE FEDERAL DE SÃO CARLOS* in the context of this Data Processing Agreement.

Mr Rogério Fortunato Júnior acts as data protection officer on behalf of the *UNIVERSIDADE FEDERAL DE SÃO CARLOS* in the context of this Data Processing Agreement.

J. Duration of the agreement

This SEA, as well as succeeding plans concerning the concrete proposals of cooperation, shall be effective after signing of the agreement by the appropriate authorities of the universities. It will remain in effect for a period of seven (7) years. At UGent, this means the following academic years/semesters: 2025-2026, 2026-2027, 2027-2028, 2028-2029, 2029-2030, 2030-2031, 2031-32. At UFSCar, this means the following academic years: 2026, 2027, 2028, 2029, 2030, 2031 and 2032.

Thereafter, the collaboration might be prolonged by negotiating and signing a new SEA.

This SEA may be terminated by either partner providing six (6) months written notice to the other partner along with return receipt. In the event of early termination hereof, eventually ongoing educational and academic exchanges will be duly concluded.

K. Dispute resolution

All disputes concerning the interpretation and application of this agreement shall be settled through mutual negotiations between the parties. If the parties cannot resolve the dispute, such dispute will be submitted to an alternative solution, subject to the rules that the parties decide to adopt. The applicable law to the interpretation and application of this agreement is the Belgian law.

L. Translation

UFSCar requests a translation of the current agreement in Portuguese. In case of any conflicts between the English and Portuguese version, the English version will prevail.

If a dispute arises the parties will continue to carry out all their respective obligations under this agreement that are not directly affected by the dispute.

For Ghent University

Rik Van de Walle

Digitally signed by Rik Van de Walle
Date: 2025.09.05 11:35:50 +02'00'

Prof. dr. Rik Van de Walle
Rector

Date: ……..

For UFSCar

ASSINADO DIGITALMENTE
ANA BEATRIZ DE OLIVEIRA
A conformidade com a assinatura pode ser verificada em:
http://serpro.gov.br/assinador-digital
SERPRO

Prof. dr. Ana Beatriz de Oliveira
Rector

Date: September 9, 2025 ……..

ANNEX I to the Student/Staff Exchange Agreement

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

1.1.1.1 Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[2] for the transfer of personal data to a third country.
(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), an
(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")
have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

1.1.1.2 Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

1.1.1.3 Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8 - Module One: Clause 8.5(e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1(b) and Clause 8.3(b);
(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
(v) Clause 13;

[2] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

1.1.1.4 Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

1.1.1.5 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

1.1.1.6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

1.1.1.7 Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

1.2.1.1 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;
(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;
(ii) of the categories of personal data processed;
(iii) of the right to obtain a copy of these Clauses;
(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organizational measures to ensure compliance with this obligation, including erasure or anonymization[3] of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural

[3] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

Not applicable.

Clause 10
Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[5] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

[5] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

Clause 11

1.2.1.2 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[6] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

1.2.2 Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C., shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these

[6] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.
(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
(ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[7];
(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter

[7] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whethertheir practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

1.4.1.1 Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
(ii) the data importer is in substantial or persistent breach of these Clauses; or
(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.
In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

1.4.2 Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Belgium.

Clause 18

1.4.3 Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) The Parties agree that those shall be the courts of Belgium.
(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

1.5 ANNEX I

A. LIST OF PARTIES

Data exporter(s):
Name: *UNIVERSIDADE FEDERAL DE SÃO CARLOS.* Address: 235km Washington Luís Highway, 13565-905 São Carlos, State of São Paulo, Brazil.

Contact person's name, position and contact details: Rogério Fortunato Júnior; Head, Office of Institutional Planning and Development; Data Protection Officer; secretario.spdi@ufscar.br; spdi@ufscar.br.

Activities relevant to the data transferred under these Clauses: student and teaching staff exchange

Role (controller/processor): joint controller of personal data

Signature and date:

Data importer(s):
GHENT UNIVERSITY, a public institution with legal entity status, established pursuant to the special decree of 26 June 1991 concerning Ghent University and University Centre Antwerp (published in the Belgian Official Journal on 29 June 1991, as subsequently amended), with its registered office at 9000 Ghent, *Sint-Pietersnieuwstraat* 25, and KBO (Crossroads Bank for Enterprises) number 0248.015.142.

Privacy statement: https://www.ugent.be/en/ghentuniv/privacy/privacystatement.htm

Data Protection Officer: Hanne Elsen (hanne.elsen@ugent.be)

Activities relevant to the data transferred under these Clauses: student and teaching staff exchange

Role (controller/processor): joint controller of personal data

B. DESCRIPTION OF TRANSFER *Categories of data subjects whose personal data is transferred*

Data subjects
The personal data transferred concern the following categories of data subjects: exchange students in the framework of an exchange agreement between Ghent University and a partner university outside of the Erasmus area.

Purposes of the transfer(s)
The transfer is made for the following purposes: international student exchange

Categories of data
The personal data transferred concern the following categories of data: first name – surname – gender – date of birth – nationality – email address – planned start and end date of the mobility – current EQF-level – EQF-level of mobility – area of study – study results

Recipients
The personal data transferred may be disclosed only to the following recipients or categories of recipients: at Ghent University: Direction of Educational Affairs (including the central International Relations Office), relevant personnel working with internationalisation in the faculty or department involved.

Sensitive data (if appropriate)
The personal data transferred concern the following categories of sensitive data: not applicable

Data protection registration information of data exporter (where applicable): not applicable

Additional useful information (storage limits or other relevant information): not applicable

Contact points for data protection enquiries

Data importer Contact: Data Protection Officer: Hanne Elsen (Hanne.Elsen@ugent.be)

Data exporter Contact: Data Protection Officer: Rogério Fortunato Júnior (secretario.spdi@ufscar.br; spdi@ufscar.br)

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13
The Data Protection Authority: https://www.dataprotectionauthority.be/citizen

ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

INFORMATION SECURITY

TECHNICAL AND ORGANIZATIONAL MEASURES AT GHENT UNIVERSITY

Non-confidential, version dd. 17 February 2022

1 INTRODUCTION

The following overview contains a number of strategies and measures for an optimal guarantee of data and information security at Ghent University. It lists measures Ghent University takes to guarantee the integrity, availability, confidentiality and cyber resilience, as well as the non-repudiation, the authenticity of information and the auditability of information processing systems. This is a non-exhaustive overview, meaning that not all the measures taken are listed.

2 GENERAL SECURITY POLICY AND ORGANIZATION OF INFORMATION SECURITY

2.1 Information Security Policy

Ghent University has a modular data protection and information security policy. The various modules of this policy have been built up gradually in recent years. The policy as a whole is assessed annually and updated where necessary.

The policy has been adapted to the context of Ghent University, it is in accordance with the provisions of the applicable legislation and relevant decrees, and of the General Data Protection Regulation.

Ghent University's information security policy includes:

- procedures for protecting the information data contained in electronic messages;
- procedures for protection against data loss;
- malware protection procedures (updated antivirus, firewall, ...);
- a user access management policy that restricts access to systems and services to authorized users and prevents unauthorized access;
- an appropriate password policy;
- procedures for protecting access to the servers;
- procedures for protecting access to the network;
- procedures for the protection of the work stations;
- procedures regarding the classification of information data according to their value or their critical or sensitive nature in the event of modification or unauthorized disclosure , and regarding the consequences of the classification.

The IT infrastructure for digital preservation of highly confidential data is protected against any known risk of individual intrusion and against unauthorized access to the information it contains. Any form of individual intrusion or unauthorized access to the files is detected. In the event of such a detection, the necessary countermeasures, including alarms, come into immediate effect. This security system functions independently of the computer systems used for digital storage of these highly confidential data.

2.2 IT Security Officer

Ghent University has appointed an IT Security Officer. The IT Security Officer is responsible for IT security and for information and data protection. The IT Security Officer is a permanently invited expert in Ghent University’s ICT Committee and is a member of the Privacy and Data Protection Committee. The IT Security Officer reports to the Director of the ICT Department.

2.3 Data Protection Officer

Ghent University has appointed a Data Protection Officer. The Data Protection Officer is responsible for internal supervision of compliance with the GDPR and national data protection regulations. To this end, the Data Protection Officer collaborates with the IT Security Officer, and is assisted by a Privacy and Data Protection Committee with representatives from all levels of the university. The Data Protection Officer reports to the Director of the Administrative Affairs Department and to the Vice-chancellor.

2.4 Information Security and Data Protection Responsibilities

Responsibilities of Ghent University staff are documented and published formally in the modular data protection and information security policy.

Important documents are the “Generic Code of Conduct for Personal Data and Confidential Information Processing” and the “Regulations for the Acceptable Use of Ghent University’s ICT Infrastructure” (i.e. the Acceptable Use Policy).

2.5 Risk Analysis, Management and Control

Ghent University carries out periodical risk analyses of its security measures and checks their compliance with the various information security procedures.

As far as central IT services are concerned, this is the responsibility of the IT Security Officer, in collaboration with the ICT Department and the Data Protection Officer.

General risk management in the field of data protection and IT security is subject to selective audits by Ghent University's Internal Audit Service. Results of such audits are communicated to Ghent University's Audit Committee and the Board of Governors.

As far as the decentralized IT applications are concerned, risk management is a shared responsibility of the IT Security Officer and decentralized IT administrators. Ghent University's modular information security policy provides guidelines for IT administrators and IT end users for information security risk management.

3 SECURE PERSONNEL POLICY

3.1 Training Sessions on the Importance of Security and Handling of Personal Data

Ghent University regularly communicates about the importance of information security to all staff and students. Online training modules are made available to staff members. Where necessary, specific training and/or information sessions are organized, for example for new employees.

Ghent University's system engineers (ICT Department) take a thorough training upon recruitment. Additional training sessions are provided at regular intervals to ensure that their knowledge remains accurate and up-to-date.

3.2 Authorizations

Ghent University implements and maintains authentication and authorization management systems to control access to systems containing personal data. Where possible, role-based authorizations are used.

At a minimum, logical access to each information system is secured with strictly personal credentials (username/password). Authentication and authorizations are always based on the information that is present in redundantly designed central repositories (LDAP and AD, partly on-prem, partly in cloud with AAD in a hybrid setup).

Account granting and authorization is based solely on board-approved rules, and is linked directly to primary staff and student management resources. They expire automatically when the individual's statute expires. The rules for correct use of the personal credentials and account are laid down in Ghent University's Acceptable Use Policy.

3.3 Segregation of Duties

Ghent University applies segregation of duties as much as possible to prevent individuals from gaining access to data they do not need to carry out their duties. This is technically enforced where possible.

4 PHYSICAL SECURITY OF WORK AND OFFICE SPACE

Ghent University restricts access to work and office space where personal data or confidential information is processed pursuant to its mandate. Where necessary and based on risk analysis, access is strictly limited to identified and authorized individuals. Burglary protection and/or badge readers are installed to prevent unauthorized access where necessary.

Managing and securing physical access to Ghent University premises is the responsibility of the Security Co-ordinator at Ghent University's Emergency Centre.

5 DATA CENTRE SECURITY

5.1 Introduction

The data of Ghent University's various central server and storage systems is part of information systems in two separate data centres located in Ghent. The primary data centre is located at Campus Sterre, the secondary data centre at Campus Ardoyen.

5.2 Physical Data Centre Security

Physical access to our own data centres is strictly managed and controlled, and secured according to industry standards, including video surveillance and intruder alarms.

Access to the data rooms is secured by badge readers. The server rooms in each data centre are only accessible to authorized Ghent University system engineers. If external parties need physical access to one of the data centres, this is always done in the presence and under the supervision of a Ghent University

system engineer (ICT Department). Badges are issued in accordance with a strict physical identification process, and each staff member must register in person to obtain their badge. All entrances can be read centrally so that entrance to the rooms can be checked at any time.

Each data centre is equipped with fire extinguishers. In the event of a fire, the fire can be extinguished with minimal impact on the IT systems. The temperature and humidity in the rooms is measured continuously. The system sounds the alarm when certain threshold values are exceeded.

For applications and data that are hosted in external cloud systems, an analysis is made beforehand to determine whether the associated risks are sufficiently under control and acceptable.

5.3 Redundancy

All facilities and services in our own data centres are protected against unforeseen failures with sufficient redundancy.

Each data centre is equipped with professional installations to guarantee continuity of power supply (by means of UPS installations and diesel generators) and cooling (by means of redundant cooling machines and fans).

In addition to the primary data centre, Ghent University also has a fail-over data centre. The most critical information systems are redundantly designed over the two data centres, so that in the event of a failure of a single system or even the loss of an entire data centre, the operational functioning of various crucial services at Ghent University can still be provided.

5.4 Disaster Recovery Planning

Ghent University has disaster recovery plans to minimize downtime in the event of disasters involving the IT infrastructure in the central data centres. The disaster recovery plans are updated regularly and the emergency scenarios are in principle tested and assessed annually.

A dual backup and restore strategy, based on snapshot technology and data replication on the one hand, and daily backup copies on the other, guarantees that data loss in the event of a disaster in one of the centres is kept to a minimum. Backups are taken on specific backup storage systems. An identical copy of all backup data is kept in both data centres.

6 INTERNAL NETWORK SECURITY

Ghent University's internal network (UGentNet) is highly compartmentalized and equipped with advanced control mechanisms (firewall, intrusion detection & prevention) that protect the internal network appropriately against unauthorized access and unwanted actions from outside. To this end, Ghent University collaborates with its Internet Service Provider Belnet.

Up-to-date encryption protocols are used for the wireless networks to provide maximum protection for the transferred data.

7 SECURITY OF DATA AT REST

7.1 Data Encryption

Ghent University’s data storage policy stipulates that digital personal data and confidential information must be stored on centrally provided storage options. External cloud services must not be used to store high-risk data, unless the data is encrypted beforehand (i.e. client-side) in a secure and reliable manner with cryptographic tools.

7.2 Antivirus and Security Updates

Fixed and mobile user equipment is protected by up-to-date antimalware tools. Ghent University provides its central IT systems and user equipment with the latest security updates under central management. These are followed up as closely as possible and installed according to a reliable patch management process.

7.3 Malicious Software

Ghent University performs anti-malware checks to prevent malicious software from causing damage, e.g. gaining unauthorized access or making access to its own data impossible (protection against ransomware).

7.4 Access Logs

ICT system administrators log and monitor access to Ghent University's ICT infrastructure to ensure its proper functioning and to detect and prevent abuse. The level of detail is no more and the retention time no longer than necessary to achieve this goal.

Depending on the type of data or information and their degree of confidentiality, the logging is less or more detailed. For critical information systems, access and actions are logged extensively. Logging information is confidential and can only be released after a formal request accepted by university management (e.g. a court order).

8 SECURITY OF DATA IN MOTION

Ghent University uses up-to-date encryption protocols (TLS, HTTPS, VPN) for the transmission of data inside and outside the Ghent University network.

9 GHENT UNIVERSITY ACCOUNT SECURITY

Ghent University accounts are protected by a password that must be renewed at least annually. The passwords must have a certain level of complexity. These requirements are also enforced technically. All Ghent University accounts are secured with an additional multifactor authentication.

10 IT SYSTEMS AND SERVER SECURITY

Ghent University applies risk management to the security of all its IT systems. Critical systems and critical applications are subject to a regular safety test by an independent third party. The requirements for data and systems protection are also analysed and specified where necessary in collaboration with IT suppliers.

11 INCIDENT MANAGEMENT

All centrally managed information systems are monitored continuously. The ICT Department has a 24/24 and 7/7 on-call service to be able to intervene immediately in the event of a malfunction.

For the triage and handling of incidents, the ICT Department has developed a scenario for all IT incidents, including those involving personal data. When Ghent University acts as a personal data processor, and in the event of a data security incident that has a significant impact on the confidentiality or integrity of that personal data, Ghent University will inform the Data Protection Officer (and any other interested parties) without undue delay.

Incident management is registered and monitored by a central management system. A monthly incident report is drawn up, including every occurrence, their impact and solution, and lessons learnt.

To minimize the chance of incidents, fixed maintenance windows are scheduled to perform the necessary proactive maintenance activities. In case of urgent maintenance work, urgency maintenance windows are scheduled. During such a maintenance window (a group of) systems may be temporarily unavailable. Each maintenance window (and its possible impact) are therefore widely announced throughout the organization (via intranet).

12 ADDITIONAL MEASURES

The above elements describe Ghent University's general, centrally co-ordinated IT services security policy. Based on a more detailed risk analysis, additional appropriate measures are taken for specific processing operations on central or decentralized IT infrastructure, in particular in the context of research projects involving personal data or confidential information.