



Binding Corporate Rules - Ellucian as Data Controller

Table of Contents

BACKGROUND	3
PURPOSE	3
DEFINITIONS	3
1 BINDING NATURE	4
1.1 THE DUTY TO RESPECT THE BCRs	4
1.2 BINDING NATURE OF BCRs	4
1.3 THIRD-PARTY BENEFICIARY RIGHTS	4
1.4 ELLUCIAN IRELAND LIMITED ACCEPTS LIABILITY.....	6
1.5 [NOT USED].....	6
1.6 BURDEN OF PROOF LIES WITH ELLUCIAN AND NOT THE INDIVIDUAL DATA SUBJECT	6
1.7 TRANSPARENCY AND EASY ACCESS TO BCRs	6
2 EFFECTIVENESS.....	7
2.1 THE EXISTENCE OF A SUITABLE TRAINING PROGRAMME	7
2.2 THE EXISTENCE OF A COMPLAINT HANDLING PROCESS FOR THE BCRs	7
2.3 THE EXISTENCE OF AN AUDIT PROGRAMME COVERING THE BCRs	7
2.4 THE CREATION OF A NETWORK OF DATA PROTECTION OFFICERS (DPO) OR APPROPRIATE STAFF FOR MONITORING COMPLIANCE WITH THE BCRs.....	8
2.5 ON-GOING ASSESSMENT OF THE EFFECTIVENESS OF THE BCRs	8
3 DUTIES OF COOPERATION.....	9
3.1 DUTY TO COOPERATE WITH SUPERVISORY AUTHORITIES.....	9
4 DESCRIPTION OF PROCESSING AND DATA FLOWS	9
4.1 MATERIAL SCOPE OF THE BCRs.....	9
4.2 GEOGRAPHICAL SCOPE OF THE BCRs	9
5 MECHANISMS FOR REPORTING AND RECORDING CHANGES	9
5.1 PROCESS FOR UPDATING THE BCRs.....	9
6 DATA PROTECTION SAFEGUARDS	9
6.1.1 DATA PROTECTION PRINCIPLES.....	9
6.1.2 ACCOUNTABILITY AND OTHER TOOLS.....	11
6.2 ENTITIES BOUND BY THESE BCRs.....	12
6.3 TRANSPARENCY WHEN LEGISLATION PREVENTS COMPLIANCE WITH THE BCRs	13
6.4 THE RELATIONSHIP BETWEEN NATIONAL LAWS AND BCRs	13
ANNEX 1.....	15
ADOPTION AGREEMENT	15
ANNEX 2.....	15
PRIVACY NOTICE INFORMATION	15
ANNEX 3.....	15
BCR COMPLAINT PROCESS IN WRITTEN STEPS.....	15
BCR COMPLAINT PROCESS DIAGRAM.....	15
ANNEX 4.....	15
BCR AUDIT PROGRAMME	15
ANNEX 5.....	15
DATA PROCESSING PARTICULARS	15
ANNEX 6.....	15
PROCESS FOR CHANGING BINDING CORPORATE RULES	15
ANNEX 7.....	15
DATA SUBJECT RIGHTS	15
ANNEX 8.....	15
DATA PROCESSING CLAUSES.....	15
ANNEX 9.....	15
RECORD OF PROCESSING ACTIVITIES	15
ANNEX 10.....	15
TRANSFER RISK ASSESSMENT	15
ANNEX 11.....	15

BACKGROUND

Data protection laws govern how Ellucian handles Personal Data in each country in which we operate. Where Ellucian Processes Personal Data of job applicants, employees, website visitors and personnel and staff of our customers, partners, vendors, third-party suppliers and contractors for Ellucian's own purposes (as opposed to on behalf of our customers), we are a Data Controller (as defined below).

There are specific 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 European Union (“**EU**”) laws is 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 Controller under these BCRs;
- explain the scope and application of these BCRs;
- define the data protection principles Ellucian will abide by;
- define Ellucian employees' data protection responsibilities and accountability for implementing and complying with these BCRs;
- explain how Ellucian handles complaints and Data Subjects' 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 Controllers and the Annexes which are applicable to and binding on each Group Member.

Data Controller means the 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 Data Processor not in the Group which is 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: (i) acts as a Data Controller; or (ii) acts as a Data Processor on behalf of a Group Member acting as a Data Controller.

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.

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, organization, 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.

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

These rules 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.

1.2 Binding nature of BCRs

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

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 rules.

[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 general data protection principles relating to transparency, fairness and lawfulness; purpose limitation; having a legal basis for Processing; Processing of Special Categories of Personal Data, data minimization; limited storage periods; data quality, data protection by design and by default, measures to ensure data security;

and requirements in respect of onward transfers to bodies not bound by the BCRs ([Rule 6.1.1](#));

- ii. duty to ensure transparency and easy access to the BCRs by ensuring all Data Subjects are provided with the following information:
 - a. Identity and contact details of the Data Controller (and where applicable, the Data Controller's representative);
 - b. Contact details of the person with responsibility for data protection matters within the organisation;
 - c. Purpose(s) of the Processing and the lawful basis for the Processing;
 - d. Where Processing is based on the legitimate interests of the Data Controller or a third party, the legitimate interests of the Data Controller;
 - e. Any other recipient(s) of the Personal Data;
 - f. Where applicable, details of any intended transfers to a non-EEA country or international organisation and details of adequacy decisions and safeguards;
 - g. The retention period (how long an organisation holds onto Personal Data) or, if that is not possible, the criteria used to determine the retention period;
 - h. The existence of the following rights: Right of access, Right to rectification, Right to erasure, Right to restrict Processing, Right to data portability, Right to object, and to request these rights from the Data Controller;
 - i. Where Processing is based on consent, the right to withdraw consent at any time, without affecting the lawfulness of Processing based on consent before its withdrawal;
 - j. The right to lodge a complaint with a Supervisory Authority;
 - k. Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failing to provide the Personal Data;
 - l. The existence of any automated decision making Processes that will be applied to the Personal Data, including profiling, and meaningful information about how decisions are made, the significance and the consequences of Processing;
 - m. Information on the types of Personal Data held about the Data Subject;
 - n. Information on how the Personal Data was obtained and whether it came from publicly accessible sources,
 - o. information on the Data Subject's third party beneficiary rights and on the means to exercise those rights, information on how they can hold Group Members liable and information relating to the data protection principles described in (i) above ([Rule 1.7](#) and [Rule 6.1.1](#) and Annex 7 (Data Subject Rights));

where such information shall be provided: (a) at the time where the Personal Data are obtained where the data are obtained directly from the Data Subject; or (b) where the Personal Data are obtained from a source other than the Data Subject: (i) within a reasonable period, but not later than one month, after obtaining the data; or (ii) at the latest at the time of the first communication to the Data Subject, if the Personal Data are being used to communicate with the Data Subject; or (iii) at the latest when the Personal Data are first disclosed if the disclosure of the Personal Data is made to another recipient.

- iii. duty to respect rights of access, rectification, erasure, restriction, objection to Processing, right not to be subject to decisions based solely on automated Processing (including profiling) ([Rule 6.1.1](#) and [Annex 7](#) (Data Subject Rights));
- iv. duty to assess on an ongoing basis as whether national legislation prevents the Group Member from fulfilling its obligations under the BCRs ([Rule 2.5](#) and [Rule 6.4](#));
- v. duty to be transparent if national legislation prevents the Group Member from fulfilling its obligations under the BCRs including by: (i) notifying the DPO (who will notify the 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 has substantial effect on the guarantees provided by the BCRs ([Rule 6.4](#)); and (ii) notifying the competent Supervisory Authority of any legal requirement that the Group Member

is subject to in a non-EEA country that 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 law enforcement authority or state security body ([Rule 2.5](#) and [Rule 6.3](#));

- vi. duty to respect the right to complain through the internal complaint mechanism of the Group Members ([Rule 2.2](#));
- vii. duty to cooperate with Supervisory Authorities to ensure compliance by Group Members with the BCRs ([Rule 3.1](#)); and
- viii. with respect to the liability and jurisdiction provisions under which Data Subjects may enforce the BCRs against a Group Member and Ellucian Ireland Limited accepts responsibility for actions of Group Members outside of the EEA and agrees to pay compensation for material and non-material damage resulting from the violation of the BCRs by a Group Member outside of the EEA ([Rules 1.3](#) and [1.4](#)).

Without prejudice to any other administrative or judicial remedy, every Data Subject shall have the right to: (a) lodge a complaint with a Supervisory Authority, in particular, Data Subjects shall be entitled to 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 Group Member is established; or (ii) 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. However, a Group Member shall not be liable where it proves that it is not in any way responsible for the event giving rise to the damage.

Where an infringement of these BCRs is caused by a Group Member outside of the EEA [Rule 1.4](#) below applies.

1.4 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 outside of the EEA that are bound by these BCRs and to pay compensation for material and non-material damage resulting from the violation of these BCRs by a Group Member.

If a Group Member 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 outside the EEA is based.

1.5 [Not Used]

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

Ellucian Ireland Limited recognizes it has the burden of proof to demonstrate that a Group Member outside the EEA is not liable for any violation of the BCRs which has resulted in the Data Subject claiming damages.

If Ellucian Ireland Limited can demonstrate that the Group Member outside the EEA is not responsible for the event giving rise to the damage, it may discharge itself from any responsibility and liabilities.

1.7 Transparency and easy access to BCRs

All Data Subjects whose Personal Data are Processed pursuant to these BCRs shall be provided with m: the definitions set out in [Definitions](#) section, the material scope of the BCRs as set out in [Rule 4.1](#), [Rule 4.2](#), [Rule 6.2](#) and Annex 5 (Data Processing Particulars), the information set out in [Rule 1.3 ii.](#), information on their third-party beneficiary rights set out in [Rule 1.3](#), the means to exercise those rights also set out in [Rule 1.3](#), the data protection principles set out in [Rule 6.1.1](#), information on the complaint

handling process set out in [Rule 2.2](#) and information on how the Group accepts liability in [Rule 1.3](#) and [Rule 1.4](#). These parts of the BCRs (at least) will be made available on the Group's intranet for the Group's staff and will be published online.

Data subjects shall also be provided with at least the information set out in Annex 2 (Privacy Notice Information), except where the Data Subject already has such information.

Reference: Please see [Annex 2](#) for the Privacy Notice Information.

2 EFFECTIVENESS

2.1 The existence of a suitable training programme

Group Members provide data protection training, including appropriate training on these BCRs, to all employees 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. Ellucian'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 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 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.

Complaints will be dealt with without undue delay, and in any event within one month from receipt of the request, by the DPO and their team. Taking into account the complexity and number of requests, 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.

Reference: Please see attached [Annex 3](#) 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

The Group will have 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) on a yearly basis by either internal or external accredited auditors or on specific request to the DPO by the Executive Team or the Board of Directors. Supervisory Authorities can have access to the results of a data protection audit upon request and have the authority to carry out a data protection audit of any Group Member if required.

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 in the annual update.

Reference: Please see attached Annex 4 for additional details on the Group's audit programme.

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

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 sits in the Legal & Compliance organisation 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 handles Supervisory Authority investigations, monitors and annually reports on compliance at a global level, handles complaints from Data Subjects, 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 BCRs

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 authorizing 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 10](#) (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 Group Member exporting the data with relevant information and agrees that it will continue to cooperate with the Group Member exporting the data in ensuring compliance with these BCRs. The Group Members 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 notify the Group Member exporting the data promptly if, after having commenced transfers of data pursuant to these BCRs, it 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 of 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 Group Member exporting the data, or if the Group Member exporting data otherwise has reason to believe that the Group Member importing the data can no longer fulfil its obligations under these BCRs, the Group Member exporting the data shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the Group Members involved in the data transfer to address the situation.

The Group Member exporting the data shall suspend the transfer of Personal Data if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent Supervisory Authority to do so.

3 DUTIES OF COOPERATION

3.1 Duty to cooperate with Supervisory Authorities

Group Members shall cooperate with all Supervisory Authorities. Group Members will submit to be audited by the Supervisory Authorities regarding these BCRs and will comply with the advice and abide by the decisions of the Supervisory Authorities on any issue related to the BCRs.

4 DESCRIPTION OF PROCESSING AND DATA FLOWS

4.1 Material Scope of the BCRs

The Group Processes Personal Data from its job applicants, employees and their families, dependents or beneficiaries, personnel and staff of customers, prospective customers, partners, vendors, third-party suppliers and contractors, and website visitors. The Group collects, uses and Processes Personal Data for the purposes of operating and improving its business. These purposes include recruitment, fulfilling the Group's obligations and interests as an employer, administrative activities such as information security, providing products, services and support to our customers, hosting and attending events to promote the Group's business, promotional and marketing purposes, and communications with partners, vendors, third-party suppliers and contractors in order to support the Group's business. The Data Subjects, categories of Personal Data and purposes of Processing are more fully described in [Annex 5](#) (Data Processing Particulars).

Reference: Please see [Annex 5](#) for a full description of the Data Subjects, categories of Personal Data and purposes of Processing.

All Group Members listed in [Rule 6.2](#) below are bound by these BCRs. These BCRs do not apply to a Group Member when it is acting as a Data Processor for a third party.

The Group maintains the same security standards for Personal Data for all Group Members globally.

4.2 Geographical Scope of the BCRs

All Group Members listed in [Rule 6.2](#) below are bound by these BCRs. The BCRs apply to all transfers of Personal Data within the Group.

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 set out in [Annex 6](#). The DPO or their delegate shall inform Group Members of any changes without undue delay. The DPO will inform all relevant Supervisory Authorities via the Lead Supervisory Authority of changes to the BCRs with a brief explanation of the reasons justifying the update. This notification will be made promptly upon any change that would possibly affect the level of protection offered by the BCRs (e.g., changes to the binding character), or will be made annually for other changes.

Reference: Please see attached [Annex 6](#) which contains the Process for Changing Binding Corporate Rules.

6 DATA PROTECTION SAFEGUARDS

6.1.1 Data protection principles

Group Members when acting as Data Controllers shall observe the following principles in the Processing of Personal Data:

- i. **Transparency, fairness and lawfulness:** Group Members will Process Personal Data lawfully, fairly and in a transparent manner. Group Members will provide for the rights set out in [Annex 7](#) (Data Subject Rights). Specifically, the Group Members shall commit to only Process and transfer information on criminal convictions of employees and customers' employees in accordance with requirements under applicable national law.
- ii. **Purpose limitation:** Group Members will Process Personal Data for specified, explicit and legitimate purposes for which the Group Member has a legal basis, and will not further Process such Personal Data in a manner that is incompatible with those purposes. These purposes shall be set out in the relevant staff privacy notices or the privacy notice available online to personnel and staff of customers, prospective customers, partners, vendors, third-party suppliers and contractors, and website visitors.
- iii. **Legal basis for Processing:** Group Members will only Process Personal Data if at least one of the following grounds is fulfilled: (a) the Data Subject has given consent to the Processing of Personal Data for one or more specific purposes after receiving, in clear and plain language all necessary information; (b) Processing is necessary for the performance of a contract to which the Data Subject is a party or to take steps at the request of the Data Subject prior to entering into a contract; (c) Processing is necessary for compliance with a legal obligation to which the Group Member is subject; (d) Processing is necessary to protect the vital interests of the Data Subjects or of another natural person; (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Group Member; or (f) Processing is necessary to pursue the legitimate interests of the Group Member or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.
- iv. **Data minimization and accuracy:** Group Members will ensure Personal Data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected, accurate and where necessary, kept up to date.
- v. **Storage limitation:** Group Members shall retain Personal Data in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are Processed or for which they are further Processed according to that Group Member's Records Management Policy.
- vi. **Processing of Special Categories of Personal Data:** Special Categories of Personal Data should be not Processed unless the Group Member has a lawful basis for Processing pursuant to [Rule 6.1.1\(iii\)](#) above and it either has explicit consent from the Data Subject or relies on another exemption which may include where the Processing: (a) is necessary for the purposes of carrying out rights and obligations under employment law; (b) is necessary to protect the vital interest of the Data Subject or of another person; (c) relates to Personal Data manifestly made public by the Data Subject; (d) is necessary for the establishment, exercise or defense of a legal claim; (e) is necessary for reasons of a substantial public interest on the basis of EU or EEA member state law; (f) is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems; (g) is necessary for reasons of public interest in the area of public health; or (h) is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.
- vii. **Security:** Group Members 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. These measures include an obligation to enter into contracts with all Group Data Processors and External Data Processors that comprise all requirements as set out in [Annex 8](#). After becoming aware of any Personal Data Breach

Group Members shall notify without undue delay: (i) the DPO, (ii) Ellucian Ireland Limited, (iii) the competent Supervisory Authority (where required), and (iv) the Data Subjects where the Personal Data Breach is likely to result in a high risk to their rights and freedoms. Any Personal Data Breach should be documented (comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken) and the documentation should be made available to a Supervisory Authority on request.

- viii. **Restrictions on transfers:** Group Members shall only transfer (including onward transfer) Personal Data to External Data Processors or external Data Controllers located outside of the EEA if: (a) the country in which the Data Processor or Data Controller is located has been deemed to offer an adequate level of protection by the European Commission; or (b) if appropriate safeguards are in place such as (i) a legally binding and enforceable instrument between public authorities or bodies; (ii) binding corporate rules; (iii) standard data protection clauses adopted by the European Commission; (iv) standard data protection clauses adopted by a Supervisory Authority and approved by the European Commission; (v) an approved code of conduct together with binding and enforceable commitments to apply appropriate safeguards including as regards Data Subjects' rights in the country to which the transfer is being made; or (vi) an approved certification mechanism together with binding and enforceable commitments to apply appropriate safeguards including as regards Data Subjects' rights in the country to which the transfer is being made; or (c) in the absence of appropriate safeguards subject to a derogation including where: (i) Data Subject has provided their explicit consent to the proposed transfer after being informed of the possible risks of such transfer for the Data Subject due to the absence of an adequacy decision and appropriate safeguards; (ii) the transfer is 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; (iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and another natural or legal person; (iv) the transfer is necessary for important reasons of public interest; (v) the transfer is necessary for the establishment, exercise of defense of legal claims; (vi) the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent; or (vii) the transfer is made from a register which according to EU or EEA member state law is intended to provide information to the public and which is open to consultation either by the public or in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in EU or EEA member state law for consultation are fulfilled in the particular case.

Group Members when acting as Data Processors on behalf of a Group Member that is a Data Controller shall observe the principles above relating to security ([Rule 6.1.1\(vii\)](#)) and restrictions on transfers ([Rule 6.1.1\(viii\)](#)) and shall not Process Personal Data except on the instructions from the Data Controller, 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.

Reference: Please see attached [Annex 7](#) which contains a description of Data Subject rights and [Annex 8](#) which contains data processing clauses.

6.1.2 Accountability and other tools

Each Group Member is responsible for and must be able to demonstrate compliance with these BCRs.

In order to demonstrate compliance, Group Members must maintain a record of all categories of Processing activities carried out in line with the requirements as set out in [Annex 9](#) (Record of Processing Activities). This record should be maintained in writing, including in electronic form, and should be made available to any Supervisory Authority on request.

Group Members must carry out a data protection impact assessment (“**DPIA**”) for Processing operations that are likely to result in a high risk to the rights and freedoms of Data Subjects. Where a DPIA indicates that the Processing would result in a high risk to Data Subjects, the Group Member must take measures to mitigate the risk. In the absence of measures taken by the Group Member to mitigate the risk, the competent Supervisory Authority should be consulted prior to Processing.

Each Group Member must both at the time of the determination of the means for Processing and at the time of the Processing itself, implement appropriate technical and organizational measures, which are designed to implement the data protection principles in an effective manner and to integrate the necessary safeguards in order to comply with these BCRs in practice known as “data protection by design and 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	7796864	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

Group Member	Registration Number	Country	Contact Details
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 +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 a public authority) 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 its obligations under, 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 Group Member exporting the data and the DPO and comply with the procedure in [Annex 11](#) (Government Access Requests). The DPO will inform Ellucian Ireland Limited and the 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 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 competent Supervisory Authority, the DPO on behalf of the Group Member shall annually provide general information on the requests it received to the 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 authorizing 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 10](#) (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 Group Member 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 by the Group Members to address the situation. The Group Member 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. The Group Member importing the data will promptly inform the DPO of the issue in accordance with [Rule 6.3](#). The DPO will inform Ellucian Ireland Limited and report the issue to the competent Supervisory Authority unless prohibited by law. In the event notification to the 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 11](#) (Government Access Requests).

Reference: Please see attached [Annex 10](#) which contains factors to consider in undertaking a transfer risk assessment and [Annex 11](#) which sets out a procedure for dealing with government access requests.

Annex 1

Adoption Agreement

Annex 2

Privacy Notice Information

Annex 3

BCR Complaint Process Steps

BCR Complaint Process Diagram

Annex 4

BCR Audit Programme

Annex 5

Data Processing Particulars

Annex 6

Process for Changing Binding Corporate Rules

Annex 7

Data Subject Rights

Annex 8

Data Processing Clauses

Annex 9

Record of Processing Activities

Annex 10

Transfer Risk Assessment

Annex 11

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

1.1 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.

1.2 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

1.3 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.

2. Group Member Commitments

2.1 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.

2.2 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.

3. **Third Party Beneficiary**

- 3.1 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.
- 3.2 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.

4. **Accession**

- 4.1 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.
- 4.2 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.

5. **Default**

- 5.1 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.
- 5.2 Ellucian Ireland may also deem a Group Member as withdrawn from the BCRs pursuant to Clause 8.3.

6. **Withdrawal**

- 6.1 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**”).
- 6.2 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.

- 6.3 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.
- 6.4 Withdrawal is conducted without prejudice to all obligations and liabilities under the BCRs and especially Clause 10.
- 6.5 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.
- 6.6 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.

7. Confidentiality

- 7.1 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**".

7.2 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.

7.3 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.

8. Indemnity

8.1 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**”).

8.2 The Group Member shall forthwith notify Ellucian Ireland if a Claim is brought against the Group Member.

8.3 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.

8.4 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.

9. Notices

9.1 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.

9.2 Any notice for Ellucian Ireland should be sent to the DPO by email to privacy@ellucian.com.

10. Amendments

10.1 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.

- 10.2 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.

11. **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.

12. **Applicable Law and Competent Jurisdiction**

- 12.1 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.
- 12.2 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.
- 12.3 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

- a. 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.
- b. 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

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

Privacy Notice Information

Data subjects shall be provided with at least the following information at the time when their personal data are collected or, for information that is obtained otherwise than from the data subject, within a reasonable period after, except where the data subject already has such information:

1. the identity and contact details of the Controller and of its representative (where applicable);
2. the contact details of the relevant DPO;
3. the purposes of the processing for which the data are intended, and, when appropriate, the purpose(s) of the transfer(s) outside the EEA;
4. the legal basis for the processing;
5. the recipients or categories of recipients of the personal data;
6. the categories of personal data concerned, where personal data have not been obtained from the data subject;
7. where the processing is based on legitimate interests, the legitimate interests pursued by the Controller or by a third party;
8. where applicable, which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
9. where applicable, the fact that the Controller intends to transfer personal data to a third country or international organisation, the reference to the appropriate or suitable safeguards and the means by which to obtain a copy thereof or where they have been made available;
10. the period for which the personal data will be stored, or the criteria used to determine that period;
11. the existence of the right to request from the Controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
12. where the processing is based on the consent of the data subject, the existence of the right to withdraw consent at any time;
13. the right to lodge a complaint with a Supervisory Authority;
14. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is

obliged to provide the personal data and the possible consequences of failure to provide such personal data;

15. the existence of automated decision-making, including profiling, which produces legal effects concerning the data subject or similarly significantly affects them, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

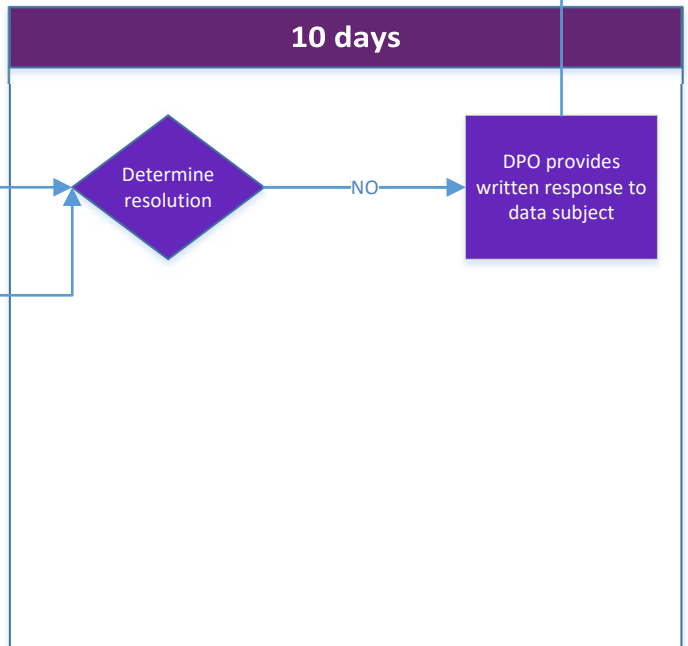
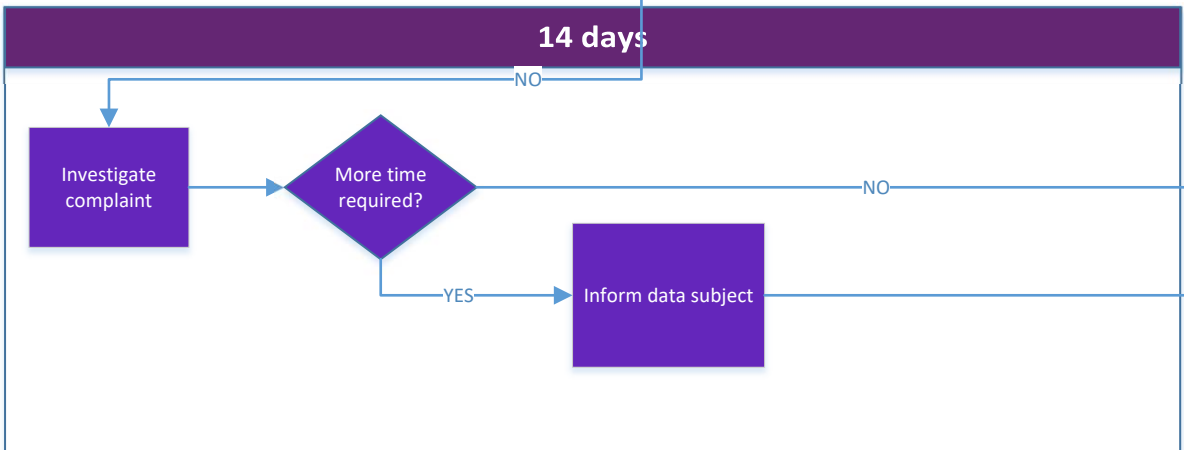
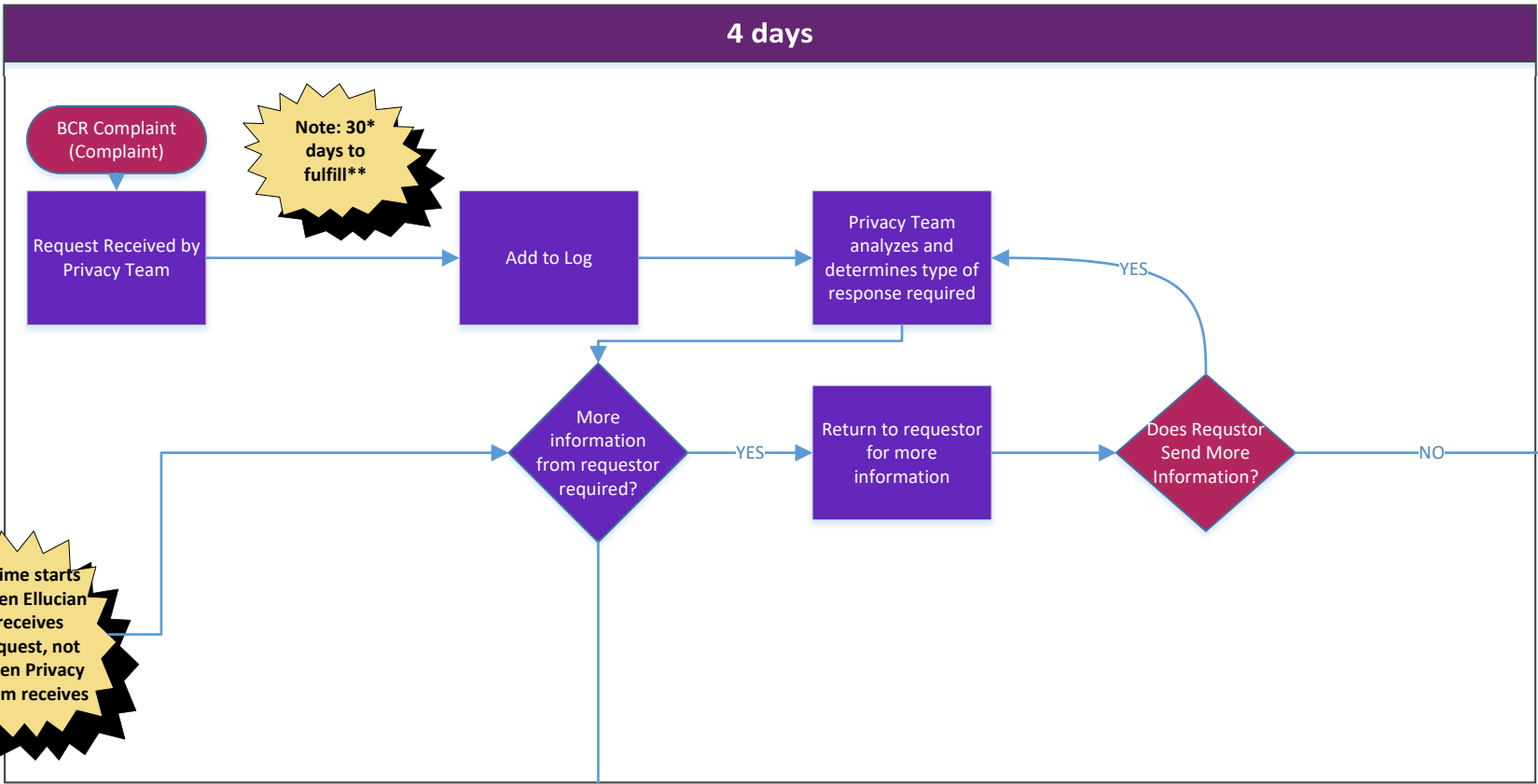
Annex 3

Binding Corporate Rules (“BCRs”) Complaint Resolution Process


This Annex relates to Rule 2.2 of the BCRs and sets out the process (also described in diagram form [here](#)) 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	Requests 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 request, that person should forward to privacy@ellucian.com
	Add to log	A member of Privacy team adds the request 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 request and determines next 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 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: <ul style="list-style-type: none"> - 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).




Color Key

- 

DPO/
Privacy
Team
- 

SME Group
- 

Data
Subject
- 

Alerts

Annex 4

Binding Corporate Rules (BCRs) Audit Programme

This Annex relates to Rule 2.3 of the BCRs.

The Group will have data protection audits to verify compliance with all aspects of these BCRs on a yearly basis (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 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.

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.

In relation to employee data, the Group requests SOC 2 Type II certification from its vendors prior to the time the vendor is selected.

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 in the annual update.

Supervisory Authorities may have access to the results of the audit upon request and 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 5

Data Processing Particulars

Employee, Vendor and Website Visitor Data

PART A: EMPLOYEE

Categories of data for:

- Current employees (whatever the type of employment contract, e.g. fixed term, permanent, internship);
- Former employees;
- Individuals applying for employment with the Group;
- Dependents, beneficiaries and family members of current and former employees;
- Emergency contact persons of current and former employees of the data exporter.

Category of Data	Type of Data	Purpose of Processing
Name and Initials	First name / initial	<ul style="list-style-type: none"> - Recruitment and job application management; - To comply with specific requests made by prospective employees prior to entering into an employment agreement; - Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.
	Middle name / initial	
	Last name	
	Initials	
Student Records, Education, and Professional Qualifications	Enrolment Information	<ul style="list-style-type: none"> - Recruitment and job application management; - To comply with specific requests made by prospective employees prior to entering into an employment agreement; - Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training,
	Degrees and schooling Information	
	Licenses and professional memberships	
	Professional certification	

		<p>succession planning, career development and compliance with respect to company policies and procedures.</p>
Personal characteristics	Age	<ul style="list-style-type: none"> - Recruitment and job application management; - To comply with specific requests made by prospective employees prior to entering into an employment agreement; - Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.
	Date of birth	
	Gender	
	Birth certificate number	
	Height	
	Weight	
	Marital status	
	Nationality	
	Leisure and interests	
	Photographs	
	Information about a person's children/family	
Personal White Page Information	Home postal address	<ul style="list-style-type: none"> - Recruitment and job application management; - To comply with specific requests made by prospective employees prior to entering into an employment agreement; - Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.
	Home telephone number	
	Home facsimile number	
	Personal electronic mail address	
	Personal cellular, mobile or wireless number	
Business White Page Information	Business postal address	<ul style="list-style-type: none"> - Recruitment and job application management; - To comply with specific requests made by prospective employees prior to entering into an employment agreement; - Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.
	Business telephone number	
	Business facsimile number	
	Business electronic mail address	
	Business cellular, mobile or wireless number	
	Personal assistant contact information	

		succession planning, career development and compliance with respect to company policies and procedures.
Health Related Information	Information about physical or psychological state of health, disease state, medical history, medical treatment, or diagnosis by a health care professional	<ul style="list-style-type: none"> - Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.
	Health insurance identification or account number	
Professional and Employment	Occupation / title	<ul style="list-style-type: none"> - Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.
	Income / salary / service fees / other compensation	
	User identification and / or employee number as assigned by an employer	
	User employee account or other password	
	Employment history, evaluations and disciplinary actions	
	Employer or taxpayer identification number	
	Digitized or other electronic signature	
	Date of hire	
	Information relating to employee job (such as job title, company, department number, supervisor, work phone and business email)	
	Standard hours	
	Performance ratings	
	Emergency contact details	
	Payroll information	
Absences and leaves		

	<p>Information relating to benefits</p> <p>Information relating to expenses</p> <p>Information relating to bonus</p> <p>Resume and summary of work experience and education</p> <p>Training courses completed</p> <p>Use of Company Group assets and facilities</p> <p>Job position being applied for</p>	
<p>Sensitive Personal Information</p>	<p>Sexual behavior or sexual preference</p> <p>Racial or ethnic origin</p> <p></p> <p>Medicare or Medicaid number</p> <p>Background checks</p> <p>Criminal convictions</p>	<ul style="list-style-type: none"> - Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures; - Information on sexual behaviour or sexual preference or racial or ethnic origin is not currently requested by the Group, however this information may be provided by an employee on a voluntary basis in relation to a HR grievance or investigation.
<p>Other Confidential Information</p>	<p>National identification number</p> <p>State/province-issued identification number</p> <p>Driver's or operator's license number</p> <p>Passport number</p> <p>Alien registration number</p> <p>Other government-issued identification number (e.g. country-identification)</p> <p>Credit report information</p>	<ul style="list-style-type: none"> - Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.

	Insurance claim history	
	IP address	
	Data subject to litigation holds or e-discovery	
	Mother's maiden name	
Financial Information/Payment Card Industry Information	Financial institution account number	<ul style="list-style-type: none"> - Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.
	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	

PART B: VENDORS AND CUSTOMERS

Categories of data for:

- Vendor's current and former employees and vendors / contractors; and
- Customer's current and former employees and vendors / contractors.

Category of Data	Type of Data	Purpose of Processing
Name and Initials	First name / initial	<ul style="list-style-type: none"> - Management and development of Group business relations; - Decision-making with regards to the development and operation of Group business; - Providing goods and services to Group or Group's customers as described in contracts.
	Middle name / initial	
	Last name	
	Initials	
Student Records, Education, and Professional Qualifications	Enrolment Information	<ul style="list-style-type: none"> - Management and development of Group business relations; - Decision-making with regards to the development and operation of Group business; - Providing goods and services to Group or Group's customers as described in contracts.
	Degrees and schooling Information	
	Licenses and professional memberships	
	Professional certification	
Personal characteristics	Photographs	<ul style="list-style-type: none"> - Management and development of Group business relations; - Decision-making with regards to the development and operation of Group business; - Providing goods and services to Group or Group's customers as described in contracts.
Business White Page Information	Business postal address	<ul style="list-style-type: none"> - Management and development of Group business relations; - Decision-making with regards to the development and operation of Group business; - Providing goods and services to Group or Group's customers as described in contracts.
	Business telephone number	
	Business facsimile number	
	Business electronic mail address	
	Business cellular, mobile or wireless number	
	Personal assistant contact information	
Professional and Employment	Occupation / title	<ul style="list-style-type: none"> - Management and development of Group business relations; - Decision-making with regards to the development and operation of Group business; - Providing goods and services to Group or Group's customers as described in contracts.
	Compensation	
	User identification and / or employee number as assigned by an employer	
	User employee account or other password	
	Employment history, evaluations and disciplinary actions	

	Employer or taxpayer identification number	
	Digitized or other electronic signature	
	Date of hire	
	Information relating to employee job (such as job title, company, department number, supervisor, work phone and business email)	
	Standard hours	
	Performance ratings	
	Emergency contact details	
	Payroll information	
	Absences and leaves	
	Information relating to expenses	
	Resume and summary of work experience and education	
	Training courses completed	
	Use of Company Group assets and facilities	
Sensitive Personal Information	Background checks	<ul style="list-style-type: none"> - Management and development of Group business relations; - Decision-making with regards to the development and operation of Group business; - Providing goods and services to Group or Group’s customers as described in contracts.
	Criminal convictions	
Other Confidential Information	National identification number	<ul style="list-style-type: none"> - Management and development of Group business relations; - Decision-making with regards to the development and operation of Group business; - Providing goods and services to Group or Group’s customers as described in contracts.
	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)	
	Credit report information	

	IP address	
	Data subject to litigation holds or e-discovery	
Financial Information/Payment Card Industry Information	Details of financial transactions or account information	<ul style="list-style-type: none"> - Management and development of Group business relations; - Decision-making with regards to the development and operation of Group business; - Providing goods and services to Group or Group's customers as described in contracts.

PART C: WEBSITE VISITORS

Categories of data for:

- Visitors to the Ellucian website (<https://www.ellucian.com/>).

Category of Data	Type of Data	Purpose of Processing
Online identifiers	IP address, other persistent identifier, device information,	<ul style="list-style-type: none"> - Management and development of the website
Location	Location information	<ul style="list-style-type: none"> - Management and development of the website
Usage information	Pages accessed, how long spent on pages	<ul style="list-style-type: none"> - Management and development of the website

Annex 6

Process for Changing Binding Corporate Rules (BCRs)

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

Step	Process Flow
Monitor obligations and list of BCR Group Members	The data protection officer (DPO) or his/her delegate shall keep a fully updated list of the BCR Group Members and keep track of and monitors regulatory changes that may impact the BCRs and provide necessary information to Data Subjects or Supervisory Authorities upon 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	<p>Compliance team consults with impacted business units regarding the changes</p> <p>Compliance team drafts changes to the BCRs based on input from the business</p> <p>Compliance team sends draft updates to impacted business team(s) for review and comment</p> <p>Repeat this step until the proposed updates are accurate and contain the information legally required.</p>
Compliance approval	<p>VP of Compliance to review and approve. If changes are needed, repeat the steps listed above until the updates are approved.</p> <p>If applicable (check with VP of Compliance if unsure), discuss with the Compliance Committee before posting.</p>
Post	<p>The updated BCRs will be posted to any internal and external website where the prior version of the BCRs had been posted.</p> <p>The DPO will keep a record of all BCR changes made.</p>
Inform Group Members	The DPO will inform Group management of the changes with 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 Member is effectively bound by the BCRs and can deliver compliance with the BCRs.
Inform Supervisory Authority of updates	<p>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, together with a brief explanation of the reasons justifying the update.</p> <p>However, notification will be made promptly to the relevant Supervisory Authorities via the competent Supervisory Authority for</p>

Step	Process Flow
	any change that would possibly affect the level of protection offered by the BCRs (<i>i.e.</i> , changes to the binding character).

Annex 7

Data Subject Rights

This Annex relates to Rule 6.1.1(i) of the BCRs.

1.1 Transparency and information right

All Group Members will process personal data in a transparent manner. Group Members will ensure that data subjects are adequately informed about the purposes for which their personal data are processed and provide any other information to the data subjects which may be required.

The BCRs will be made available to data subjects via the Ellucian intranet and Ellucian website. Furthermore, a data subject will always be able to obtain, upon request, a copy of the BCRs from the DPO using privacy@ellucian.com.

The Group Member will provide or make available to the data subject at least the following information, except where the data subject already has such information:

- (a) the identity and contact details of the Data Controller and of its representative;
- (b) the contact details of the DPO;
- (c) the purposes of the processing for which the personal data are intended;
- (d) the legal basis for the processing;
- (e) the recipients or categories of recipients of the personal data;
- (f) the categories of personal data concerned, where personal data have not been obtained from the data subject;
- (g) where the processing is based on legitimate interests, the legitimate interests pursued by the Data Controller or by a third party;
- (h) where applicable, the fact that the Data Controller intends to transfer personal data to a third country or international organization, the reference to the appropriate or suitable safeguards and the means by which to obtain a copy or a link to where they have been made available;
- (i) the period for which the personal data will be stored, or the criteria used to determine that period;
- (j) the existence of the right to request from the Data Controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- (k) where the processing is based on the consent of the data subject, the existence of the right to withdraw consent at any time;
- (l) the right to lodge a complaint with a Supervisory Authority;
- (m) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged

to provide the personal data and the possible consequences of failure to provide such personal data; and

(n) the existence of automated decision-making, including profiling, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The Group Member will also notify data subjects if their personal data are to be used for a different or new purpose unless such a change is within their expectations and they can express their concerns or there is a legitimate basis for not doing so consistent with the applicable law of the EU country in which the personal data was collected.

This right to information does not apply in exceptional cases where the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the safeguards in Article 89(1) of the GDPR or where this obligation is likely to render impossible or seriously impair the achievement of the objectives of that processing. Information may also not be provided if recording or disclosure is expressly laid down by law, which law provides appropriate measures to protect the data subject's legitimate interests.

Timing: Where personal data relating to a data subject are collected from the data subject, the Group Member will provide the information above at the time when the personal data are obtained. Where the personal data has not been directly obtained from the data subjects, the Group Member will provide the information above: (i) within a reasonable period, but not later than one month, after obtaining the data; or (ii) at the latest at the time of the first communication to the data subject if the personal data are being used to communicate with the data subject; or (iii) at the latest when the personal are first disclosed if the disclosure of the personal data is made to another recipient.

1.2 Rights of data subjects

Data subject will be clearly informed as to how they can exercise their rights through the relevant employee privacy notice or the privacy notice available to customers, prospective customers, partners, vendors, third-party suppliers and contractors, and website visitors available online.

All requests from data subjects should be acknowledged promptly. Where the Group Member has reasonable doubts concerning the identity of the data subject making the request, the data subject may be asked to provide additional information to verify their identity.

Timing: In general, all requests should be responded to within one month of receipt of the request. In exceptional circumstances, this period may be extended by two further months where necessary, taking into account the complexity and number of the requests in which case the data subject will be notified of the need to rely on an extension within one month of receipt of the request together with the reasons for the delay.

1.3 Right of access

Data subjects have the right to obtain from the Group Member within the timeline set out in section [1.2](#) above, confirmation as to whether or not personal data relating to them are being processed, and where this is the case, access to at least the following information:

1.3.1 the purposes of the processing;

1.3.2 the categories of personal data concerned;

- 1.3.3 the recipients or categories of recipients to whom the personal data are disclosed in particular recipients in third countries or international organisations and the right to be informed of the appropriate safeguards in place;
- 1.3.4 the period for which the personal data will be stored or the criteria used to determine that period;
- 1.3.5 the rights granted to the data subject, including the right to request rectification, restriction and erasure of incorrect data and to object to processing of personal data;
- 1.3.6 the right to lodge a complaint with a Supervisory Authority;
- 1.3.7 where the personal data are not collected from the data subject, any available information as to their source;
- 1.3.8 as the case may be, the existence of automated decision-making, including profiling, and in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The Group Member will provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Group Member may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information will be provided in a commonly used electronic form. The right to obtain a copy of personal data will not adversely affect the rights and freedoms of others.

1.4 Right to rectification

Data subjects have a right to obtain from the Group Member, without undue delay, the rectification of inaccurate personal data concerning them. Taking into account the purposes of the processing, data subjects have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

The Group Member will communicate any rectification of personal data request to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Group Member will inform the data subject about those recipients if the data subject requests.

1.5 Right to erasure (“right to be forgotten”)

Data subjects have the right to obtain from the Group Member, without undue delay, the erasure of personal data concerning them. The Group Member will proceed to such erasure in the following cases:

- 1.5.1 the personal data are no longer necessary in relation to the purposes for which they were collected or processed;
- 1.5.2 the data subject has withdrawn their consent to the processing and there is no other legal ground for processing;
- 1.5.3 the data subject objects to the processing and there are no overriding legitimate grounds for processing;
- 1.5.4 the personal data have been unlawfully processed;

- 1.5.5** the personal data have to be erased for compliance with a legal obligation to which the Group Member is subject;
- 1.5.6** the personal data have been collected in relation to the offer of information society services to children.

Where the Group Member has made the personal data public and is obliged on request to erase the personal data, the Group Member, taking account of available technology and the cost of implementation, will take reasonable steps, including technical measures, unless this proves impossible or involves disproportionate effort, to inform recipients processing the personal data that the data subject has requested the erasure of any links to, or copy or replication of, those personal data. The Group Member will inform the data subject about those recipients if the data subject requests.

1.6 Right to restriction

Data subjects have the right to request restriction of processing of their personal data where:

- 1.6.1** the accuracy of the personal data is contested by the data subject in which case processing will be restricted for a period enabling the Group Member to verify the accuracy of the personal data;
- 1.6.2** the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of its use instead;
- 1.6.3** the Group Member no longer needs the personal data for the purposes of the processing for which it was kept, but it is required to be kept by request of the data subject for the establishment, exercise or defence of legal claims; and
- 1.6.4** the data subject has objected to processing pursuant to Article 21(1) of the GDPR pending verification of whether the legitimate grounds of the Group Member override those of the data subject.

Where processing has been restricted, the personal data will, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest set out in the law of origin of the personal data.

A data subject will be informed by the Group Member before the restriction of processing is lifted.

The Group Member will communicate any restriction of processing request to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Group Member will inform the data subject about those recipients if the data subject requests.

1.7 Right to data portability

Data subjects have the right to receive personal data concerning them, which they have provided to the Group Member, in a structured, commonly used and machine-readable format and request this personal data is sent to another entity, where:

- 1.7.1** the processing is based on consent or necessity for the performance of a contract; and
- 1.7.2** the processing is carried out by automated means.

1.8 Right to object

Data subjects have the right to object at any time to the processing of personal data relating to them on grounds relating to their particular situation where processing is based on the performance of a task carried out in the public interest or the Group Member's or another entity's legitimate interest. The Group Member will no longer process the personal data unless the Group Member demonstrates that the Group Member or another entity have compelling legitimate grounds for the processing which override the interests of the data subject, or for the establishment exercise or defence of legal claims.

At any time, a data subject may object to the processing of personal data for direct marketing purposes, which includes profiling to the extent that it is related to the direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data will no longer be processed for such purposes.

Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1) of the GDPR, the data subject, on grounds relating to their particular situation, will have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

1.9 Automated individual decisions including profiling

Data subjects have a right not to be subjected to a decision which has legal consequences for them, or which similarly significantly affects them, if this decision has been taken solely on the basis of automated processing of personal data including profiling, e.g. with regard to their creditworthiness, reliability or conduct.

Automated individual decision-making may take place only if: (1) the decision is necessary for the entering into, or performance of, a contract between the Group Member and the data subject; (2) it is authorized by law to which the Group Member is subject and which sets forth suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; (3) it is based on the data subject's explicit consent. Automated decision-making will not be based on special categories of personal data.

In order to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, the Group Member will at least provide the right to obtain human intervention on the part of the Data Controller, so that the data subject may express their point of view and to contest the decision.

Annex 8

Data Processing Clauses

This Annex relates to Rule 6.1.1(vii) of the BCRs.

A Data Controller which discloses or provides access to personal data by a Data Processor wherever located is obliged to enter into a written contract with the 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 Data Processor shall process personal data only in accordance with the Controller's documented instructions, including with regard to transfers, and inform the Controller if an instruction infringes the BCRs;
3. the Data Processor shall ensure that all persons authorised 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 Data Processor shall take appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, including as appropriate: (a) the pseudonymisation 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 Data Processor shall only enlist a sub-Data Processor with the prior specific or general written authorisation of the Data Controller and if general authorisation is provided the Data Processor shall inform the Data Controller of any intended changes, additions or replacements to sub-Data Processors and give the Data Controller an opportunity to object to such changes;
6. the Data Processor shall impose on the sub-Data Processor the same obligations as imposed on the Data Processor under the data processing clauses and remain fully liable to the Data Controller for the performance of the sub-Data Processor's obligations;
7. the Data Processor shall assist the Data Controller in complying with its obligations under the BCRs, 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 Data Processor shall assist the Data Controller in complying with its obligations and in respect of data security, data breach notifications to Supervisory Authorities and data subjects (where relevant) and data protection impact assessments;
9. the Data Processor shall, upon the Data Controller'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 Data Processor shall make available to 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 Controller, an external auditor appointed by the Data Controller or any Supervisory Authority.

Annex 9

Record of Processing Activities

1. Each Data Controller shall maintain a record of processing activities containing:
 - 1.1 the name and contact details of the Data Controller and, where applicable, the joint Data Controller, the Data Controller's representative and the DPO;
 - 1.2 the purposes of the processing;
 - 1.3 a description of the categories of data subjects and of the categories of personal data;
 - 1.4 the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
 - 1.5 where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1) GDPR, the documentation of suitable safeguards;
 - 1.6 where possible, the envisaged time limits for erasure of the different categories of data; and
 - 1.7 where possible, a general description of the technical and organisational security measures referred to in Article 32(1) GDPR.
2. Each Data Processor shall maintain a record of all categories of processing activities carried out on behalf of a Data Controller, containing:
 - 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 third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; and
 - d. where possible, a general description of the technical and organisational security measures referred to in Article 32(1) GDPR.

Annex 10

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:
 - a. the content and duration of the processing;
 - b. the scale and regularity of transfers;
 - c. the length of the processing chain;
 - d. the number of actors involved and the transmission channels used;
 - e. the type of recipients;
 - f. the purpose of processing;
 - g. the nature of the personal data transferred; and
 - h. 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 11

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 Group Member exporting the data from the EEA;
 - 1.2 the DPO (and the DPO shall inform Ellucian Ireland Limited and the 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 body, 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 DPO, the Data Subjects and/or the 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.

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.