

FIRST ADDENDUM TO THE
INTERNATIONAL COOPERATION
AGREEMENT Nº 037/2021 – UFLA,
BETWEEN THE FEDERAL
UNIVERSITY OF LAVRAS AND THE
INSTITUT POLYTECHNIQUE DE
GRENOBLE.

PRIMEIRO TERMO ADITIVO AO
ACORDO DE COOPERAÇÃO
INTERNACIONAL Nº 037/2021 – UFLA,
QUE ENTRE SI CELEBRAM A
UNIVERSIDADE FEDERAL DE LAVRAS
E O INSTITUT POLYTECHNIQUE DE
GRENOBLE.

I

I

The **FEDERAL UNIVERSITY OF LAVRAS** located in the city of Lavras, in the state of Minas Gerais, Brazil, University *Campus* hereinafter **UFLA**, herein represented by its Director for International Affairs Professor **Antonio Chalfun Junior**, by act of delegation of powers, according to Ordinance nº 287, of 11/04/2022 and the **INSTITUT POLYTECHNIQUE DE GRENOBLE**, located in Grenoble, France hereinafter referred to as **Grenoble INP**, herein represented by its President, **Pierre Benech**, agree to celebrate the present First Addendum to the International Cooperation Agreement nº 037/2021 - UFLA, signed between the participants on 24/11/2021, which will be governed by the terms and conditions explained below:

A **UNIVERSIDADE FEDERAL DE LAVRAS**, com sede na cidade de Lavras, Estado de Minas Gerais, Brasil, *Campus* Universitário, doravante denominada **UFLA**, neste ato representada por seu Diretor de Relações Internacionais, Professor **Antonio Chalfun Junior**, por ato de delegação de competência, conforme a Portaria nº 287, de 11/04/2022 e o **INSTITUT POLYTECHNIQUE DE GRENOBLE**, com sede na cidade de Grenoble, França, doravante denominado **Grenoble INP**, neste ato representada por seu Presidente, **Pierre Benech**, resolvem celebrar o presente Primeiro Termo Aditivo ao Acordo de Cooperação Internacional nº 037/2021 – UFLA, firmado entre as partes em 24/11/2021, que reger-se-á mediante as cláusulas e condições a seguir explicitadas:

II

II

The present Instrument has as object the **INCLUSION** of an annex regarding the use of personal data to the International Cooperation Agreement nº 037/2021 – UFLA, signed between the two institutions on 24/11/2021, under the terms provided in its article 14 (fourteen).

O presente Instrumento tem por objeto a **INCLUSÃO** de um anexo referente ao uso de dados pessoais ao Acordo de Cooperação Internacional nº 037/2021 – UFLA, firmado entre as partes em 24/11/2021, nos termos previstos em seu artigo 14 (quatorze).

III

III

The remaining clauses of the International Cooperation Agreement nº 037/2021 - UFLA, that were not explicitly altered, remain in force.

As demais cláusulas do Acordo de Cooperação Internacional nº 037/2021 – UFLA, que aqui não foram expressamente alteradas, permanecem em vigor.



The undersigned being duly authorized by their respective institutions approve this document made and duplicated in copies of equal content and form.

Os abaixo signatários devidamente autorizados por suas respectivas Instituições aprovam o presente documento confeccionado e duplicado em vias de igual teor e forma.

Grenoble, 26/09/2022



Pierre Benech
President
Institut Polytechnique Grenoble

Lavras, 17/11/2022



Antonio Chalfun Junior
Diretor de Relações Internacionais
Universidade Federal de Lavras



Antonio Chalfun Junior
Director of International Relations
Federal University of Lavras

Pierre Benech
Presidente
Institut Polytechnique Grenoble



ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 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) 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'), and
 - 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

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 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.

N

Clause 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, Clause 8.5 (e) and Clause 8.9 (b);
 - iii) Clause 12 (a) and (d) ;
 - iv) Clause 13;
 - v) Clause 15.1(c), (d) and (e);
 - vi) Clause 16(e);
 - vii) Clause 18(a) and (b)
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 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

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

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

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

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 organisational 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 organisational measures to ensure compliance with this obligation, including erasure or anonymisation ⁽¹⁾ 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

¹ 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.

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 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 ⁽²⁾ (in the same country as the data importer or in another third country, hereinafter 'onward

² 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.

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.

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

Without object

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. ⁽³⁾ 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 lay 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.

³ 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.

- (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.

Clause 11

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.
- (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

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 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 ⁽⁴⁾;
 - 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

⁴ 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 whether their 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.

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 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

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

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 France.

Clause 18

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 France.
- (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

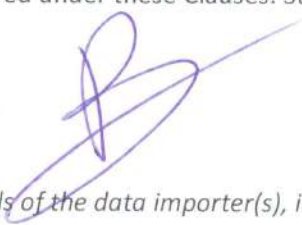
ANNEX I

A. LIST OF PARTIES

Contact Point for data protection enquiries:

- Grenoble INP – UGA: dpo@grenoble-inp.fr
Bâtiment DSIM Domaine universitaire
31, rue des mathématiques
38400 Saint-Martin-d'Hères
33 (0)4 56 52 90 44
- Universidade Federal de Lavras - UFLA: dri@ufla.br
Campus Universitário 3037
37200-900 | Lavras, MG | Brasil
+55 35 3829-1858

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: Institut Polytechnique de Grenoble (**Grenoble INP – UGA**) represented by Prof. Pierre Benech, President.
Address: 46 avenue Felix Viallet 38031 Grenoble France
Activities relevant to the data transferred under these Clauses: Student's mobility informations
Role (controller/processor): Controller
Signature and date: 26/09/2022 

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: Universidade Federal de Lavras (UFLA) represented by prof. Antonio Chalfun Junior, Director of International Relations.
Address: Campus Universitário 3037 | 37200-900 | Lavras, MG, Brasil
Contact person's name, position and contact details: Office of International Affairs - dri@ufla.br
Activities relevant to the data transferred under these Clauses: Student's mobility information
Role (controller/processor): Controller
Signature and date:  17/11/2022

This Annex is in English and Portuguese. English is the negotiating language of this Agreement. Any translation shall be faithful to the English version.

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred:

- Exchange students from Grenoble INP – UGA
- Exchange students from UFLA

2. Categories of personal data transferred:

For Grenoble INP – UGA:

- a. Gender, Last Name, First name, postal address, phone number and email, date and place of birth, citizenship of the Exchange Students, copy of Exchange Students passport
- b. Transcript of grades, previous degrees obtained, Resume/CV, contact information for the school or university
- c. Proof of English Language Proficiency
- d. Emergency contact information: Name, postal address, phone number

For UFLA:

- a. Contact information;
- b. Financial information;
- c. Educational data, including exam results and evaluations.

3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive data transferred

4. The frequency of the transfer:

Once a year and depending of the academic period (FY or semester)

5. Nature of the processing

Students' data transfer for his/her nomination before his/her mobility

6. Purpose(s) of the data transfer and further processing

Ensure the students' international mobility during his/her curriculum and process to data analysis.

7. The period for which the personal data will be retained:

Personal data will be retained during the students' mobility duration and the mobility agreements duration.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority in accordance with Clause 13 is the CNIL.



ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Technical & Organisational measure for Grenoble INP

- Technical security measures:

- Datacenters protected by restricted access; fire fighting system with sirens, plus manual extinguishers, automatic extinguishing; redundancy of power supply and air conditioning
- Data backup on remote site
- Access to workstations with login and password
- Anti-virus solutions on workstations and servers
- Access to applications with login and password, logged
- User rights management
- Deployment of security patches on software and operating systems, consolidation of system configurations, systems and network monitoring
- Use of firewalls and network segmentation
- Encryption of exchanges (HTTPS / SSL), remote access via encrypted VPN

- Organisational security measures:

- Data protection officer (DPO), Information Systems Security Manager (ISSM)
- Register of personal data processing activities
- Incident management procedures
- Privacy impact assessments for processing operations posing a significant risk to the privacy of data subjects
- Charter for the use of computer and communication resources relevant by all employees; Charter for IT people
- Information and awareness (employee intranet, welcoming new staff) about Privacy and good practices

Technical & Organisational measure for UFLA:

Ordinance N°. 1896, of December 23, 2020

(https://sistemaslegados.ufla.br/documentos/arquivos/21_1896_23122020.pdf): which regulates the technical measures to ensure data security, guarantees the protection of personal data collected and or kept in physical and electronic databases of the Federal University of Lavras, in compliance with *Law N°. 13.709 of 2018* (http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm).

Handwritten signature

ANEXO

CLÁUSULAS CONTRATUAIS PADRÃO

SEÇÃO I

Cláusula 1

Finalidade e âmbito

- a) O objetivo destas cláusulas contratuais padrão é garantir o cumprimento dos requisitos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, sobre a proteção de pessoas físicas no que diz respeito ao tratamento de dados pessoais e sobre a livre circulação de tais dados (Regulamento Geral de Proteção de Dados) para a transferência de dados pessoais para um país terceiro.
- b) Os Partícipes:
- i) a(s) pessoa(s) física(s) ou jurídica(s), autoridade(s) pública(s), agência(s) ou outro(s) organismo(s) (doravante denominado "entidade(s)") que transfere os dados pessoais, conforme listado no Anexo I.A (doravante, cada "exportador de dados"), e
 - ii) a(s) entidade(s) de um terceiro país que está recebendo os dados pessoais do exportador de dados, direta ou indiretamente, por meio de outra entidade também Partícipe destas Cláusulas, conforme listado no Anexo I.A (doravante, cada "importador de dados") concordaram com estas cláusulas contratuais padrão (doravante: "Cláusulas").
- c) Estas Cláusulas se aplicam à transferência de dados pessoais conforme especificado no Anexo I.B.
- d) O Apêndice a estas Cláusulas contendo os Anexos nele referidos é parte integrante destas Cláusulas.

Cláusula 2

Efeito e invariabilidade das Cláusulas

- a) Estas Cláusulas estabelecem garantias adequadas, incluindo os direitos aplicáveis dos titulares dos dados e soluções legais eficazes, nos termos do Artigo 46(1), e do Artigo 46(2)(c), do Regulamento (UE) 2016/679 e, no que diz respeito às transferências de dados dos controladores para processadores e / ou processadores para processadores, cláusulas contratuais padrão nos termos do Artigo 28(7) do Regulamento (UE) 2016/679, desde que não sejam modificadas, exceto para selecionar o(s) Módulo(s) apropriado(s) ou para adicionar ou atualizar informações no Apêndice. Os Partícipes não são impedidos de incluir as Cláusulas contratuais padrão, estabelecidas nessas Cláusulas, em um acordo mais amplo e/ou adicionar outras Cláusulas ou garantias adicionais, desde que não contradigam, direta ou indiretamente, essas Cláusulas ou prejudiquem os direitos fundamentais ou liberdades dos titulares dos dados.
- b) Estas cláusulas não prejudicam as obrigações às quais o exportador de dados está sujeito em virtude do Regulamento (UE) 2016/679.



Cláusula 3
Terceiro beneficiário

- a) Os titulares dos dados podem recorrer e aplicar estas Cláusulas, como terceiro beneficiários, contra o exportador de dados e/ou importador de dados, com as seguintes exceções:
- i) Cláusula 1, Cláusula 2, Cláusula 3, Cláusula 6, Cláusula 7;
 - ii) Cláusula 8, Cláusula 8.5 (e) e Cláusula 8.9 (b);
 - iii) Cláusula 12 (a) e (d);
 - iv) Cláusula 13;
 - v) Cláusula 15.1(c), (d) e (e);
 - vi) Cláusula 16(e);
 - vii) Cláusula 18 (a) e (b).
- b) Parágrafo (a) não prejudica os direitos dos titulares dos dados sob o Regulamento (EU) 2016/679.

Cláusula 4
Interpretação

- a) Sempre que estas Cláusulas utilizarem os termos definidos no Regulamento (UE) 2016/679, esses termos terão o mesmo significado do Regulamento.
- b) As presentes Cláusulas devem ser lidas e interpretadas à luz das disposições do Regulamento (UE) 2016/679.
- (c) As presentes Cláusulas não devem ser interpretadas de forma a entrar em conflito com os direitos e obrigações previstos no Regulamento (UE) 2016/679.

Cláusula 5
Hierarquia

Em caso de contradição entre estas Cláusulas e as disposições dos acordos entre os Partícipes existentes no momento em que estas Cláusulas forem acordadas, ou celebradas posteriormente, as Cláusulas prevalecerão.

Cláusula 6
Descrição da(s) transferência(s)

Os detalhes da(s) transferência(s), em particular a categoria de dados pessoais transferidos e os fins para os quais são transferidos, são especificados no Anexo I.B.

Cláusula 7
Cláusula de adesão

- a) Uma entidade que não seja parte destas Cláusulas pode, com o consentimento dos Partícipes, aderir a estas Cláusulas a qualquer momento, seja como exportador de dados ou como importador de dados, preenchendo o Apêndice e assinando o Anexo I.A.
- b) Depois de preencher o Apêndice e assinar o Anexo I.A, a entidade aderente se tornará parte destas Cláusulas e terá os direitos e obrigações de um exportador ou importador de dados de acordo com sua designação no Anexo I.A.
- c) A entidade aderente não terá direitos ou obrigações decorrentes destas Cláusulas no período anterior a se tornar um Partícipe.

SEÇÃO II - OBRIGAÇÕES DOS PARTÍCIPIES

Cláusula 8
Garantia de proteção de dados

O exportador de dados garante que empregou esforços necessários para determinar se o importador de dados é capaz, por meio da implementação de medidas técnicas e organizacionais apropriadas, de cumprir suas obrigações sob estas Cláusulas.

8.1 Finalidade limitada

O importador de dados deve processar os dados pessoais apenas para os fins específicos de transferência, conforme estabelecido no Anexo I.B. Ele só poderá processar os dados pessoais para outra finalidade:

- i) quando obtiver o consentimento prévio do titular dos dados;
- ii) quando necessário para o estabelecimento, exercício ou defesa de ações judiciais no contexto de procedimentos administrativos, regulamentares ou judiciais específicos; ou
- iii) se necessário, para proteger os interesses vitais do titular dos dados ou de outra pessoa física.

8.2 Transparência

(a) A fim de permitir que os titulares dos dados exerçam efetivamente seus direitos de acordo com a Cláusula 10, o importador de dados deve informá-los, diretamente ou por meio do exportador de dados:

- i) de sua identidade e detalhes de contato;
- ii) das categorias de dados pessoais processados;
- iii) do direito de obter uma cópia destas Cláusulas;
- iv) quando tiver a intenção de transferir os dados pessoais, para qualquer terceiro, do destinatário

ou categorias de destinatários (conforme apropriado, visando fornecer informações significativas), informar a finalidade dessa transferência posterior e o fundamento, portanto, de acordo com a Cláusula 8.7.

- (b) O parágrafo (a) não se aplica quando o titular dos dados já possuir as informações, inclusive quando tais informações já forem fornecidas pelo exportador de dados, ou quando o fornecimento das informações for impossível ou envolver um esforço desproporcional para o importador de dados. Neste último caso, o importador de dados deve, na medida do possível, disponibilizar as informações ao público.
- (c) Mediante solicitação, os Partícipes disponibilizarão gratuitamente ao titular dos dados uma cópia destas Cláusulas, incluindo o Apêndice conforme preenchido por elas. Na medida do necessário para proteger segredos comerciais ou outras informações confidenciais, incluindo dados pessoais, os Partícipes podem editar parte do texto do Apêndice antes de compartilhar uma cópia, mas devem fornecer um resumo significativo caso o titular dos dados não seja capaz de compreender seu conteúdo ou exercer seus direitos. Mediante solicitação, os Partícipes fornecerão ao titular dos dados os motivos das retificações, na medida do possível, sem revelar as informações retidas.
- (d) Os parágrafos (a) e (c) não prejudicam as obrigações do exportador de dados sob os Artigos 13 e 14 do Regulamento (UE) 2016/679.

8.3 Precisão e minimização de dados

- (a) Cada Partícipe assegurará que os dados pessoais sejam exatos e, quando necessário, atualizados. O importador de dados deve tomar todas as medidas plausíveis para garantir que os dados pessoais inexatos, considerando a(s) finalidade(s) do processamento, sejam apagados ou retificados sem demora.
- (b) Se um dos Partícipes tomar consciência de que os dados pessoais que transferiu e recebeu são inexatos ou desatualizados, deve informar o outro Partícipe sem atraso indevido.
- (c) O importador de dados deve garantir que os dados pessoais são adequados, relevantes e limitados ao que é necessário em relação ao (s) objetivo (s) do processamento.

8.4 Limitação de armazenamento

O importador de dados deve reter os dados pessoais por tempo não mais que o necessário para os fins pelos quais são processados. Deve pôr em prática medidas técnicas ou organizacionais adequadas para garantir o cumprimento desta obrigação, incluindo o apagamento ou anonimização¹ dos dados e todas as cópias de segurança no final do período de retenção.

8.5 Segurança do processamento

- (a) O importador de dados e, durante a transferência, também o exportador de dados, devem implementar medidas técnicas e organizacionais adequadas para garantir a segurança dos dados pessoais, incluindo proteção contra uma violação de segurança que leva à destruição acidental ou ilegal, perda, alteração, divulgação ou acesso não autorizado (doravante 'violação de dados

¹ É necessário tornar os dados anônimos de forma que o indivíduo deixe de ser identificável por qualquer pessoa, em conformidade com o item 26 do Regulamento (UE) 2016/679, e este processo deve ser irreversível.

personais¹). Ao avaliar o nível de segurança apropriado, eles devem levar em consideração o estado da técnica, os custos de implementação, a natureza, o escopo, o contexto e a finalidade(s) do processamento, e os riscos para o titular dos dados envolvendo o processamento. Os Partícipes deverão, em particular, considerar recursos para encriptação ou pseudonimização, incluindo durante a transferência, quando o propósito do processamento puder ser cumprido dessa forma.

- (b) Os Partícipes concordaram sobre as medidas técnicas e organizacionais estabelecidas no Anexo II. O importador de dados deve realizar controles regulares para garantir que essas medidas continuem a proporcionar um nível de segurança adequado.
- (c) O importador de dados deve garantir que as pessoas autorizadas a processar os dados pessoais se comprometam com a confidencialidade, ou estejam sob uma obrigação legal de confidencialidade adequada.
- (d) Em caso de violação de dados pessoais relativos ao processamento pelo importador de dados sob essas Cláusulas, o importador de dados deve tomar as medidas adequadas para resolver a violação, incluindo medidas para mitigar os seus possíveis efeitos adversos.
- (e) Em caso de violação de dados pessoais que possa resultar em risco para os direitos e liberdade das pessoas físicas, o importador de dados deve, sem atraso indevido, notificar tanto o exportador de dados quanto a autoridade supervisora competente de acordo com a Cláusula 13. Tal notificação deve conter i) uma descrição da natureza da violação (incluindo, quando possível, categorias e número aproximado de titulares de dados e registros de dados pessoais em questão), ii) suas prováveis consequências, iii) as medidas tomadas ou propostas para lidar com a violação, e iv) os detalhes de um contato do qual mais informações podem ser obtidas. No caso de não ser possível para o importador de dados fornecer todas as informações ao mesmo tempo, ele pode fazê-lo em partes, sem atrasos indevidos.
- (f) No caso de uma violação de dados pessoais que possa resultar em um alto risco para os direitos e liberdade das pessoas físicas, o importador de dados deve também notificar, sem atrasos indevidos, os titulares dos dados em causa sobre a violação de dados pessoais e sua natureza, se necessário em cooperação com o exportador de dados, juntamente com as informações referidas no parágrafo (e), pontos ii) a iv), a menos que o importador de dados tenha implementado medidas para reduzir significativamente o risco para os direitos ou liberdade das pessoas físicas, ou no caso da notificação envolver esforços desproporcionais. Neste último caso, o importador de dados deve, em vez disso, emitir uma comunicação pública ou tomar uma medida semelhante para informar o público da violação de dados pessoais.
- (g) O importador de dados deve documentar todos os fatos relevantes relacionados à violação de dados pessoais, incluindo seus efeitos e qualquer ação corretiva tomada, e manter um registro dos mesmos.

8.6 Dados confidenciais

Quando a transferência envolver dados pessoais que revelam origem racial ou étnica, opiniões políticas, crenças religiosas, filosóficas ou filiação em sindicatos, dados genéticos ou dados biométricos com o objetivo de identificar de forma única uma pessoa física, dados relativos à saúde ou à vida sexual de uma pessoa, orientação sexual ou dados relativos a condenações criminais ou infrações, (a seguir designados «dados confidenciais»), o importador de dados deve aplicar restrições específicas e/ou garantias adicionais adaptadas à natureza específica dos dados e aos riscos envolvidos. Isso pode incluir a restrição do pessoal autorizado a acessar os dados pessoais, medidas

de segurança adicionais (como pseudonimização) e/ou restrições adicionais relativas à divulgação posterior.

8.7 Transferências posteriores

O importador de dados não divulgará os dados pessoais a terceiros localizados fora da União Europeia² (no mesmo país que o importador de dados ou em outro país terceiro, doravante denominado "transferência posterior"), a menos que o terceiro seja um Partícipe ou concorde em ser regido por estas Cláusulas, sob o Módulo apropriado. Caso contrário, uma transferência posterior pelo importador de dados só pode ocorrer se:

- i) for para um país beneficiado uma decisão de adequação nos termos do A45.º do Regulamento (UE) 2016/679 que abrange a transferência posterior;
- ii) o terceiro garantir de outra forma proteção adequada aos termos dos Artigos 46.º ou 47.º do Regulamento (UE) 2016/679 no que diz respeito ao tratamento em questão;
- iii) o terceiro celebra um instrumento vinculativo com o importador de dados, garantindo o mesmo nível de proteção de dados que estas Cláusulas, e o importador de dados fornecer uma cópia dessas proteções ao exportador de dados;
- iv) for necessário para o estabelecimento, exercício ou defesa de ações judiciais no contexto de procedimentos administrativos, regulamentares ou judiciais específicos;
- v) for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa física; ou
- vi) quando nenhuma das outras condições se aplicar, o importador de dados obtiver o consentimento explícito do titular dos dados para uma transferência posterior em uma situação específica, após tê-lo informado do(s) seu(s) objetivo(s), a identidade do destinatário e os possíveis riscos de tal transferência para ele/ela devido à falta de garantia de proteção de dados adequadas. Nesse caso, o importador de dados deve informar o exportador de dados e, a pedido deste, deve transmitir-lhe uma cópia das informações fornecidas ao titular dos dados.

Qualquer transferência posterior está sujeita ao cumprimento, pelo importador de dados, de todas as outras garantias destas Cláusulas, em particular a finalidade limitada.

8.8 Processamento sob a autoridade do importador de dados

O importador de dados deve garantir que qualquer pessoa que atue sob sua autoridade, incluindo um processador, processe os dados apenas de acordo com suas instruções.

8.9 Documentação e conformidade

(a) Cada Partícipe deverá ser capaz de demonstrar o cumprimento de suas obrigações sob estas

² O Acordo sobre o Espaço Econômico Europeu (Acordo EEE) prevê a extensão do mercado interno da União Europeia aos três Estados do EEE: Islândia, Liechtenstein e Noruega. A legislação da UE em matéria de proteção de dados, incluindo o Regulamento (UE) 2016/679, é abrangida pelo Acordo EEE e foi incorporada no seu anexo XI. Portanto, qualquer divulgação pelo importador de dados a um terceiro localizado no EEE não se qualifica como uma transferência subsequente para os fins destas Cláusulas.

Cláusulas. Em particular, o importador de dados deve manter a documentação adequada das atividades de processamento realizadas sob sua responsabilidade.

- (b) O importador de dados deve disponibilizar essa documentação à autoridade de supervisão competente, mediante pedido.

Cláusula 9

Uso de subprocessadores

Sem objeto

Cláusula 10

Direitos dos titulares dos dados

- (a) O importador de dados, quando pertinente com a assistência do exportador de dados, deve lidar com quaisquer consultas e solicitações que receber de um titular de dados em relação ao processamento de seus dados pessoais e ao exercício de seus direitos sob estas Cláusulas sem atraso indevido e, o mais tardar, um mês após a recepção da consulta ou pedido³). O importador de dados deve tomar as medidas adequadas para facilitar tais consultas, solicitações e o exercício dos direitos do titular dos dados. Qualquer informação fornecida ao titular dos dados deve ser feita de forma inteligível e facilmente acessível, utilizando uma linguagem clara e simples.

- (b) Em particular, a pedido do titular dos dados, o importador de dados deve, gratuitamente:

i) Fornecer confirmação ao titular dos dados se os dados pessoais que lhe dizem respeito estão sendo processados e, se for o caso, uma cópia dos dados que lhe dizem respeito e das informações contidas no Anexo I; se os dados pessoais foram ou serão transferidos posteriormente, forneça informações sobre os destinatários ou categorias de destinatários (conforme apropriado, a fim de fornecer informações significativas) para os quais os dados pessoais foram ou serão transferidos posteriormente, a finalidade de tais transferências posteriores, e seu fundamento de acordo com a Cláusula 8.7; e fornecer informações sobre o direito de apresentar uma reclamação a uma autoridade supervisora de acordo com a Cláusula 12 (c) (i);

ii) retificar dados inexatos ou incompletos relativos ao titular dos dados;

iii) apagar dados pessoais relativos ao titular dos dados se tais dados estiverem sendo, ou tiverem sido, processados violando qualquer uma das Cláusulas que garantem os direitos de beneficiário dos terceiros, ou se o titular dos dados retirar o consentimento no qual o processamento se baseia.

- (c) Sempre que o importador de dados processar os dados pessoais para fins de marketing direto, deve cessar o processamento para esses fins se o titular dos dados se opor.

³ Esse prazo pode ser prorrogado, no máximo, por mais dois meses, na medida do necessário, tendo em conta a complexidade e o número de pedidos. O importador de dados deve informar devida e prontamente o titular dos dados de qualquer extensão.



- (d) O importador de dados não deve tomar uma decisão com base apenas no processamento automatizado dos dados pessoais transferidos (doravante 'decisão automatizada'), que produziria efeitos jurídicos em relação ao titular dos dados ou o afetaria de forma semelhantemente significativa, a menos que tenha o consentimento explícito de o titular dos dados ou se for autorizado a fazê-lo sob a legislação do país de destino, desde que essas leis estabeleçam medidas adequadas para garantir os direitos e interesses legítimos do titular dos dados. Nesse caso, o importador de dados deve, quando necessário, em cooperação com o exportador de dados:
- i) informar o titular dos dados sobre a decisão automatizada prevista, as consequências previstas e a lógica envolvida; e
 - ii) implementar garantia adequada, pelo menos permitindo ao titular dos dados contestar a decisão, expressar o seu ponto de vista e obter a revisão por um ser humano.
- (e) Quando os pedidos de uma pessoa em causa forem excessivos, em particular devido ao seu carácter repetitivo, o importador de dados pode cobrar uma taxa razoável, levando em conta os custos administrativos de deferimento do pedido, ou recusar-se a dar seguimento ao pedido.
- (f) O importador de dados pode recusar o pedido do titular dos dados se tal recusa for permitida pelas leis do país de destino, e for necessária e proporcionada em uma sociedade democrática, para proteger um dos objetivos listados no Artigo 23 (1) do Regulamento (UE) 2016 / 679.
- (g) Se o importador de dados pretender recusar o pedido de uma pessoa em causa, deve informar a pessoa os motivos da recusa e da possibilidade de apresentar uma reclamação à autoridade de controlo competente e/ou procurar reparação judicial.

Cláusula 11 **Ressarcimento**

- (a) O importador de dados deve informar os titulares dos dados, de forma transparente e facilmente acessível, através de aviso individual ou no seu *website*, sobre contato autorizado para o tratamento de reclamações. Deve tratar prontamente todas as reclamações que receber de uma pessoa em causa.
- (b) Em caso de litígio entre o titular dos dados e um dos Partícipes em relação ao cumprimento destas Cláusulas, esse Partícipe deverá utilizar de todos os esforços para resolver a questão amigavelmente em tempo hábil. Os Partícipes devem manter-se mutuamente informados sobre tais controvérsias e, quando apropriado, cooperar para resolvê-las.
- (c) Quando a pessoa em causa invocar um direito de terceiro beneficiário nos termos da Cláusula 3, o importador de dados deve aceitar a decisão da pessoa em causa de:
- i) apresentar reclamação à autoridade de fiscalização do Estado-Membro da sua residência habitual ou local de trabalho, ou à autoridade de controlo competente nos termos da Cláusula 13;
 - ii) encaminhar a controvérsia aos tribunais competentes na acepção da Cláusula 18.
- (d) Os Partícipes aceitam que a pessoa em causa pode ser representada por um organismo, organização ou associação sem fins lucrativos, nas condições estabelecidas no artigo 80.º, n.º 1,

do Regulamento (UE) 2016/679.

- (e) O importador de dados deve respeitar uma decisão que seja vinculativa sob a legislação aplicável da UE ou dos Estados-Membros.
- (f) O importador de dados concorda que a escolha feita pelo titular dos dados não prejudicará seus direitos substantivos e processuais de buscar soluções de acordo com as leis aplicáveis.

Cláusula 12 **Responsabilidade**

- (a) Cada Partícipe será responsável perante o(s) outro(s) Partícipe(s) por quaisquer danos que causar ao(s) outro(s) Partícipe(s) por qualquer violação destas Cláusulas.
- (b) Cada Partícipe será responsável perante o titular dos dados, e o titular dos dados terá o direito de receber compensação por quaisquer danos, materiais ou não materiais, que o Partícipe causar ao titular ao violar os direitos de terceiros beneficiários sob estas Cláusulas. Tal não prejudica a responsabilidade do exportador de dados sob o Regulamento (UE) 2016/679.
- (c) Quando mais de um Partícipe for responsável por qualquer dano causado ao titular dos dados como resultado de uma violação destas Cláusulas, todos os Partícipes responsáveis serão conjunta e solidariamente responsáveis, e o titular dos dados tem o direito de mover uma ação judicial contra qualquer um destes Partícipes.
- (d) Os Partícipes concordam que, se um Partícipe for considerado responsável nos termos do parágrafo (c), terá o direito de reivindicar do(s) outro(s) Partícipe(s) a parte da indenização correspondente à sua responsabilidade pelos danos.
- (e) O importador de dados não pode recorrer à conduta de um processador ou subprocessador para evitar sua própria responsabilidade.

Cláusula 13 **Supervisão**

- (a) [Quando o exportador de dados está estabelecido em um Estado-Membro da UE:] A autoridade de supervisão com a responsabilidade de assegurar o cumprimento pelo exportador de dados do Regulamento (UE) 2016/679 no que diz respeito à transferência de dados, como indicado no Anexo I.C, atuará como autoridade de supervisão competente.

[Quando o exportador de dados não está estabelecido em um Estado-Membro da UE, mas se enquadra no âmbito territorial de aplicação do Regulamento (UE) 2016/679 de acordo com seu artigo 3(2) e nomeou um representante de acordo com o artigo 27(1) do Regulamento (UE) 2016/679:] À autoridade supervisora do Estado-Membro no qual o representante, na acepção do artigo 27(1) do Regulamento (UE) 2016/679 é estabelecido, conforme indicado no Anexo I.C, atuará como autoridade supervisora competente.

[Quando o exportador de dados não está estabelecido em um Estado-Membro da UE, mas se enquadra no âmbito territorial de aplicação do Regulamento (UE) 2016/679, de acordo com seu

artigo 3(2), sem, no entanto ter que nomear um representante de acordo com o artigo 27(2) do Regulamento (UE) 2016/679:] A autoridade de supervisão de um dos Estados-Membros nos quais as pessoas cujos dados pessoais são transferidos sob estas cláusulas em relação à oferta de bens ou serviços para elas, ou cujo comportamento é monitorado, estão localizadas, como indicado no Anexo I.C, atuará como autoridade de supervisão competente.

- (b) O importador de dados concorda em submeter-se à jurisdição e cooperar com a autoridade supervisora competente em quaisquer procedimentos que visem garantir o cumprimento destas cláusulas. Em particular, o importador de dados concorda em responder a consultas, submeter-se a auditorias e cumprir com as medidas adotadas pela autoridade supervisora, incluindo medidas corretivas e compensatórias. O importador de dados deverá fornecer à autoridade supervisora uma confirmação por escrito de que as medidas necessárias foram tomadas.

SEÇÃO III – LEIS E OBRIGAÇÕES LOCAIS EM CASO DE ACESSO POR AUTORIDADES PÚBLICAS

Cláusula 14

Leis e práticas locais que afetam o cumprimento das Cláusulas

- (a) Os Partícipes garantem que não têm motivos para acreditar que as leis e práticas do país terceiro de destino aplicáveis ao processamento dos dados pessoais pelo importador de dados, incluindo quaisquer exigências de divulgação de dados pessoais ou medidas de autorização de acesso por Partícipe das autoridades públicas, impeçam o importador de dados de cumprir suas obrigações nos termos destas Cláusulas. Isto se baseia no entendimento de que leis e práticas que respeitam a essência dos direitos e liberdades fundamentais e não excedem o que é necessário e proporcional em uma sociedade democrática para salvaguardar um dos objetivos listados no artigo 23(1) do Regulamento (UE) 2016/679, não estão em contradição com estas Cláusulas.
- (b) Os Partícipes declaram que, ao fornecer a garantia no parágrafo (a), levaram em devida consideração, em particular, os seguintes elementos:
- i) as circunstâncias específicas da transferência, incluindo a extensão da cadeia de processamento, o número de atores envolvidos e os canais de transmissão utilizados; as transferências posteriores previstas; o tipo de destinatário; a finalidade do processamento; as categorias e o formato dos dados pessoais transferidos; o setor econômico no qual a transferência ocorre; o local de armazenamento dos dados transferidos;
 - ii) as leis e práticas do país terceiro de destino - incluindo aquelas que exigem a divulgação de dados às autoridades públicas ou que autorizam o acesso por tais autoridades - relevantes à luz das circunstâncias específicas da transferência, e as limitações e salvaguardas aplicáveis ⁽⁴⁾;

⁴ No que diz respeito ao impacto de tais leis e práticas no cumprimento destas Cláusulas, diferentes elementos podem ser considerados como parte de uma avaliação global. Esses elementos podem incluir experiência prática relevante e documentada com instâncias anteriores de solicitações de divulgação de autoridades públicas, ou a ausência de tais solicitações, cobrindo um período de tempo suficientemente representativo. Refere-se, em especial, a registros internos ou outra documentação, elaborados de forma contínua de acordo com a devida diligência e certificados a nível de gestão sênior, desde que esta informação possa ser legalmente partilhada com terceiros. Quando essa experiência prática for considerada para concluir que o importador de dados não será impedido de cumprir essas Cláusulas, ela precisa ser apoiada por outros elementos objetivos e relevantes, e cabe às Partícipes considerar cuidadosamente se esses elementos juntos carregam peso, em termos de confiabilidade e representatividade, para apoiar esta conclusão. Em particular, as Partícipes devem levar em consideração se sua experiência prática é corroborada e não contrariada por informações confiáveis

iii) quaisquer salvaguardas contratuais, técnicas ou organizacionais relevantes, implementadas para complementar as salvaguardas previstas nestas cláusulas, incluindo medidas aplicadas durante a transmissão e ao processamento dos dados pessoais no país de destino.

(c) O importador de dados garante que, ao realizar a avaliação de acordo com o parágrafo (b), fez seus melhores esforços para fornecer ao exportador de dados informações relevantes e concorda que continuará a cooperar com o exportador de dados para assegurar o cumprimento destas cláusulas.

(d) Os Partícipes concordam em documentar a avaliação sob o parágrafo (b) e torná-la disponível à autoridade supervisora competente, mediante solicitação.

(e) O importador de dados concorda em notificar imediatamente o exportador de dados se, após ter concordado com estas cláusulas e pela duração do acordo, tiver razões para acreditar que está ou se tornou sujeito a leis ou práticas que não estejam de acordo com os requisitos do parágrafo (a), inclusive após uma mudança nas leis do país terceiro ou uma medida (como um pedido de divulgação) indicando uma aplicação de tais leis na prática que não esteja de acordo com os requisitos do parágrafo (a).

(f) Após uma notificação nos termos do parágrafo (e), ou se o exportador de dados tiver razões para acreditar que o importador de dados não pode mais cumprir suas obrigações nos termos destas cláusulas, o exportador de dados deverá identificar imediatamente as medidas apropriadas (por exemplo, medidas técnicas ou organizacionais para garantir a segurança e a confidencialidade) a serem adotadas pelo exportador e/ou importador de dados para resolver a situação [para o Módulo Três; se apropriado em consulta com o controlador]. O exportador de dados suspenderá a transferência de dados se considerar que não podem ser asseguradas salvaguardas apropriadas para tal transferência, ou se instruído pelo [para o Módulo Três: o controlador ou] a autoridade de supervisão competente para fazê-lo. Neste caso, o exportador de dados terá o direito de rescindir o acordo, na medida em que este diga respeito ao processamento de dados pessoais sob estas cláusulas. Se o acordo envolver mais de dois Partícipes, o exportador de dados poderá exercer este direito de rescisão somente em relação ao Partícipe relevante, a menos que os Partícipes tenham acordado de outra forma. Quando o acordo for rescindido seguindo esta Cláusula, as Cláusulas 15 (d) e (e) serão aplicáveis.

Cláusula 15

Obrigações do importador de dados em caso de acesso pelas autoridades públicas

15.1 Notificação

(a) O importador de dados concorda em notificar o exportador de dados e, sempre que possível, o envolvido imediatamente (se necessário, com a ajuda do exportador de dados), se:

i) receber um pedido legalmente vinculativo de uma autoridade pública, incluindo autoridades

publicamente disponíveis ou acessíveis de outra forma sobre a existência ou ausência de solicitações dentro do mesmo setor e/ou a aplicação da lei na prática, como jurisprudência e relatórios de órgãos de supervisão independentes.



judiciais, nos termos das leis do país de destino, para a divulgação de dados pessoais transferidos de acordo com estas cláusulas; tal notificação deverá incluir informações sobre os dados pessoais solicitados, a autoridade requerente, a base legal para o pedido e a resposta fornecida; ou

ii) tomar conhecimento de qualquer acesso direto das autoridades públicas aos dados pessoais transferidos de acordo com estas cláusulas, de acordo com as leis do país de destino; tal notificação deve incluir todas as informações disponíveis para o importador.

(b) Se o importador de dados estiver proibido de notificar o exportador de dados e/ou o envolvido sob as leis do país de destino, o importador de dados concorda em envidar seus melhores esforços para obter uma renúncia à proibição, com o objetivo de comunicar o máximo de informações possível, o mais rápido possível. O importador de dados concorda em documentar seus melhores esforços a fim de poder demonstrá-los a pedido do exportador de dados.

(c) Quando permitido pelas leis do país de destino, o importador de dados concorda em fornecer ao exportador de dados, em intervalos regulares pela duração do acordo, o máximo de informações relevantes sobre as solicitações recebidas (em particular, número de solicitações, tipo de dados solicitados, autoridade/entidades solicitantes, se as solicitações foram contestadas e o resultado de tais desafios, etc.). [Para o Módulo Três: O exportador de dados deve encaminhar as informações ao controlador].

(d) O importador de dados concorda em preservar as informações de acordo com os parágrafos (a) a (c) pela duração do acordo e colocá-las à disposição da autoridade supervisora competente, mediante solicitação.

(e) Os parágrafos (a) a (c) não prejudicam a obrigação do importador de dados de acordo com a cláusula 14(e) e a cláusula 16 de informar prontamente o exportador de dados quando não puder cumprir com estas cláusulas.

15.2 Revisão da legalidade e minimização de dados

(a) O importador de dados concorda em rever a legalidade do pedido de divulgação, em particular se ele permanece dentro dos poderes concedidos à autoridade pública requerente, e em contestar o pedido se, após avaliação cuidadosa, concluir que existem motivos razoáveis para considerar que o pedido é ilegal sob as leis do país de destino, obrigações aplicáveis sob o direito internacional e princípios de cortesia internacional. O importador de dados deverá, sob as mesmas condições, buscar possibilidades de recurso. Ao contestar um pedido, o importador de dados deve buscar medidas provisórias com vistas a suspender os efeitos do pedido até que a autoridade judicial competente tenha decidido sobre seu mérito. Ele não divulgará os dados pessoais solicitados até que seja solicitado a fazê-lo de acordo com as regras processuais aplicáveis. Estes requisitos não prejudicam as obrigações do importador de dados nos termos da Cláusula 14(e).

(b) O importador de dados concorda em documentar sua avaliação legal e qualquer contestação ao pedido de divulgação e, na medida do permitido pelas leis do país de destino, disponibilizar a documentação para o exportador de dados. Também a colocará à disposição da autoridade de supervisão competente, mediante solicitação. [Para o Módulo Três: O exportador de dados deverá colocar a avaliação à disposição do controlador].

(c) O importador de dados concorda em fornecer a quantidade mínima de informações permitidas ao responder a um pedido de divulgação, com base em uma interpretação razoável do pedido.

SEÇÃO IV – DISPOSIÇÕES FINAIS

Cláusula 16

Não cumprimento das Cláusulas e Rescisão

(a) O importador de dados deve informar imediatamente o exportador de dados se ele não puder cumprir essas cláusulas, por qualquer razão.

(b) No caso do importador de dados violar estas cláusulas ou não conseguir cumprir com elas, o exportador de dados suspenderá a transferência de dados pessoais para o importador de dados até que o cumprimento seja novamente assegurado ou até que o acordo seja rescindido. Isto é sem prejuízo da Cláusula 13 (f).

(c) O exportador de dados terá o direito de rescindir o acordo, na medida em que diga respeito ao processamento de dados pessoais sob estas cláusulas, em que:

i) o exportador de dados suspendeu a transferência de dados pessoais para o importador de dados nos termos do parágrafo (b) e o cumprimento destas cláusulas não é restaurado dentro de um prazo razoável e, de qualquer forma, dentro de um mês da suspensão;

ii) o importador de dados estiver em violação substancial ou persistente destas cláusulas; ou

iii) o importador de dados não cumpre uma decisão vinculativa de um tribunal ou autoridade de supervisão competente em relação a suas obrigações nos termos destas cláusulas.

Nestes casos, deverá informar à autoridade supervisora competente [para o Módulo Três: e o controlador] de tal não conformidade. Quando o acordo envolver mais de dois Partícipes, o exportador de dados poderá exercer este direito de rescisão somente em relação ao Partícipe relevante, a menos que os Partícipes tenham acordado de outra forma.

(d) [Para os Módulos Um, Dois e Três: Os dados pessoais que foram transferidos antes da rescisão do acordo nos termos do parágrafo (c) serão imediatamente devolvidos ao exportador de dados ou apagados em sua totalidade, à escolha do exportador de dados. O mesmo se aplica a quaisquer cópias dos dados]. [Para o Módulo Quatro: Os dados pessoais coletados pelo exportador de dados na UE que tenham sido transferidos antes da rescisão do acordo nos termos do parágrafo (c) serão imediatamente apagados em sua totalidade, incluindo qualquer cópia dos mesmos]. O importador de dados deverá certificar o apagamento dos dados ao exportador de dados. Até que os dados sejam apagados ou devolvidos, o importador de dados deverá continuar a assegurar o cumprimento destas cláusulas. No caso de leis locais aplicáveis ao importador de dados que proíbam a devolução ou o apagamento dos dados pessoais transferidos, o importador de dados garante que continuará a assegurar o cumprimento destas cláusulas e só processará os dados na medida e pelo tempo que for exigido por essa lei local.

(e) Qualquer um dos Partícipes pode revogar seu acordo de ficar vinculada por estas cláusulas quando (i) a Comissão Europeia adotar uma decisão nos termos do artigo 45(3) do Regulamento (UE) 2016/679 que abrange a transferência de dados pessoais aos quais estas cláusulas se aplicam; ou (ii) o Regulamento (UE) 2016/679 se tornar parte da estrutura legal do país para o qual os dados pessoais são transferidos. Isto sem prejuízo de outras obrigações aplicáveis ao processamento em questão nos termos da Regulamentação (UE) 2016/679.

Cláusula 17
Legislação vigente

Estas cláusulas serão regidas pela lei de um dos Estados-Membros da UE, desde que tal lei permita direitos de terceiros beneficiários. Os Partícipes concordam que esta será a lei da Bélgica.

Cláusula 18
Escolha do foro e jurisdição

- (a) Qualquer disputa decorrente dessas cláusulas será resolvida pelos tribunais de um Estado membro da UE.
- (b) Os Partícipes concordam que esses serão os tribunais da França.
- (c) A pessoa em questão também pode mover ações judiciais contra o exportador e/ou importador de dados perante os tribunais do Estado-Membro no qual ele/ela tem sua residência habitual.
- (d) Os Partícipes concordam em submeter-se à jurisdição de tais tribunais.



APÊNDICE

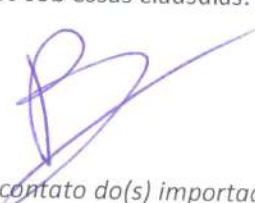
ANEXO I

A. LISTA DE PARTICIPANTES

Ponto de contato para questões de proteção de dados

- Grenoble INP – UGA: dpo@grenoble-inp.fr
Bâtiment DSIM Domaine universitaire
31, rue des mathématiques
38400 Saint-Martin-d'Hères
33 (0)4 56 52 90 44
- Universidade Federal de Lavras - UFLA: dri@ufla.br
Campus Universitário 3037
37200-900 | Lavras, MG | Brasil
+55 35 3829-1858

Exportador(es) de dados: *[Identidade e detalhes de contato do(s) exportador(es) de dados e, quando aplicável, do(s) seu(s) responsável(eis) pela proteção de dados e/ou representante na União Europeia].*

1. Nome: Institut Polytechnique de Grenoble (**Grenoble INP – UGA**) representado pelo Prof. Pierre Benech, Presidente.
Endereço: 46 avenue Felix Viallet 38031 Grenoble France
Atividades relevantes para aos dados transferidos sob essas cláusulas: informações sobre a mobilidade de estudantes
Papel (controlador/processador): Controlador
Assinatura e data: 26/09/2022 

Importador(es) de dados: *[Identidade e detalhes de contato do(s) importador(es) de dados, incluindo qualquer pessoa de contato com responsabilidade pela proteção de dados].*

1. Nome: Universidade Federal de Lavras (**UFLA**) representada por prof. Antonio Chalfun Junior, Diretor de Relações Internacionais
Endereço: Campus Universitário 3037 | 37200-900 | Lavras, MG, Brasil
Nome do contato, posição e detalhes: Diretoria de Relações Internacionais - dri@ufla.br
Atividades relevantes para aos dados transferidos sob essas cláusulas: informações sobre a mobilidade de estudantes
Papel (controlador/processador): Controlador
Assinatura e data:  17/11/2022

Este Anexo está nas versões em Inglês e Português. Inglês é o idioma da negociação deste instrumento. Qualquer tradução deve ser fiel à versão inglesa.

B. DESCRIÇÃO DA TRANSFERÊNCIA

1. Categorias de pessoas cujos dados pessoais são transferidos:

- Estudantes intercambistas do Grenoble INP - UGA
- Estudantes intercambistas da UFLA

2. Categorias de dados pessoais transferidos:

Para o Grenoble INP - UGA:

- a. Gênero, sobrenome, primeiro nome, endereço postal, número de telefone e e-mail, data e local de nascimento, cidadania dos estudantes intercambistas, cópia do passaporte do estudante intercambista;
- b. Transcrição das notas, diplomas anteriores obtidos, currículo, informação de contato da escola ou universidade;
- c. Prova da proficiência no idioma inglês;
- d. Informação de contato de emergência: nome, endereço postal, telefone.

Para a UFLA:

- a. Informações de contato;
- b. Informações financeiras;
- c. Dados educacionais, incluindo resultados de exames e avaliações.

3. Dados sensíveis transferidos (se aplicável) e aplicadas restrições ou salvaguardas que levem plenamente em consideração a natureza dos dados e os riscos envolvidos, tais como, por exemplo, limitação estrita da finalidade, restrições de acesso (incluindo acesso somente para o pessoal que tenha seguido treinamento especializado), manutenção de um registro de acesso aos dados, restrições para transferências posteriores ou medidas de segurança adicionais.

Sem transferência de dados sensíveis.

4. A frequência da transferência:

Uma vez por ano dependendo do período acadêmico (por ano ou semestre)

5. Natureza do processo:

Transferência de dados do estudante para sua nomeação antes da mobilidade.

6. Objetivo da transferência de dados e demais processamentos:

Assegurar a mobilidade internacional do estudante e análise de dados.

7. O período pelo qual os dados pessoais serão retidos:

Os dados pessoais serão retidos durante a mobilidade do estudante e a duração do acordo.

C. AUTORIDADE FISCALIZADORA COMPETENTE

A autoridade fiscalizadora competente em conformidade com a Cláusula 12 é o CNIL.

ANEXO II

MEDIDAS TÉCNICAS E ORGANIZACIONAIS, INCLUINDO MEDIDAS TÉCNICAS E ORGANIZACIONAIS PARA GARANTIR A SEGURANÇA DOS DADOS

Medidas técnicas e organizacionais para o Grenoble INP:

Medidas técnicas de segurança:

- *Datacenters* protegidos por acesso restrito; sistema de combate a incêndio com sirenes, extintores manuais, extinção automática; redundância de alimentação e ar condicionado;
- Backup de dados em site remoto;
- Acesso às estações de trabalho com login e senha;
- Soluções antivírus em estações de trabalho e servidores;
- Acesso aos aplicativos com login e senha, logados;
- Gerenciamento de direitos do usuário;
- Implantação de *patches* de segurança em softwares e sistemas operacionais, consolidação de sistema;
- Configurações, sistemas e monitoramento de rede;
- Uso de firewalls e segmentação de rede;
- Criptografia de trocas (HTTPS/SSL), acesso remoto via VPN criptografada.

Medidas organizacionais de segurança:

- Diretor de proteção de dados (DPO), Gerente de Segurança de Sistemas de Informação (ISSM);
- Registro de atividades de tratamento de dados pessoais;
- Procedimentos de gerenciamento de incidentes;
- Avaliações de impacto de privacidade para operações de processamento que representam um risco significativo para a privacidade dos dados;
- Carta de utilização de recursos informáticos e de comunicação relevantes por todos os colaboradores; Carta para pessoal de TI;
- Informação e sensibilização (intranet do funcionário, boas-vindas ao novo pessoal) sobre privacidade e boas práticas

Medidas técnicas e organizacionais para a UFLA:

A Portaria nº 1896, de 23 de dezembro de 2020 (https://sistemaslegados.ufla.br/documentos/arquivos/21_1896_23122020.pdf) que regula as medidas técnicas para garantir a segurança de dados, garante a proteção dos dados pessoais coletados e/ou mantidos em bancos de dados físicos e eletrônicos da Universidade Federal de Lavras, atendendo à Lei nº 13.709 de 2018 (http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/l13709.htm).