



Binding Corporate Rules – Ellucian as Data Processor

Table of Contents

BACKGROUND	4
PURPOSE	4
DEFINITIONS	4
1 BINDING NATURE	5
1.1 THE DUTY TO RESPECT THE BCRs	5
1.2 BINDING NATURE OF BCRs	5
1.3 THIRD-PARTY BENEFICIARY RIGHTS	6
1.4 RESPONSIBILITY TOWARDS THE DATA CONTROLLER	8
1.5 ELLUCIAN IRELAND LIMITED ACCEPTS LIABILITY	8
1.6 [NOT USED]	8
1.7 BURDEN OF PROOF LIES WITH ELLUCIAN AND NOT THE INDIVIDUAL DATA SUBJECT	8
1.8 EASY ACCESS TO THESE BCRs FOR THE DATA CONTROLLER AND DATA SUBJECTS	8
2 EFFECTIVENESS	9
2.1 THE EXISTENCE OF A SUITABLE TRAINING PROGRAMME	9
2.2 THE EXISTENCE OF A COMPLAINT HANDLING PROCESS FOR THE BCRs	9
2.3 THE EXISTENCE OF AN AUDIT PROGRAMME COVERING THE BCRs	9
2.4 THE CREATION OF A NETWORK OF DATA PROTECTION OFFICERS (DPOs) OR APPROPRIATE STAFF FOR MONITORING COMPLIANCE WITH THE RULES	10
2.5 ON-GOING ASSESSMENT OF THE EFFECTIVENESS OF THE RULES	10
3 DUTIES OF COOPERATION	11
3.1 DUTY TO COOPERATE WITH SUPERVISORY AUTHORITIES	11
3.2 DUTY TO COOPERATE WITH THE DATA CONTROLLER	11
4 DESCRIPTION OF PROCESSING AND DATA FLOWS	11
4.1 MATERIAL SCOPE	11
4.2 GEOGRAPHICAL SCOPE OF THE BCRs	12
5 MECHANISMS FOR REPORTING AND RECORDING CHANGES	12
5.1 PROCESS FOR UPDATING THE BCRs	12
6 DATA PROTECTION SAFEGUARDS	13
6.1 DATA PROTECTION PRINCIPLES	13
i. Transparency, fairness and lawfulness:	13
ii. Purpose limitation:	13
iii. Data quality:	14
iv. Security:	14
v. Data subject rights:	14
vi. Sub-processing within the Group:	14
vii. Onward transfers to External Data Processors:	15
6.1.2 ACCOUNTABILITY AND OTHER TOOLS	15
6.2 ENTITIES BOUND BY THESE BCRs	16
6.3 TRANSPARENCY WHEN LEGISLATION PREVENTS COMPLIANCE WITH THE BCRs	17
6.4 THE RELATIONSHIP BETWEEN NATIONAL LAWS AND BCRs	17
ANNEX 1	19
ADOPTION AGREEMENT	19
ANNEX 2	19
BCR COMPLAINT PROCESS STEPS	19
BCR COMPLAINT PROCESS DIAGRAM	19
ANNEX 3	19
BCR AUDIT PROGRAMME	19
ANNEX 4	19
DATA PROCESSING PARTICULARS	19
ANNEX 5	19
PROCESS FOR CHANGING BINDING CORPORATE RULES	19
ANNEX 6	19
DATA PROCESSING CLAUSES	19
ANNEX 7	19
TRANSFER RISK ASSESSMENT	19
ANNEX 8	19

GOVERNMENT ACCESS REQUESTS 19

BACKGROUND

Data protection laws govern how Ellucian handles personal data in each country in which we operate. Where Ellucian acts as a service provider to Process Personal Data on behalf of our customers we are a Data Processor (as defined below).

There are specific European Union (“**EU**”) data protection requirements on transferring Personal Data from the European Economic Area (“**EEA**”) to another country outside the EEA. Such transfers are generally only permitted if the country of transfer is deemed by the European Commission to have an adequate level of data protection or if an appropriate safeguard pursuant to EU law in place. Binding Corporate Rules (“**BCRs**”) are an example of an appropriate safeguard.

PURPOSE

The purpose of this document is to:

- explain Ellucian’s data protection obligations as a Data Processor and/or sub-Data Processor under these BCRs;
- explain the scope and application of these BCRs;
- define Ellucian employees’ data protection responsibilities and accountability for implementing and complying with these BCRs;
- explain how Ellucian handles complaints and Data Subject rights under the BCRs; and
- provide information on how to contact Ellucian directly.

DEFINITIONS

Binding Corporate Rules or **BCRs** means this set of EU Binding Corporate Rules for Processors including the Annexes hereto which are applicable to, and binding on, each Group Member.

Data Controller means the Ellucian customer (a natural or legal person, public authority, agency or other body) which, alone or jointly with others, determines the purpose and means of the Processing of Personal Data.

Data Processor means the natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller.

Data Subject means a natural person who is the subject of Personal Data.

DPO means the Group’s Data Protection Officer.

EEA means the European Economic Area.

Ellucian or **Group** means the collection of all Group Members.

EU means the European Union.

External Data Processor means a sub-Data Processor not in the Group engaged by a Group Member.

General Data Protection Regulation or **GDPR** means regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data and repealing Directive 95/46/EC.

Group Member means an Ellucian entity which has executed the intra-group adoption agreement referred to in [Rule 1.2](#) and is a Data Processor or sub-Data Processor on behalf of a Data Controller (which Data Controller is not in the Group).

Lead Supervisory Authority means the lead supervisory authority for Ellucian's BCRs, being the Irish Data Protection Commission.

Personal Data means any information relating to an identified or identifiable natural person. The term "Personal Data" as used in these BCRs shall mean any Personal Data Processed by a Group Member in providing services to a Data Controller(s).

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

Process or **Processing** means any operation or set of operations which is performed on personal data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. **Processed** and **Processes** shall be construed accordingly.

Service Agreement means an agreement(s) between a Group Member and an Ellucian customer in the customer's capacity as a Data Controller that pursuant to its terms specifies the Processing of Personal Data by the Group Member.

Special Categories of Personal Data means Personal Data revealing, directly or indirectly, the racial or ethnic origin, political, philosophical or religious beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Supervisory Authority means an independent public authority which is established by an EEA member state pursuant to Article 51 of the GDPR.

1 BINDING NATURE

1.1 The duty to respect the BCRs

The BCRs and the Annexes are legally binding on all Group Members listed in [Rule 6.2](#) and each Group Member and its employees accept their duty to respect the BCRs.

Each Group Member and its employees shall respect the instructions from the Data Controller regarding the Processing of Personal Data as described in a Service Agreement.

1.2 Binding nature of BCRs

Each Group Member is required to enter into the intra-group adoption agreement among all of the Group Members binding that Group Member to comply with these BCRs and the Annexes.

These BCRs are binding on all Group Members listed in [Rule 6.2](#).

A new Group Member will accede to the BCRs by executing the intra-group adoption agreement either directly or through an adherence agreement obliging that Group Member to comply with these BCRs.

[Rule 6.2](#) will be updated accordingly in accordance with [Rule 5.1](#).

Reference: Please see attached [Annex 1](#) which is a copy of the intra-group adoption agreement.

1.3 Third-party beneficiary rights

Each Data Subject whose Personal Data is Processed by a Group Member shall have the ability to enforce the following elements of these BCRs as a third-party beneficiary, including the ability to seek judicial remedies and, where appropriate, compensation:

- i. duty to respect the instructions from the Data Controller regarding the Processing of Personal Data including in relation to data transfers to a non-EEA country ([Rule 1.1](#), Rule 6.1(ii) and Rule 6.1(vii));
- ii. duty to implement appropriate technical and organizational security measures (Rule 6.1(iv));
- iii. duty to notify any Personal Data Breach to the Data Controller (Rule 6.1(iv));
- iv. duty to respect certain conditions when engaging a Group Data Processor or External Data Processor (Rule 6.1(vi) and Rule 6.1(vii));
- v. duty to cooperate with and assist the Data Controller in complying and demonstrating compliance with applicable data protection law such as in relation to answering requests from Data Subjects on their rights ([Rule 3.2](#), Rule 6.1(i), Rule 6.1(iii), Rule 6.1(iv), Rule 6.1(v) and [Rule 6.1.2](#));
- vi. duty to provide Data Subjects with easy access to the BCRs ([Rule 1.8](#));
- vii. duty to cooperate with Supervisory Authorities to ensure compliance by Group Members with the BCRs ([Rule 3.1](#));
- viii. with respect to the liability and jurisdiction provisions under which Data Subjects may enforce the BCRs, Ellucian Ireland Limited accepts responsibility for actions of Group Members and External Data Processors which are located outside of the EEA and agrees to pay compensation for material and non-material damage resulting from the violation of the BCRs by such Group Data Processors or External Data Processors ([Rules 1.3](#) and [1.4](#));
- ix. duty to assess on an ongoing basis as whether national legislation prevents the Group Member from fulfilling its obligations under the BCRs ([Rule 6.4](#));
- x. duty to be transparent if national legislation prevents the Group Member from fulfilling its obligations under the BCRs including by promptly notifying the DPO (who will notify Ellucian Ireland Limited, the Data Controller and the Data Controller's competent Supervisory Authority) if the Group Member has reason to believe that the legislation applicable to it prevents it from fulfilling its obligations under the BCRs or any legal requirement that the Group Member is subject to in a non-EEA country is likely to have a substantial adverse effect on the guarantees provided by the BCRs (including any legally binding request for disclosure of Personal Data by a public authority) ([Rule 2.5](#), [Rule 6.3](#) and [Rule 6.4](#)); and
- xi. duty to respect the right to complain through the internal complaint mechanism of the Group Members ([Rule 2.2](#)).

If a Data Subject is not able to bring a claim against the Data Controller because the Data Controller has disappeared, ceased to exist, or become insolvent, and there is no successor entity that has assumed the legal obligations of the Data Controller, a Data Subject may enforce the following rules against Ellucian Ireland Limited:

[Rule 1.1](#): The BCRs are binding on all Group Members and each Group Member and its employees accept their duty to respect the BCRs. Each Group Member and its employees shall respect the instructions from the Data Controller regarding data Processing as described in a Service Agreement.

[Rule 1.3](#): Each Data Subject whose Personal Data is Processed by a Group Member shall have the ability to enforce the elements of these BCRs listed above in (i) to (xi) as a third-party

beneficiary, including the ability to seek judicial remedies and, where appropriate, compensation.

[Rule 1.5:](#) Ellucian Ireland Limited, the EEA Group Member with delegated data protection responsibilities from the Group, accepts responsibility for other Group Members outside of the EEA that are bound by these BCRs or External Data Processors outside the EEA and agrees to pay compensation for material and non-material damage resulting from the violation of these BCRs by Group Members or External Data Processors located outside of the EEA.

[Rule 1.7:](#) Ellucian Ireland Limited will have the burden of proof to demonstrate that a Group Member or an External Data Processor outside the EEA is not liable for any violation of these BCRs which has resulted in the Data Subject claiming damages.

[Rule 1.8:](#) These BCRs will be made easily accessible online for Data Controllers and Data Subjects.

[Rule 2.2:](#) Complaints will be dealt with without undue delay, and in any event within one month, unless an extension period is required and notified to the Data Subject within the initial one month period.

[Rule 3.1:](#) Group Members will cooperate with all Supervisory Authorities, will accept and submit to be audited by such Supervisory Authorities regarding these BCRs and will comply with the advice of and abide by the decisions of these Supervisory Authorities on any issue related to the BCRs.

[Rule 3.2:](#) Group Members will cooperate and assist the Data Controller to comply with applicable data protection law.

[Rule 6.1:](#) When Processing Personal Data Group Members will observe the principles relating to: transparency, fairness and lawfulness; purposes limitation; data quality; security; Data Subject rights; sub-Processing and onward transfers.

[Rule 6.2:](#) The entities that are bound by these BCRs are set out in [Rule 6.2.](#)

[Rule 6.3:](#) Where a Group Member believes that laws and practices in the non-EEA country of destination applicable to the Processing of the Personal Data by it may prevent it from fulfilling the instructions received from the Data Controller or its obligations under these BCRs or Service Agreement, the Group Member shall, unless prohibited by law, promptly inform the DPO. The DPO will then, unless prohibited by law, inform Ellucian Ireland Limited, the Data Controller and the Data Controller's competent Supervisory Authority.

Without prejudice to any other administrative or judicial remedy, every Data Subject shall have the right to lodge a complaint with a Supervisory Authority, in particular, Data Subjects shall be entitled to: (a) lodge a complaint before the competent Supervisory Authority of the EEA country of: (i) their habitual residence; (ii) their place of work; or (iii) the place of alleged infringement; and/or (b) initiate proceedings before the competent court in the EEA country where: (i) the Data Controller is established; (ii) the Group Member is established; or (iii) the Data Subject has their habitual residence.

A Data Subject has a right to receive full and effective compensation for material or non-material damage that results from an infringement of the BCRs by a Group Member or External Data Processor. However, a Group Member or External Data Processor shall not be liable where it proves that it is not in any way responsible for the event giving rise to the damage.

If a Group Member and/or External Data Processor and the Data Controller involved in the same processing are found responsible for any damage caused by such processing, the Data Subject shall be entitled to receive compensation for the entire damage directly from the applicable Group Member or External Data Processor.

Where an infringement of these BCRs is caused by a Group Member or an External Data Processor outside of the EEA, then [Rule 1.5](#) below applies.

1.4 Responsibility towards the Data Controller

These BCRs shall be made binding toward the Data Controller through a specific reference to them in the Service Agreement. The Data Controller shall have the right to enforce the BCRs against: (a) the Group Member that is a party to the Service Agreement for any breaches of these BCRs or the Service Agreement that Group Member caused; or (b) against Ellucian Ireland Limited for (i) any breach of these BCRs or the Service Agreement by a Group Member located outside the EEA; or (ii) a breach of the agreement with an External Data Processor located outside of the EEA (as envisaged in Rule 6.1(vii)). The Data Controller's contractual remedies (such as termination) shall be as described in the Service Agreement and such judicial remedies shall be as available in the jurisdiction of the claim.

1.5 Ellucian Ireland Limited accepts liability

Ellucian Ireland Limited, the EEA Group Member with delegated data protection responsibilities from the Group, accepts responsibility for, and agrees to take necessary action(s) to remedy the acts of other Group Members or External Data Processors outside the EEA and to pay compensation for material and non-material damage resulting from the violation of these BCRs by Group Members or External Data Processors located outside of the EEA.

If a Group Member or an External Data Processor outside the EEA violates the BCRs, the courts or other competent authority(ies) in the EEA will have jurisdiction and the Data Subject will have the rights and remedies against Ellucian Ireland Limited as if the violation had been caused by Ellucian Ireland Limited in Ireland instead of the location where the Group Member or External Data Processor outside the EEA is based. Ellucian Ireland Limited may not rely on a breach by a sub-Data Processor (either a Group Member or an External Data Processor) of its obligations in order to avoid its liabilities under this [Rule 1.5](#).

1.6 [Not Used]

1.7 Burden of proof lies with Ellucian and not the individual Data Subject

Ellucian Ireland Limited will have the burden of proof to demonstrate that a Group Member or an External Data Processor outside the EEA is not liable for any violation of these BCRs which has resulted in the Data Subject claiming damages.

Where the Data Controller can demonstrate that it suffered damage and establish facts which show it is likely that the damage has occurred because of a Group Member's breach of these BCRs, it will be for Ellucian Ireland Limited to prove that: (a) the Group Member or the External Data Processor outside of the EEA was not responsible for the breach of the BCRs giving rise to those damages; or (b) that no such breach took place.

If Ellucian Ireland Limited can demonstrate that the Group Member or the External Data Processor outside the EEA is not responsible for the act, it may discharge itself from any responsibility and liabilities.

1.8 Easy access to these BCRs for the Data Controller and data subjects

These BCRs will be included or electronically accessible (i.e. hyperlinked) in the Service Agreement between a Group Member and the Data Controller.

Every Data Subject whose Personal Data is Processed by the Group has the right to have easy access to these BCRs. Upon approval, these BCRs will be published on the Group's website(s) in a way easily accessible to Data Subjects.

2 EFFECTIVENESS

2.1 The existence of a suitable training programme

Group Members provide data protection training to all employees, including appropriate training on these BCRs, who: (a) have permanent or regular access to Personal Data; (b) are involved in the collection of Personal Data; or (c) are involved in the development of tools used to process Personal Data. This training is provided to each relevant employee upon hire and annually thereafter. The Group's privacy and information security teams monitor completion of training and escalate to management as needed to ensure the training is completed. Group Members will confirm that sub-Data Processors provide data protection training to all personnel who, while working with Group Members, will (a) have permanent or regular access to Personal Data; (b) are involved in the collection of Personal Data; or (c) are involved in the development of tools used to Process Personal Data. Group Members may provide direct training to sub-Data Processor personnel as appropriate.

2.2 The existence of a complaint handling process for the BCRs

Any complaints regarding the BCRs from any Data Subject regarding any Group Member may be submitted to the DPO by emailing privacy@ellucian.com, by calling +1 703 261 2161 or sending a complaint by post to Data Protection Officer, Ellucian, 4 Country View Road, Malvern, PA 19355, USA. Group Member personnel who receive complaints from Data Subjects will submit the complaints via the same process. Any complaints howsoever received will be communicated without undue delay to the Data Controller without any obligation to handle such complaint except if otherwise agreed with the Data Controller.

If a Data Controller has disappeared, ceased to exist or become insolvent, or a Group Member has agreed to handle complaints from Data Subjects on behalf of that Data Controller, those complaints will be handled by the Group Member without undue delay, and in any event within one month from receipt of the complaint, by the DPO and their team. Taking into account the complexity and number of complaints, the one month period may be extended at maximum by two further months upon notice to the Data Subject within the initial one month period.

A Data Subject is not obliged to utilize Ellucian's internal complaint handling process and may instead choose to bring their complaint directly before a Supervisory Authority and/or a competent court at any time. A Data Subject has a right to receive full and effective compensation for material or non-material damage that results from an infringement of the BCRs by a Group Member or an External Data Processor. However, a Group Member or any External Data Processor shall not be liable where it proves that it is not in any way responsible for the event giving rise to the damage.

Reference: Please see attached [Annex 2](#) which contains the BCR Complaint Process in written steps and the BCR Complaint Process in diagram form.

2.3 The existence of an audit programme covering the BCRs

On a yearly basis, the Group will conduct data protection audits to verify compliance with all aspects of these BCRs by Group Members including methods and action plans ensuring that corrective actions have been implemented. When appropriate, data protection audits of External Data Processors will be conducted based on the level of risk posed by the processing of that

External Data Processor. These audits will be carried out by either internal auditors or external professionally-accredited auditors or on specific request to the DPO from the Executive Team or the Board of Directors. Further, at the request of the Data Controller, any Group Member will submit to an audit of their data processing facilities relating to the Processing activities of that Data Controller. These audits will be carried out by the Data Controller or an independent professionally-accredited inspection body bound by a duty of confidentiality selected by the Data Controller, in agreement with the Supervisory Authority (where applicable).

If non-compliance is identified through an audit, by a Supervisory Authority or otherwise, the Group Member shall rectify the identified non-compliance without undue delay. Such non-compliance shall be notified to the DPO, Vice President of Compliance, and/or the Compliance Committee, depending on the nature of the issue. The DPO will be kept informed of resolution measures, will oversee resolution measures and will direct any suspension and resumption of data transfers to that Group Member. If non-compliance persists and is not resolved without undue delay, then the DPO shall remove the Group Member from the BCR and the DPO will notify the Lead Supervisory Authority in the annual update.

Audit results will be made available to the Data Controller and the Data Controller's competent Supervisory Authority on request.

Reference: Please see attached [Annex 3](#) for additional details on the Group's audit programme.

2.4 The creation of a network of data protection officers (DPOs) or appropriate staff for monitoring compliance with the rules

The Group commits to designate a DPO where required pursuant to Article 37 of the GDPR or any other person or entity (such as a Chief Privacy Officer) with responsibility to monitor compliance with the BCRs which role shall enjoy the highest management support for the fulfilling of their tasks.

The Group has appointed one DPO whose role covers all Group Members. The DPO role which sits in the Legal & Compliance organization and receives the highest management support. The DPO monitors compliance with data protection obligations and, as part of that, will monitor compliance with the BCRs. In addition, the DPO informs and advises the highest Group management on data protection issues, deals with Supervisory Authorities' investigations, monitors and annually reports on BCR compliance at a global level, and monitors training and compliance regarding data protection. The DPO reports to the audit committee of the Group's board of directors (the highest management level) at least annually.

2.5 On-going assessment of the effectiveness of the rules

Before a Group Member can rely on these BCRs for a transfer of Personal Data outside of the EEA, the Group Member engaged in the Processing that requires a transfer of Personal Data outside of the EEA shall warrant that they have no reason to believe that the laws and practices in the non-EEA country of destination applicable to the Processing of the Personal Data by the Group Member importing the data (including any requirements to disclose Personal Data or measures authorising access by public authorities) prevent the Group Member importing the data from fulfilling its obligations under these BCRs. 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 are not in contradiction with these BCRs. The Group Member shall in providing this warranty take into account the elements set out in [Annex 7](#) (Transfer Risk Assessment). The Group Member importing the data warrants that, in carrying out this assessment that it has used best efforts to provide the Data Controller exporting the data with relevant information and agrees that it will continue to cooperate with the Data Controller in ensuring compliance with these BCRs. The Data Controller and the Group Member

involved in the transfer agree to document this assessment and make it available to any competent Supervisory Authority on request.

The Group Member importing the data agrees to promptly notify the Data Controller exporting the data if, after having commenced transfers of data pursuant to these BCRs, the Group Member has reason to believe that it is or has become subject to laws or practices that mean an essentially equivalent level of data protection as provided under these BCRs cannot be adhered to and more specifically that the requirements contained in these BCRs cannot be respected in line with the warranty in the preceding paragraph, including following a change in the laws in the non-EEA country of destination 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 the warranty in the preceding paragraph. The Group Member importing the data shall also notify the DPO of this fact in accordance with [Rule 6.3](#).

Following such notification to the Data Controller, or if the Data Controller exporting the data has reason to believe that the Group Member importing the data can no longer fulfil its obligations under these BCRs, the Data Controller shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the Group Member involved in the data transfer to address the situation.

The Data Controller may suspend the transfer of Personal Data and/or terminate the applicable contract with the Group Member if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by a Supervisory Authority to do so in respect to only those services which cannot be provided by the Group Member in accordance with these BCRs and otherwise where such termination is in accordance with the terms and conditions of that contract.

3 DUTIES OF COOPERATION

3.1 Duty to cooperate with Supervisory Authorities

Group Members shall cooperate with all Supervisory Authorities (including the Data Controller's competent Supervisory Authority), accept and submit to be audited by such Supervisory Authorities regarding these BCRs, comply with the advice of and abide by the decisions of these Supervisory Authorities on any issue related to the BCRs.

3.2 Duty to cooperate with the Data Controller

Group Members and any External Data Processors shall cooperate and assist the Data Controller to comply with applicable data protection law (such as the duty to respect Data Subject rights or to handle Data Subject complaints, or to reply to an investigation or inquiry from Supervisory Authorities). This cooperation and assistance shall be provided in a reasonable time and to the extent reasonably possible within the scope of the relationship between the Group Member and the Data Controller and in accordance with the terms of the Service Agreement between the Group Member and the Data Controller.

4 DESCRIPTION OF PROCESSING AND DATA FLOWS

4.1 Material Scope

All Group Members listed in [Rule 6.2](#) below are bound by these BCRs.

These BCRs apply to all Personal Data that Group Members Process on behalf of a Data Controller. For example, this Personal Data may include: (a) Personal Data stored or Processed by the Data Controller in hosted or software-as-a-service (“**SaaS**”) software that uses infrastructure owned or controlled by a Group Member; (b) Personal Data provided to a Group Member by the Data Controller for the purpose of the Group Member providing support, implementation, consulting, or other services to the Data Controller; or (c) Personal Data provided by a customer or another person who has a relationship with the Data Controller to a Group Member for the purpose of troubleshooting or other services.

Ellucian’s customers, the Data Controllers, are institutions of higher education and other organisations that provide education to their employees or the public. Ellucian’s software and services facilitate running an entire institution of higher education. Therefore, Data Controllers may use Group Members to Process almost any category of Personal Data, and the Data Subjects could be individuals in any type of relationship with the Data Controller. The Data Controllers determine the categories of Personal Data collected and provided to Group Members. An example of the type of data that is processed and the purposes for processing is set out in [Annex 4](#) (Data Processing Particulars).

Group Members will Process Personal Data on behalf of a Data Controller as required to perform their obligations to the Data Controller under the terms of the Service Agreement and for related administrative purposes.

Personal Data is transferred among Group Members for the purposes of performing their obligations to the Data Controller under the terms of the Service Agreement and for related administrative purposes. Personal Data is transferred to External Data Processors when necessary to perform a Group Member’s obligations to a Data Controller, and when the data protection practices of such External Data Processors are appropriate based on the circumstances and consistent with the Group’s obligations to the Data Controller.

These BCRs do not apply to Personal Data Processed by Ellucian as a data controller for its own purposes such as recruitment, employment or marketing.

Reference: Please see attached [Annex 4](#) which sets out the Data Processing Particulars.

4.2 Geographical Scope of the BCRS

All Group Members listed in [Rule 6.2](#) below are bound by these BCRs.

The Data Controller must decide whether these BCRs apply to Personal Data Processed for activities which are subject to EU law or all Processing of Personal Data by a Group Member as Data Processor wherever the origin of the data.

5 MECHANISMS FOR REPORTING AND RECORDING CHANGES

5.1 Process for updating the BCRs

The BCRs including the Annexes can be modified when needed, by following the Group’s Process for Changing Binding Corporate Rules.

The DPO (or their delegate) will:

- keep a fully updated list of the Group Members and External Data Processors involved in the data Processing activities for the Data Controller which will be made accessible to the Data Controller, Data Subjects and Supervisory Authorities on request;

- keep track of and record any updates to the BCRs and provide the necessary information to the Data Controllers on such updates and to Supervisory Authorities on request;
- inform Data Controllers of any changes without undue delay so that the Data Controller has the possibility to object to the change or to terminate the applicable contract in respect to only those services which are affected by the update (in accordance with the terms and conditions of that contract) before the modification is made (for instance, on any intended changes concerning the addition or replacement of sub-Data Processors, before the data is provided to the new sub-Data Processor);
- inform Group Members of any changes to the BCRs without undue delay so that the Group Member is aware that it is bound by such change;
- inform the competent Supervisory Authority annually for changes to the BCRs including any changes to the Annexes or list of Group Members together with a brief explanation of the reasons justifying the update; and
- inform the relevant Supervisory Authorities via the competent Supervisory Authority promptly of any change that would possibly affect the level of protection offered by the BCRs (i.e., changes to the binding character) together with a brief explanation of the reasons justifying the update.

No transfers of Personal Data should be made to a new Group Member before the new Group Member is effectively bound by the BCRs and can deliver compliance with the BCRs.

Reference: Please see attached [Annex 5](#) which contains the Process for Changing Binding Corporate Rules.

6 DATA PROTECTION SAFEGUARDS

6.1 Data protection principles

Group Members shall observe the following principles in the Processing of Personal Data:

- Transparency, fairness and lawfulness:** Group Members and External Data Processors will have a general duty to help and assist the Data Controller to comply with applicable data protection law (for example, to be transparent about sub-Data Processor activities in order to allow the Data Controller to correctly inform the Data Subjects);
- Purpose limitation:** Group Members have a duty to Process Personal Data only on behalf of the Data Controller and in compliance with instructions from the Data Controller, including with respect to transfers of Personal Data to a non-EEA country unless required to do so by EU or EEA member state law to which the Group Member is subject. In that case, the Group Member shall inform the Data Controller of that legal requirement before Processing takes place, unless that law prohibits such information on important grounds of public interest. In other cases, if the Group Member cannot comply, it shall promptly inform the Data Controller of its inability to comply, in which case the Data Controller is entitled to suspend the transfer of Personal Data and/or terminate the applicable contract which relates to the services which cannot be provided by the Group Member in accordance with the Data Controller's instructions (and where such termination is in accordance with the terms and conditions of that contract).

Upon the termination of the provision of services under the Service Agreement, the Group Member and any Group Data Processors and/or External Data Processors shall, at the choice of the Data Controller, delete or return all the Personal Data Processed pursuant to the Service Agreement and delete any copies thereof according to the Group's then-applicable data retention and disposal policies. Upon request, the Group Member will certify to the Data Controller that it has done so, unless EU or EEA member state law requires to the continued storage of the Personal Data. In that case, the Group Member will inform the Data Controller and warrant that it will guarantee the confidentiality of the

Personal Data and will not further Process the Personal Data otherwise than as required by the EU or EEA member state law.

- iii. **Data quality:** Group Members and any External Data Processors will have a general duty to help and assist the Data Controller to comply with applicable data protection law, in particular:
 - o Group Members and any External Data Processors will execute any necessary measures when asked by the Data Controller, to update, correct or delete the data. Group Members and any External Data Processors will inform each Group Member to whom the data have been disclosed of any rectification or deletion of personal data.
 - o Group Members and any External Data Processors will execute any necessary measures, when asked by the Data Controller and subject to the terms of the Service Agreement, in order to delete or anonymize the data from the moment identifiable data is not necessary anymore. Group Members and any External Data Processors will communicate to each entity to whom the Personal Data have been disclosed of any request to delete or anonymize the data.
- iv. **Security:** Group Members and External Data Processors will have a duty to implement appropriate technical and organizational measures as described in the Group's Information Security Policy to ensure a level of security appropriate to the risks presented by the processing. Group Members and External Data Processors will also have a duty to assist the Data Controller in ensuring compliance with its data protection obligations, taking into account the nature of Processing and information available to the Group Member and External Data Processor. Group Members and External Data Processors must implement technical and organizational measures which at least meet the requirements of applicable law in the Data Controller's jurisdiction and the Service Agreement between the Group Member and the Data Controller. Group Members shall inform the Data Controller without undue delay after becoming aware of any Personal Data Breach. In addition, sub-Data Processors shall have the duty to inform the Group Member acting as Data Processor without undue delay after becoming aware of any Personal Data Breach, and the Group Member will then notify the Data Controller pursuant to the terms of the Service Agreement.
- v. **Data subject rights:** Group Members and External Data Processors will implement any appropriate technical and organizational measures, insofar as this is possible and subject to the terms of the Service Agreement, when asked by the Data Controller, for the fulfilment of the Data Controller's obligations to respond to requests for exercising Data Subjects' rights including by communicating any useful information in order to help the Data Controller to comply with the duty to respect the rights of the Data Subjects. Group Members and External Data Processors will transmit to the Data Controller any Data Subject request without answering it unless the Group Member is authorized to do so.
- vi. **Sub-processing within the Group:** Personal data may be sub-Processed by other Group Members only with the prior informed specific or general written authorization of the Data Controller. The Service Agreement between the Group Member and the Data Controller will specify if a general prior authorization given at the beginning of the provision of services would be sufficient or if a specific authorization will be required for each new sub-Data Processor. If a general authorization is given, the Data Controller should be informed by the Group Member of any intended changes concerning the addition or replacement of a sub-Data Processor in such a timely fashion that the Data Controller has the possibility to object to the change before the Personal Data are communicated to the new sub-Data Processor and/or terminate the applicable contract which relates to the services which cannot be provided by the Group Member without the use of the objected-to sub-Data Processor (in accordance with terms and conditions of that contract).

- vii. **Onward transfers to External Data Processors:** Personal Data may be sub-Processed by External Data Processors only with the prior informed specific or general written authorization of the Data Controller. If a general authorization is given, the Data Controller should be informed by the Group Member of any intended changes concerning the addition or replacement of a External Data Processor in such a timely fashion that the Data Controller has the possibility to object to the change and/or to terminate the applicable contract which relates to the services which cannot be provided by the Group Member without the use of the objected-to External Data Processor (in accordance with terms and conditions of that contract) before the Personal Data are communicated to the new External Data Processor.

Where a Group Member bound by these BCRs sub-contracts its obligations under the Service Agreement with the Data Controller, with the authorization of the Data Controller, it shall do so only by way of a contract or other legal act under EU or EEA member state law with the sub-Data Processor which provides that adequate data protection is provided and which ensures that the same data protection obligations as set out in the Service Agreement between the Data Controller and the Group Member and Rules [1.3](#), [1.4](#), [3](#) and [6](#) of these BCRs are imposed on the sub-Data Processor, in particular it must ensure the sub-Data Processor guarantees to implement appropriate technical and organizational measures for Processing that are appropriate to the risk of Processing. The minimum data processing clause that must be contained in a sub-processor contract are set out in [Annex 6](#) (Data Processing Clauses).

Reference: Please see attached Annex 6 which contains Data Processing Clauses.

6.1.2 Accountability and other tools

Each Group Member will, according to the applicable Service Agreement, make available to the Data Controller all information necessary to demonstrate compliance with their data protection obligations and allow for and contribute to audits, including inspections conducted by the Data Controller or another auditor mandated by the Data Controller in accordance with the Service Agreement. In addition, the Group Member shall immediately inform the Data Controller if in its opinion, an instruction infringes the GDPR or other EU or EEA member state data protection law.

In order to demonstrate compliance with these BCRs, Group Members will maintain written records (which may be in electronic form) of all categories of Processing activities carried out on behalf of each Data Controller. This record shall include: (a) the name and contact details of the Data Processor(s) and of each Data Controller on behalf of which the Data Processor is acting, and, where applicable, of the Data Controller's or the Data Processor's representative, and the DPO; (b) the categories of Processing carried out on behalf of each Data Controller; (c) where applicable, transfers of Personal Data to a non-EEA country or an international organization, including the identification of that non-EEA country or international organization and, in the case of transfers necessary for the performance of a contract between the Data Subject and the Data Controller or the implementation of pre-contractual measures taken at the Data Subject's request, the documentation of suitable safeguards; and (d) where possible, a general description of the technical and organizational security measures to ensure a level of security appropriate to the risk of varying likelihood and severity for the rights and freedoms of natural persons, including:

- i. the pseudonymization and encryption of Personal Data;
- ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- iii. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- iv. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing..

These records will be made available to the Supervisory Authority upon request.

The Group Members shall also assist the Data Controller as described in the applicable Service Agreement in implementing appropriate technical and organizational measures to comply with data protection principles and facilitate compliance with the requirements of these BCRs in practice including the principle of data protection by design and by default.

6.2 Entities bound by these BCRs

The following list contains Ellucian Group Members that are bound by these BCRs. All of these Group Members can be contacted through the Group's DPO using privacy@ellucian.com.

Group Member	Registration Number	Country	Contact Details
Ellucian Ireland Limited	109961	Ireland	privacy@ellucian.com +1.703.261.2161
Ellucian Company L.P.	45-3767548	United States of America	privacy@ellucian.com +1.703.261.2161
Ellucian Netherlands B.V.	62790994	Netherlands	privacy@ellucian.com +1.703.261.2161
Ellucian UK Limited	10537345	United Kingdom	privacy@ellucian.com +1.703.261.2161
Ellucian Global Limited	7853571	United Kingdom	privacy@ellucian.com +1.703.261.2161
Ellucian SMS Ltd	7796864	United Kingdom, with a branch in the United Arab Emirates	privacy@ellucian.com +1.703.261.2161
Ellucian Technologies Canada ULC	C0925316	Canada	privacy@ellucian.com +1.703.261.2161
Ellucian Australia Pty Limited	ACN 154097248	Australia	privacy@ellucian.com +1.703.261.2161
Ellucian Singapore Private Limited	201925626M	Singapore	privacy@ellucian.com +1.703.261.2161
Ellucian Technology de Mexico, S. de RL de CV	RFC: ETM980123LR0	Mexico	privacy@ellucian.com +1.703.261.2161
Ellucian Tecnológica de Chile Limitada	RUT: 76182124-5	Chile	privacy@ellucian.com +1.703.261.2161
Ellucian Tecnología de Colombia SAS	NIT: 900782794-9	Colombia	privacy@ellucian.com

Group Member	Registration Number	Country	Contact Details
			+1.703.261.2161
Ellucian Higher Education Systems India Private Limited	AAQCS6720G	India	privacy@ellucian.com +1.703.261.2161
Ellucian Technologies, Unipessoal Limitada	516453599	Portugal	privacy@ellucian.com +1.703.261.2161

This list may be amended from time to time in accordance with [Rule 5.1](#).

6.3 Transparency when legislation prevents compliance with the BCRs

In accordance with [Rule 2.5](#), each Group Member shall continually assess whether it has reason to believe that the laws and practices in the non-EEA country of destination applicable to the Processing of the Personal Data by the Group Member importing the data (including any requirements to disclose Personal Data or measures authorizing access by public authorities) prevent the Group Member from fulfilling its obligations under the BCRs. If the laws and practices in the non-EEA country of destination applicable to the Processing of the Personal Data by the Group Member importing the data prevent it from fulfilling the instructions received from the Data Controller or its obligations under these BCRs or Service Agreement or otherwise have a substantial adverse effect on the guarantees provided by the BCRs, the Group Member shall, unless prohibited by law, promptly inform the Data Controller exporting the data and the DPO and comply with the procedure in [Annex 8](#) (Government Access Request) where applicable. The DPO will inform Ellucian Ireland Limited, the Data Controller (which may suspend the transfer of data and/or terminate the applicable contract which relates to the services which cannot be provided by the Group Member in compliance with these BCRs in accordance with terms and conditions of that contract) and the Data Controller's competent Supervisory Authority about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure, unless otherwise prohibited by law.

In the event notification to the Data Controller's competent Supervisory Authority is prohibited, the DPO and the Group Member will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can as soon as possible and to be able to demonstrate that it did so. If, despite having used its best efforts, the DPO on behalf of the Group Member is not in a position to notify the Data Controller's competent Supervisory Authority, the DPO on behalf of the Group Member shall annually provide general information on the requests it received to the Data Controller's competent Supervisory Authority including the number of applications for disclosure, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.

Group Members acknowledge that transfers of Personal Data by a Group Member to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

6.4 The relationship between national laws and BCRs

Group Members must Process Personal Data in accordance with the BCRs. Where the national legislation requires a higher level of protection for Personal Data, such national legislation shall take precedence over these BCRs.

In accordance with [Rule 2.5](#), each Group Member established outside the EEA warrants that it has no reason to believe that the laws and practices in the non-EEA country of destination applicable to the Processing of the Personal Data by the Group Member importing the data, including any requirements to disclose Personal Data or measures authorising access by public authorities, prevent the Group Member from fulfilling its obligations under the BCRs. In making this warranty, each relevant Group Member has undertaken an assessment in particular considering the elements set out in [Annex 7](#) (Transfer Risk Assessment) and has documented this assessment. Ellucian will make available a non-privileged summary of this assessment to a Supervisory Authority on request.

Where a Group Member importing the data from the EEA has reason to believe that it is or has become subject to laws or practices in the country of destination applicable to the Processing of the Personal Data by the Group Member importing the data, including following a change in the laws of the country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the warranty in [Rule 2.5](#), the Group Member importing the data from the EEA shall promptly notify the Data Controller exporting the data from the EEA and both parties shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted to address the situation. The Data Controller exporting the data shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured or if instructed by a competent Supervisory Authority to do so and/or may terminate the applicable contract which relates to the services which cannot be provided by the Group Member in accordance with applicable law where such termination is in accordance with terms and conditions of that contract. The Group Member importing the data will promptly inform the DPO of the issue in accordance with [Rule 6.3](#). The DPO will inform the Data Controller's competent Supervisory Authority unless prohibited by law. In the event notification to the Data Controller's competent Supervisory Authority is prohibited the DPO and the Group Member will follow the process in the second paragraph of [Rule 6.3](#).

Where a Group Member receives any legally binding request for disclosure of Personal Data by a law enforcement authority or becomes aware of any direct access by public authorities to Personal Data transferred pursuant to the BCRs it shall comply with the procedure in [Annex 8](#) (Government Access Requests).

Reference: Please see attached [Annex 7](#) which contains factors to consider in undertaking a transfer risk assessment and [Annex 8](#) which set out a procedure for dealing with government access requests.

Annex 1

Adoption Agreement

Annex 2

BCR Complaint Process Steps

BCR Complaint Process Diagram

Annex 3

BCR Audit Programme

Annex 4

Data Processing Particulars

Annex 5

Process for Changing Binding Corporate Rules

Annex 6

Data Processing Clauses

Annex 7

Transfer Risk Assessment

Annex 8

Government Access Requests

Annex 1

DATED

2023

ELLUCIAN IRELAND LIMITED

GROUP MEMBERS

**Adoption Agreement For
Controller Binding Corporate Rules (BCR-C) And
Processor Binding Corporate Rules (BCR-P)**

THIS AGREEMENT is made on 2023

BETWEEN

- (1) **ELLUCIAN IRELAND LIMITED**, a company incorporated under the laws of Ireland with registered number 109961, having its registered offices at 6th Floor, South Bank House, Barrow Street, Dublin 4, Ireland ("**Ellucian Ireland**"); and
- (2) The companies that have signed this agreement referred to as the "**Group Members**" and each individually as a "**Group Member**",

(each a "**party**" together the "**parties**").

BACKGROUND

- A. The worldwide group of Ellucian companies ("**Ellucian Group**") Processes and transfers Personal Data in compliance with the provisions of the General Data Protection Regulation (EU) 2016/679 ("**GDPR**").
- B. In order to provide for adequate protection for the transfer of Personal Data outside of the European Economic Area ("**EEA**") between the Group Members, Ellucian Ireland has introduced Controller Binding Corporate Rules ("**BCR-C**"). The BCR-C are binding on: (i) each Group Member acting as Data Controller (or acting as a Joint Controller); and (ii) each Group Member acting as a Data Processor on behalf of a Group Member acting as a Data Controller.
- C. Ellucian has also introduced Processor Binding Corporate Rules ("**BCR-P**") to provide for adequate protection for the transfer of Personal Data outside of the EEA between Group Members in their role as service provider on behalf of Ellucian Group's customers. The BCR-P are binding on each Group Member acting as a Data Processor or sub-Data Processor on behalf of a Data Controller which is not in the Ellucian Group.
- D. The BCRs provide the general regulatory framework for the Processing of Personal Data by Ellucian: (i) relating to Ellucian Group's employees, customers, suppliers, business partners or future business partners under the BCR-C; and (ii) Processed on behalf of Ellucian Group's customers under the BCR-P.
- E. The parties acknowledge that the Group Members have delegated responsibility to Ellucian Ireland to monitor and enforce the provisions of the BCRs such that Ellucian Ireland has the authority to conduct any claims or complaints made against a Group Member.
- F. Each Group Member adheres to the BCRs by entering into this Adoption Agreement either directly or through an Adherence Agreement. Each Group Member agrees to cooperate with Ellucian Ireland and any relevant regulators in relation to the BCRs. A Group Member may also be required to compensate Ellucian Ireland for any claims Ellucian Ireland must pay or settle on its behalf in relation to the BCRs.

IT IS AGREED

1. **Definitions**

- 1.1 “**BCRs**” as referred to in this Adoption Agreement shall mean the BCR-C and BCR-P and their respective Annexes.
- 1.2 “**Claim**” has the meaning given that term in Clause 3.1(c).
- 1.3 For purposes of this Adoption Agreement, any defined terms shall have the meaning given to that term in the BCRs and their Annexes.
- 1.4 Notwithstanding the above, these terms and expressions used herein shall always be interpreted in accordance with the GDPR.

2. **Scope**

- 2.1 By executing this Adoption Agreement, each Group Member undertakes to comply with all provisions of the BCRs and to implement and execute all the requirements of the BCRs. Each Group Member therefore commits to submit transfers of Personal Data to the data protection principles set forth in the BCRs.
- 2.2 The BCRs are an integral part of this Adoption Agreement and are attached to the Adoption Agreement as Appendix 1 and Appendix 2 respectively.

3. **Delegation of Authority**

- 3.1 Ellucian Ireland and each Group Member agree:
 - (a) Ellucian Ireland has authority to devise and implement rules and agreements related to the BCRs which will apply to all Group Members;
 - (b) Ellucian Ireland has the authority to liaise with the Irish Data Protection Commission, as the Lead Supervisory Authority of the Ellucian Group, and any other Supervisory Authority in any other EU jurisdiction in relation to the BCRs; and
 - (c) that the Group Members have delegated to Ellucian Ireland authority and primary liability for compensation claims, demands, and/or actions related to non-compliance with the BCRs by a Group Member (each a “**Claim**”) subject to Clause 10 below.

4. **Group Member Commitments**

- 4.1 The Group Member hereby specifically undertakes to comply with the following requirements:
 - (a) BCR compliance: to comply with all the provisions of the BCRs and to implement and execute all the requirements of the BCRs;
 - (b) BCR compliance before data transfer: to ensure the BCRs are properly implemented and complied with before any transfer of Personal Data takes place based on these BCRs;
 - (c) GDPR compliance (where applicable): comply at all times with the provisions of the GDPR;
 - (d) Appointment and availability of data protection support (where appropriate): ensure staff with adequate data protection expertise are available to support the DPO;

- (e) Monitoring compliance with the BCRs: ensure compliance with the BCRs through regular review and oversight;
- (f) Training and instruction of employees: ensure implementation of the BCRs by taking appropriate measures with regard to its employees and, specifically, instructing its employees in accordance with the relevant provisions of the BCRs;
- (g) Mutual assistance and cooperation: assist Ellucian Ireland and other Group Members to handle a request or complaint from a Data Subject and cooperate with the Supervisory Authorities where required, or assist other Group Members to handle a request or investigation by the Supervisory Authorities; and
- (h) Liability: accept the liability obligations contained in the BCRs in case of non-compliance with the BCRs.

4.2 In so far as a Group Member is a Data Processor on behalf of another Group Member or an Ellucian customer, the Group Member acting as Data Processor specifically undertakes to comply with the following requirements when Processing Personal Data:

- (a) it shall Process any Personal Data only as instructed by the Data Controller and for no other purpose and shall immediately inform the Data Controller if, in its opinion, an instruction infringes applicable data protection law;
- (b) it shall comply with all of the obligations of a Data Processor under the GDPR;
- (c) it shall treat and ensure all employees treat all Personal Data Processed by it as confidential;
- (d) it shall only engage sub-Data Processors to Process the Personal Data with the authorisation of the Data Controller and subject to contractual terms no less protective than this Clause 4.2;
- (e) it shall upon written request from the Data Controller provide all information necessary to demonstrate compliance with this Clause 4.2, and will at its own cost implement any further steps that are necessary for such compliance;
- (f) it shall take all technical and organisational measures relevant to:
 - (i) secure Personal Data Processed by it;
 - (ii) assist the Data Controller in ensuring its obligations in responding to requests from Data Subjects in relation to their rights under Articles 15 to 22 of the GDPR; and
 - (iii) assist the Data Controller in ensuring compliance with its obligations pursuant to Articles 32 to 36 of the GDPR, including in relation to data breaches and data protection impact assessments,
 and
- (g) it shall, at the choice of the Data Controller, delete or return all the Personal Data to the Data Controller at the end of the provision of the services related to the Processing.

5. **Third Party Beneficiary**

- 5.1 The Group Member hereby confirms that, with respect to Personal Data falling within the scope of the BCRs, any Data Subject shall be entitled, as a third party beneficiary, to seek to enforce compliance by the Group Member with the clauses of the BCRs which confer benefits to third parties and to assert claims for compensation or damages resulting from a breach by the Group Member of such clauses.
- 5.2 In so doing, the Data Subject may, in relation to non-compliance with the relevant clauses of the BCRs:
- (a) lodge a complaint with a Supervisory Authority, in particular in the Member State where: (i) the Data Subject habitually resides; (ii) the Data Subject has their place of work; or (iii) the alleged infringement occurred; and
 - (b) seek effective judicial remedy and, where appropriate, compensation, by bringing proceedings before the competent courts of the Member State where: (i) the Group Member exporting Personal Data outside of the EEA is established; (ii) where Ellucian has an establishment in the EEA; or (iii) where the Data Subject habitually resides.

6. **Accession**

- 6.1 An Ellucian Group company may accede to the BCRs by executing the Adoption Agreement. Accession to the BCRs shall be effective as of the date of signature of this Adoption Agreement by the relevant Ellucian Group company, which shall then become a Group Member.
- 6.2 An Ellucian Group company which has not signed up to the Adoption Agreement may accede to the BCRs by signing the Adherence Agreement in substantially the form set out in Appendix 3, with accession to the BCRs effective as of the date of signature of the Adherence Agreement by the relevant Ellucian Group company, which then becomes a Group Member.

7. **Default**

- 7.1 If non-compliance is identified through an audit, by a Supervisory Authority or otherwise, the Group Member shall rectify the identified non-compliance without delay. Such non-compliance shall be notified to the DPO, vice president of compliance, and/or the Compliance Committee, depending on the nature of the issue. The DPO will be kept informed of resolution measures, will oversee resolution measures and will direct any suspension and resumption of data transfers to that Group Member. If non-compliance persists and is not resolved without undue delay, then the DPO shall remove the Group Member from the BCRs and the DPO will notify the Lead Supervisory Authority.
- 7.2 Ellucian Ireland may also deem a Group Member as withdrawn from the BCRs pursuant to Clause 8.3.

8. **Withdrawal**

- 8.1 Withdrawal by any Group Member is effective as per the date indicated in the Withdrawal Notice at Appendix 4, such date being no earlier than one (1) month from the date of receipt of such notice by the DPO (the “**Withdrawal Date**”).

- 8.2 Withdrawal from the BCRs is required for each Group Member that ceases to belong to the Ellucian Group or that wishes to terminate its participation with the BCRs. Such Group Member must immediately inform the DPO.
- 8.3 Without prejudice to Clause 7, withdrawal of a Group Member from the BCRs may also be decided unilaterally by the DPO in the event that a Group Member has committed a material breach of the BCRs and has not remedied such breach without undue delay from the date on which it has been asked to remedy it.
- 8.4 Withdrawal is conducted without prejudice to all obligations and liabilities under the BCRs and especially Clause 10.
- 8.5 Withdrawal of a Group Member from the BCRs will terminate the Adoption Agreement concluded between that Group Member and Ellucian Ireland, without prejudice to the rights and obligations accrued between these parties, before the withdrawal becomes effective, under Clauses 5 and 10. Withdrawal of a Group Member shall not affect the continuity of the Adoption Agreement between Ellucian Ireland and any other Group Members.
- 8.6 Upon withdrawal of a Group Member from the BCRs, the Group Member and any Group or external sub- Data Processors shall delete or return all the Personal Data Processed pursuant to the BCRs and delete the copies thereof according to the Group's then-applicable data retention and disposal policies. If applicable law requires the Group Member or any Group Data Processor or External Data Processor to continually store the Personal Data, then the Group Member and any Group Data Processor or External Data Processors shall agree with the Group Member or Ellucian customer exporting the Personal Data that the Personal Data may be retained by the Group Member. The Group Member shall warrant that: (i) the Personal Data will be retained in accordance with Articles 45 or 46 of the GDPR (as applicable) unless one of the derogations pursuant to Article 49 of the GDPR applies; and (ii) it will, and will ensure any Group Data Processors or External Data Processors will, guarantee the confidentiality of the Personal Data and will not further Process the Personal Data otherwise than as required by the relevant law. The Group Member will also: (i) inform the DPO of the continued retention of the Personal Data and the reasons for continued retention; and (ii) on request, certify to the DPO that it has complied with this Clause 8.6.

9. Confidentiality

- 9.1 All information disclosed by the Group Members or its advisors with regard to the Adoption Agreement or the BCRs before, during or after the termination of the Adoption Agreement in oral, written, graphic, photographic, recorded, or any other form shall be deemed to be "**Confidential Information**".
- 9.2 However, the following information shall not be regarded as Confidential Information for the purpose of this Adoption Agreement:
- (a) any information that is or falls into the public domain, or is known by professionals in the sector, other than as a result of a breach of this Adoption Agreement or any other confidentiality obligation;
 - (b) any information that has been disclosed to a Group Member in good faith by a third party that is not bound by a confidentiality obligation;
 - (c) any information a Group Member had knowledge of prior to the start of discussions regarding the Adoption Agreement;

- (d) any information that the Group Members agree in writing can be freely disclosed or used, or any information that has been expressly agreed between the Group Members as not confidential; or
 - (e) any information that a Group Member is required to disclose pursuant to a judgment rendered by a competent court or tribunal, or any statutory or regulatory provisions.
- 9.3 This confidentiality obligation shall continue in full force and effect for the term of the Adoption Agreement and shall continue in full force for five (5) years from the date the Adoption Agreement is terminated for any reason whatsoever.

10. **Indemnity**

- 10.1 Each Group Member hereby indemnifies Ellucian Ireland for any damages, loss or expense (including legal fees) incurred by Ellucian Ireland in relation to the Group Member and the BCRs, including:
- (a) any Claim, subject to Clauses 10.2 to 10.4; and/or
 - (b) any administrative fine levied on Ellucian Ireland for any default directly or indirectly by a Group Member (a “**Fine**”).
- 10.2 The Group Member shall forthwith notify Ellucian Ireland if a Claim is brought against the Group Member.
- 10.3 In the event of any Claim being initiated against the Group Member, Ellucian Ireland may, at any time and at its discretion, and at the Group Member’s expense:
- (a) take over conduct of the Claim on behalf of the Group Member. As and from the date that Ellucian Ireland takes over conduct of the Claim, the Group Member agrees to grant Ellucian Ireland exclusive control of the conduct of the Claim including any negotiations in connection therewith and provide Ellucian Ireland with full cooperation and support in the conduct of such Claim (including by the prompt provision of any information required by Ellucian Ireland); or
 - (b) allow the Group Member to retain conduct of the Claim.
- 10.4 The Group Member shall:
- (a) as soon as reasonably practicable, give written notice of the Claim to Ellucian Ireland, specifying the nature of the Claim in reasonable detail;
 - (b) not make any admission of liability, agreement or compromise in relation to the Claim without the prior written consent of Ellucian Ireland;
 - (c) should Clause 10.3(b) apply, the Group Member may, with Ellucian Ireland’s prior written consent, settle the Claim;
 - (d) give Ellucian Ireland and its professional advisers access at reasonable times (on reasonable prior notice) to its premises and its officers, directors, employees, agents, representatives or advisers, and to any relevant assets, accounts, documents and records within the power or control of the Group Member, so as to enable Ellucian Ireland and its professional advisers to examine them and to take copies for the purpose of assessing the Claim; and

- (e) take such action as Ellucian Ireland may reasonably request to avoid, dispute, compromise or defend the Claim.

11. Notices

- 11.1 Notices or communications to a Group Member should be sent to the Group Member's registered address or any other address which may be agreed in writing by the parties.
- 11.2 Any notice for Ellucian Ireland should be sent to the DPO by email to privacy@ellucian.com.

12. Amendments

- 12.1 This Adoption Agreement may be amended by the DPO of the Ellucian Group by giving prior written notice of such amendment to all Group Members. Such amendment shall be effective within ten (10) business days of receipt of such notice, unless a timely written objection is received by the DPO. If any Group Member provides a timely objection to a proposed amendment within this 10 day period, that Group Member shall promptly commence discussions with the DPO to reach an outcome satisfactory to all Group Members. Any amendment must comply with guidance from or adopted by the European Data Protection Board.
- 12.2 Ellucian Ireland will inform all relevant Supervisory Authorities via the Lead Supervisory Authority of changes to the BCRs either promptly for any change that would possibly affect the level of protection offered by the BCRs or annually for other changes.

13. Counterparts

This Adoption Agreement may be executed in any number of counterparts, each of which shall constitute an original, and all of which taken together shall constitute one and the same instrument.

14. Applicable Law and Competent Jurisdiction

- 14.1 This Adoption Agreement and any disputes or claims (including non-contractual disputes or claims) arising out of or in connection with it, its subject matter or formation shall be governed by and construed in accordance with the laws of Ireland.
- 14.2 Each party irrevocably agrees that the courts of Ireland shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Adoption Agreement or its subject matter or formation.
- 14.3 For the avoidance of doubt, Clauses 14.1 and 14.2 do not apply to claims brought by Data Subjects pursuant to Clause 5.

By their signatures, the authorized representatives of the Group Members acknowledge the Group Members' acceptance of this Adoption Agreement, which was made in as many originals as there are Group Members, each Group Member acknowledging having received one original:

Name: [●]

Title: [●]

Signed for and on behalf of **ELLUCIAN IRELAND LIMITED**

Name: [●]

Title: [●]

Signed for and on behalf of [COMPANY]

Appendix 1

BCR-P

Appendix 2

BCR-C

Appendix 3

Adherence Agreement

PARTIES

1. The persons named in Schedule 1 as the existing Group Members ("**Existing Group Members**");
2. **ELLUCIAN IRELAND LIMITED** a company incorporated under the laws of Ireland with registered number 109961, having its registered office at 6th Floor, South Bank House, Barrow Street, Dublin 4, Ireland ("**Ellucian Ireland**"); and
3. [NEW COMPANY JOINING BCR] of [INDIVIDUAL ADDRESS] ("**New Group Member**")

BACKGROUND

The New Group Member has agreed to execute this agreement under which it shall adhere to and be bound by the Adoption Agreement under which it agrees to comply with the provision of the BCRs.

IT IS AGREED

1. Interpretation

- 1.1 The following definitions and rules of interpretation apply in this agreement.
 - (a) "**Effective Date**" means [DATE].
 - (b) "**Adoption Agreement**" means the agreement in relation to the BCRs made between the Existing Group Members, as amended or supplemented from time to time.
- 1.2 Unless the context otherwise requires, words and expressions used in this agreement shall have the meaning given to them in, and shall be interpreted in accordance with, the Adoption Agreement.

2. Adherence to Adoption Agreement

The New Group Member confirms that it has been supplied with a copy of the Adoption Agreement. The New Group Member, Ellucian Ireland and each of the Existing Group Members undertake with each other and with any other person who becomes a party to the Adoption Agreement after the date of this agreement to be bound by, observe and perform the Adoption Agreement as if the New Group Member had been an original party to the Adoption Agreement and was named in the Adoption Agreement.

3. Counterparts

This agreement may be executed in any number of counterparts, each of which when executed and delivered shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement.

4. **Governing Law and Jurisdiction**

- 4.1 This agreement and any disputes or claims (including non-contractual disputes or claims) arising out of or in connection with it, its subject matter or formation shall be governed by and construed in accordance with the laws of Ireland.
- 4.2 Each party irrevocably agrees that the courts of Ireland shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this agreement or its subject matter or formation.

Schedule 1 to Appendix 3

Existing Group Members

This agreement is hereby executed by the parties below to take effect as of the Effective Date.

Name: [●]

Title: [●]

Signed for and on behalf of **ELLUCIAN IRELAND LIMITED**

Name: [●]

Title: [●]

Signed for and on behalf of [NEW GROUP MEMBER]

Appendix 4

Withdrawal Notification

Data Protection Officer

Ellucian Ireland Limited

privacy@ellucian.com

Re: Withdrawal from the BCRs

Dear [●],

In accordance with Clause 8 of the Adoption Agreement dated [DATE] and entered into by [NAME OF COMPANY] on [DATE], [NAME OF COMPANY] hereby notify its will to withdraw from the Adoption Agreement for the following reason: [CHOOSE THE REASON]

[NAME OF COMPANY] has ceased to belong to the Ellucian Group on [DATE]

[OR]

[NAME OF COMPANY] wishes to terminate its participation to the [BCR-C and/or BCR-P] with effect on [DATE].

Yours sincerely,

[NAME OF COMPANY]

Annex 2

Binding Corporate Rules (“BCRs”) Complaint Resolution Process

This Annex relates to Rule 2.2 of the BCRs and sets out the process that applies when Ellucian receives a complaint from a Data Subject regarding Ellucian’s compliance with the BCRs.

Time	Step	Process Flow
Days 1 – 4*	Ellucian receives request or complaint	Complaints should be submitted to privacy@ellucian.com or by calling +1 703 261 2161 or by sending a complaint by post to Data Protection Officer, Ellucian, 4 Country View Road, Malvern, PA 19355, USA or any other method stated in Ellucian’s privacy statement or privacy policy relating to employee data . If someone outside the legal department receives the complaint, that person should forward to privacy@ellucian.com
	Add to log	A member of Privacy team adds the complaint to the BCR complaint log here . The data protection officer (DPO) or the DPO’s delegate shall be assigned to the complaint. That person’s name is noted in the log.
	Review complaint and determine next steps	The reviewer reviews the complaint and determines next steps.
	Notify the Data Controller of the complaint	Notify the Data Controller of the complaint without undue delay and follow the Data Controller’s instructions. Where the Data Controller has disappeared, ceased to exist or become insolvent OR Ellucian has agreed to handle the complaint on behalf of the Data Controller then please proceed to the following steps.
	If applicable, go back to the data subject requesting more information	If Ellucian needs additional information to address the complaint, request that information from the Data Subject, or request a meeting with the Data Subject to discuss.
Days 5-18*	Investigate complaint	The DPO or the DPO’s delegate investigates the complaint. This investigation will follow Ellucian’s Legal Matters and Investigation Policy here .
	Inform data subject if additional time needed	If, due to the complexity or number of complaints, Ellucian requires more time to investigate, Ellucian will notify the Data Subject within the initial one month period that time to respond will be extended at maximum by two further months.

Time	Step	Process Flow
Days 19-28*	Determine resolution	Based on the investigation, Ellucian's DPO or the DPO's delegate will determine what action(s) need to be taken to resolve the complaint. The DPO will also determine a time frame during which such actions will be taken. Complaints should be resolved without undue delay and within one month unless an extension is needed as described above.
	Response to data subject	Ellucian's DPO will provide a written response to the Data Subject. That response will contain, at a minimum: - Consequences in case of rejection of the complaint, - Consequences in case the complaint is considered as justified, - Consequences if the Data Subject is not satisfied by the replies (right to lodge a claim before a competent court and/or a complaint before a Supervisory Authority).

Annex 3

Binding Corporate Rules (BCRs) Audit Programme

This Annex relates to Rule 2.3 of the BCRs.

On a yearly basis, the Group will conduct data protection audits to verify compliance with all aspects of these BCRs including methods and action plans ensuring that corrective actions have been implemented. When appropriate, data protection audits of external sub-Data Processors will be conducted based on the level of risk posed by the Processing of that sub-Data Processor. These audits will be carried out by either internal or external accredited auditors or on specific request to the data protection officer (DPO) from the executive team or the board of directors.

The main systems for which Ellucian engage vendors are: cloud services for customer data processing, secure content management, HR management, expense, travel and invoice management, document and corporate email systems, business communication systems, workflow management and customer relationship management systems.

The Group will conduct audits or request evidence of compliance with third party audits as appropriate, taking into account the risk posed by the processing undertaken by that vendor.

Further, at the request of the Data Controller, any Group Member will submit to an audit of their data processing facilities relating to the processing activities of that Data Controller. These audits will be carried out by the Data Controller or an independent professionally-accredited inspection body bound by a duty of confidentiality selected by the Data Controller, in agreement with the Supervisory Authority (where applicable). In relation to the hosting of customer data, Amazon Web Services ("AWS"), is externally audited for SOC 2 Type II certification every year and the Group is provided with evidence of this certification.

Vendors that do not engage in high risk processing (by nature of volume) will be audited on a 2-3 year basis.

Results of data protection audits will be reported to the DPO, who will then report to the Compliance Committee. The DPO or other members of the Compliance Committee will report to the audit committee of the board of directors at least annually regarding compliance.

If non-compliance is identified through an audit, by a Supervisory Authority or otherwise, the Group Member shall rectify the identified non-compliance without delay. Such non-compliance shall be notified to the DPO, vice president of compliance, and/or the Compliance Committee, depending on the nature of the issue. The DPO will be kept informed of resolution measures, will oversee resolution measures and will direct any suspension and resumption of data transfers to that Group Member. If non-compliance persists and is not resolved without undue delay, then the DPO shall remove the Group Member from the BCR and the DPO will notify the Lead Supervisory Authority.

Reports of data protection audits will be made available to the relevant Data Controller(s) and the Data Controller's competent Supervisory Authority upon request.

Supervisory Authorities may carry out a data protection audit of any Group Member if required.

The specific activities and controls audited may vary from audit to audit. The DPO, working with individuals in the Group who are qualified as auditors or external auditors, will set an audit plan at least once per year that will describe the specific audit activities for the subsequent twelve (12) months.

Additional audits may be conducted on an *ad hoc* basis for example in response to a suspected data breach has occurred or as part of a data protection impact assessment process for vendors that undertake processing that the Group deems to represent a high risk.

Annex 4

Data Processing Particulars

Customer Data

Categories of Data Subjects

Ellucian's customers' current and former (a) students, (b) prospective students, (c) parents or benefactors of students or prospective students, (d) alumni, (e) faculty members, (f) administration, (g) employees, (h) prospective employees, (i) vendors / contractors / agents, and (j) donors.

Categories of Personal Data

Category of Data	Type of Data	Purpose of Processing
Name and Initials	First name / initial	- Management and development of Group's business relation; - Providing goods and services as described in contracts between Group Affiliates and customers; - Decision-making with regards to the development and operation of Group business.
	Middle name / initial	
	Last name(s)	
	Initials	
Education and Professional Qualifications	Enrolment Information	- Management and development of Group's business relation; - Providing goods and services as described in contracts between Group Affiliates and customers; - Decision-making with regards to the development and operation of Group business.
	Degrees and schooling Information	
	Licenses and professional memberships	
	Professional certification	
Personal characteristics	Age	- Management and development of Group's business relation; - Providing goods and services as described in contracts between Group Affiliates and customers; - Decision-making with regards to the development and operation of Group business.
	Date of birth	
	Birth certificate number	
	Gender	
	Height	
	Weight	
	Marital status	
	Nationality	
	Leisure and interests	
	Photographs and video	
	Information about a person's children/family	
Personal Contact Information	Home postal address	- Management and development of Group's business relation; - Providing goods and services as described in contracts between Group Affiliates and customers; - Decision-making with regards to the development and operation of Group business.
	Home telephone number	
	Home facsimile number	
	Personal electronic mail address	
	Personal cellular, mobile or wireless number	
Business Contact Information	Business postal address	- Management and development of Group's business relation; - Providing goods and services as described in contracts between Group Affiliates and customers; - Decision-making with regards to the development and operation of Group business.
	Business telephone number	
	Business facsimile number	
	Business electronic mail address	
	Business cellular, mobile or wireless number	

	Personal assistant contact information	
IT and Facility Access/Login Info	User name	• Management and development of Group's business relation; • Providing goods and services as described in contracts between Group Affiliates and customers; • Decision-making with regards to the development and operation of Group business.
	Password	
	Use of IT assets or facilities	
	IP address	
	Mobile Device ID	
Professional and Employment	Occupation / title	• Management and development of Group's business relation; • Providing goods and services as described in contracts between Group Affiliates and customers; • Decision-making with regards to the development and operation of Group business.
	Income / salary / service fees / other compensation	
	User identification and / or employee number as assigned by an employer	
	Employment history, evaluations and disciplinary actions	
	Digitized or other electronic signature	
	Date of hire	
	Other information relating to employee job (such as company/employer name, department number, supervisor)	
	Standard hours	
	Performance ratings	
	Emergency contact details	
	Absences and leaves	
	Information relating to benefits	
	Information relating to expenses	
	Information relating to bonus	
	Resume and summary of work experience and education	
	Training courses completed	
	Job position being applied for	
Other Confidential Information	National identification number (including SSN in US)	• Management and development of Group's business relation; • Providing goods and services as described in contracts between Group Affiliates and customers; • Decision-making with regards to the development and operation of Group business.
	State/province-issued identification number	
	Driver's or operator's license number	
	Passport number	
	Alien registration number	
	Other government-issued identification number (e.g. country-identification)	
	Mother's maiden name	
Financial Information/Payment Card Industry Information	Financial institution account number	• Management and development of Group's business relation; • Providing goods and services as described in contracts between Group Affiliates and customers; • Decision-making with regards to the development and operation of Group business.
	Any required security code, access code, or password that would permit access to an individual's financial account	
	Details of financial transactions or account	

	Information (e.g., account balance Information, payment history, overdraft history, and credit or debit card purchase information)	
	Credit / debit card number	
	Cardholder name	
	Expiration date	
	Service code	
	CVV, CVC2, CID number (code verification value code)	
	PIN data	
	Insurance claim information	
	Credit report information	
Wealth/asset information	Information about a person's wealth, holdings, and financial stability	• Management and development of Group's business relation; • Providing goods and services as described in contracts between Group Affiliates and customers; • Decision-making with regards to the development and operation of Group business.
Legal/litigation hold	Data subject to litigation holds or e-discovery	• Management and development of Group's business relation; • Providing goods and services as described in contracts between Group Affiliates and customers; • Decision-making with regards to the development and operation of Group business.
Special categories of personal data	Racial or ethnic origin	• Management and development of Group's business relation; • Providing goods and services as described in contracts between Group Affiliates and customers; • Decision-making with regards to the development and operation of Group business.
	Political opinions	
	Religious or philosophical beliefs	
	Trade Union Membership	
	Genetic data	
	Data concerning health	
	Medicare or Medicaid number	
	Sex life or sexual orientation	
	Background check results	
Criminal data	Criminal convictions or offences	• Management and development of Group's business relation; • Providing goods and services as described in contracts between Group Affiliates and customers; • Decision-making with regards to the development and operation of Group business.

Annex 5

Process for Changing Binding Corporate Rules (BCRs)

This Annex relates to Rule 5.1 and sets out the process to be followed any time the Ellucian Binding Corporate Rules for Processors (BCRs) need to be updated.

Step	Process Flow
Monitor obligations and list of BCR Group Members and sub-Data Processors	The data protection officer (DPO) or his/her delegate shall keep a fully updated list of the BCR Group Members and External Data Processors which it shall provide to the Data Controllers, the Supervisory Authorities and Data Subjects on request and keep track of and monitors regulatory changes that may impact the BCRs and provide the necessary information on such updates to the Data Controllers and to the Supervisory Authorities on request.
What changes are needed?	Compliance team and/or the data protection officer (DPO) determines that changes needed to BCRs because of legal/regulatory requirements or company structure or operations.
Consult with the business	Compliance team consults with impacted business units regarding the changes Compliance team drafts changes to the BCRs based on input from the business Compliance team sends draft updates to impacted business team(s) for review and comment Repeat this step until the proposed updates are accurate and contain the information legally required.
Compliance approval	VP of Compliance to review and approve. If changes are needed, repeat the steps listed above until the updates are approved. If applicable (check with VP of Compliance if unsure), discuss with the Compliance Committee before posting.
Inform Data Controller(s)*	The DPO or his/her delegate shall inform relevant Data Controllers of the changes in a timely fashion so that the Data Controller has the possibility to object to the change or to terminate the applicable contract (in accordance with that contract's terms and conditions) which relates to services which cannot be provided by the Group Member without such modification before the modification is made (for instance, on any intended changes concerning the addition or replacement of sub-Data Processors, before the data is provide to the new sub-Data Processor).
Post	The updated BCRs will be posted to any internal and external website where the prior version of the BCRs had been posted. The DPO will keep a record of all BCR changes made.
Inform Group Members	The DPO will inform Group management of the changes without undue delay and will notify all Group Members of changes applicable to that Group Member without undue delay. No transfers of personal data should be made to a new Group Member before the new Group

Step	Process Flow
	Member is effectively bound by the BCRs and can deliver compliance with the BCRs.
Inform Supervisory Authority of updates	The DPO will inform the competent Supervisory Authority annually of changes to the BCRs including any changes to the Annexes or list of Group Members, with a brief explanation of the reasons justifying the update. However, notification will be made promptly to the relevant Supervisory Authorities via the competent Supervisory Authority for any change that would possibly affect the level of protection offered by the BCRs (<i>i.e.</i> , changes to the binding character).

Annex 6

Data Processing Clauses

In the context of Rule 6.1.1, a Data Processor who discloses or provides access to Personal Data by a sub-Data Processor wherever located is obliged to enter into a written contract with the sub-Data Processor. The written processor contract must include at least the following provisions:

1. a description of the subject matter and duration of Processing, the nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects;
2. the sub-Data Processor shall Process Personal Data only in accordance with the Data Processor's documented instructions, including with regard to transfers, inform the Data Processor if an instruction infringes the GDPR and if the sub-Data Processor it shall promptly inform the Data Processor of its inability to comply and the Data Processor shall be entitled to suspend the transfer of Personal Data and/or terminate the applicable contract;
3. the sub-Data Processor shall ensure that all persons authorized to Process the Personal Data have committed to keep the data confidential either under an appropriate statutory duty of confidentiality or on the basis of an imposed duty of confidentiality;
4. the sub-Data Processor shall take appropriate technical and organizational measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, including as appropriate: (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing;
5. the sub-Data Processor shall only enlist a sub-sub-Data Processor with the prior specific or general written authorization of the Data Processor and if general authorization is provided the Data Processor shall inform the Data Processor of any intended changes, additions or replacements to sub-sub-Data Processors and give the Data Processor an opportunity to object to such changes and/or terminate the applicable contract ;
6. the sub-Data Processor shall impose on the sub-sub-Data Processor the same obligations as imposed on the sub-Data Processor under the data Processing clauses and remain fully liable to the Data Processor for the performance of the sub-sub-Data Processor's obligations;
7. the sub-Data Processor shall assist the Data Processor with regard to the Data Controller's obligations under the GDPR, in so far as this is possible for the fulfilment of the Data Controller's obligation to respond to requests for exercising Data Subject rights;
8. the sub-Data Processor shall assist the Data Processor with regard to the Data Controller's obligations and in respective of data security, Personal Data Breach notifications to Supervisory Authorities and Data Subjects (where relevant) and data protection impact assessments;
9. the sub-Data Processor shall, upon the Data Processor's request, delete or return all the Personal Data to the Data Controller after the end of the provision of data Processing services, and delete existing copies unless applicable law requires storage of the Personal Data; and
10. the sub-Data Processor shall make available to the Data Processor and/or the Data Controller all information necessary to demonstrate compliance with the data Processing clauses and

shall submit its relevant data Processing facilities to audits and inspections by the Data Processor and/or the Data Controller, an external auditor appointed by the Data Processor and/or the Data Controller or any Supervisory Authority.

Annex 7

Transfer Risk Assessment

This Annex relates to Rule 2.5 and Rule 6.4 and sets out the elements that should be considered when undertaking a transfer risk assessment:

1. the specific circumstances of the transfer, including:
 - 1.1 the content and duration of the processing;
 - 1.2 the scale and regularity of transfers;
 - 1.3 the length of the processing chain;
 - 1.4 the number of actors involved and the transmission channels used;
 - 1.5 the type of recipients;
 - 1.6 the purpose of processing;
 - 1.7 the nature of the personal data transferred; and
 - 1.8 any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the Group Member for the type of personal data transferred;
2. the laws of the country in which the Group Member is established in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities, as well as the applicable limitations and safeguards; and
3. any safeguards in addition to those under the BCRs, including the technical and organisational measures applied during transmission and to the processing of the personal data in the country of destination in which the Group Member is established.

Annex 8

Government Access Requests

This Annex relates to Rule 2.5, Rule 6.3 and Rule 6.4 of the BCRs.

1. Where a Group Member outside the EEA receives a legally binding request for disclosure of Personal Data by a law enforcement authority or becomes aware of any direct access by public authorities to Personal Data transferred pursuant to the BCRs it shall promptly inform:
 - 1.1 the Data Controller,
 - 1.2 the DPO (and the DPO shall inform Ellucian Ireland Limited and the Data Controller's competent Supervisory Authority), and
 - 1.3 the Data Subject (where possible).
2. Such notification under paragraph 1 should include, where available: details of the Personal Data requested, the requesting authority, and the legal basis for the disclosure, to the extent permitted by applicable law.
3. In the event notification to the Group Member exporting the data from the EEA, the Data Controller, the DPO, the Data Subjects and/or competent Supervisory Authority is prohibited, the Group Member will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can as soon as possible and to be able to demonstrate that it did so. If, despite having used its best efforts, the DPO, on behalf of the Group Member, is not in a position to notify the competent Supervisory Authority, it shall annually provide general information on the requests the Group has received (e.g. number of applications for disclosure, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.) to the competent Supervisory Authority
4. The Group Member outside the EEA agrees to preserve the information pursuant to paragraphs 2 and 3 above for the duration of the Processing of Personal Data and make a non-privileged summary of this information available to any Supervisory Authority upon request.
5. The Group Member agrees to review, under the laws of the country of destination, the legality of the request for disclosure, notably whether it remains within the powers granted to the requesting public authority, and to exhaust all available remedies to challenge the request if, after a careful assessment, it concludes that there are grounds under the laws of the country of destination to do so. When challenging a request, the Group Member shall seek interim measures with a view to suspend the effects of the request until the court has decided on the merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. These requirements are notwithstanding the obligations of the Group Member pursuant to Rule 6.3 (i.e. the obligation to notify the DPO if it has reason to believe it cannot comply with the BCRs).
6. The Group Member outside the EEA agrees to document its legal assessment as well as any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make such assessment available to the Group Member exporting the data from the EEA. It shall also make a non-privileged summary of this assessment available to any Supervisory Authority upon request.
7. The Group Member outside the EEA agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.