EXODUS

BCR

BCR V1.0
1/24/26

EU Processor
Binding Corporate Rules - January 2026

Contents

Overview

1. Introduction

At Exodus, trust is foundational to everything we do. Exodus and its subsidiaries provide a social media, entertainment, publishing platform. Exodus acts as Controllers and Processors for the Personal Data Users' submit into our applications. Exodus does select or control the Users' data or Processing. Exodus provides technology for their platform on which Users' Process data and provides ancillary support for the application on the Users' behalf and for the Users' benefit. Exodus is committed to offering its Users state of the art enterprise cloud infrastructure for data security standards and support with respect to the Customer's data privacy compliance needs. Exodus has a number of employees in countries which the European Commission has deemed to provide an adequate level of protection for Personal Data under the General Data Protection Regulation (EU) 2016/679 ("GDPR"). In addition, Exodus does and will continue to offer its Users adequate data processing agreements and data transfer mechanisms based on the European Commission's Standard Contractual Clauses (Commission Implementing Decision 2021/914 of 4 June 2021), or any other successor clauses that may be approved by the European Commission ("SCCs"). The SCCs are also recognized by data protection supervisory authorities outside the EEA, including in the United Kingdom and Switzerland, subject to local addenda and modifying terms. However, to provide an alternative route to achieve compliance with data protection laws, the Exodus has implemented these Processor Binding Corporate Rules ("BCRs"). These BCRs achieve an adequate level of protection for Personal Data, as required by the GDPR and also satisfy requirements under other jurisdictions' laws. These BCRs are distinct from any other data transfer mechanism Exodus may provide at any time.

2. Scope and Application

These BCRs govern international transfers of Personal Data to and between employees of the Exodus when acting as Processors on behalf of a User and data is transferred out of the EEA. The Processing activities involve the storing of the Personal Data and the Processing necessary to operate and maintain the Service and implement the individual Users' instructions when using the Service. As required to provide its Services to its Users, Exodus may transfer the Personal Data to the countries in which the different employees of Exodus have their place of business (see Schedule 1 to the BCRs). Exodus will agree with each User in a Service Agreement which categories of the Users' data shall be covered by these BCRs, for example, only Personal Data of Data Subjects in the EEA or also Personal Data of Data Subjects in other jurisdictions. Exodus and its Personnel will comply with these BCRs with respect to the data identified in the Service Agreement. Additional privacy compliance laws and requirements may apply to specific data, locations or functions.

3. Definitions

Notwithstanding the potentially broader scope of these BCRs, as specified in a Service Agreement with a particular Customer, certain terms shall bear the following meanings in these BCRs:

Controller	means the natural or legal person which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Customer	means the legal entity with whom a employee of Exodus has entered into a Service Agreement which incorporates by reference these BCRs.
Data Subject	means an identified or identifiable natural person.
Personnel	means individual personnel whether engaged on a permanent or non-permanent basis, including contingent workers, interns and trainees.

European Economic Area or EEA	means the member states of the European Union plus Iceland, Liechtenstein and Norway.
EU	means the member states of the European Union.
Personal Data	means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. In these BCRs, the term "Personal Data" refers to any Personal Data submitted electronically into a Service.
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.
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. References to "Process", "Processess" or "Processed" shall be construed accordingly.
Processor	means a natural or legal person which Processes Personal Data on behalf of a Controller.
Service	means Exodus enterprise cloud applications listed in Schedule 3, including any consequent Processing of Personal Data (such as storage and customer support).
Service Agreement	means the service agreement between User and an employee of Exodus.
Special Category Data	means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical 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.
Subprocessor	means a natural or legal person engaged by a Processor to Process Personal Data on behalf of itself and a User.
Supervisory Authority	means an independent public authority, which is established by a member state pursuant to Article 51 GDPR.
Exodus Gaming	Exodus and its subsidiaries listed in Schedule 1.

Binding Corporate Rules

1. Binding Nature

1.1 General Obligation

All employees of Exodus and its Personnel have the duty to respect the BCRs and the instructions regarding the Personal Data Processing and the security and confidentiality measures as provided in the Service Agreement.

1.2 Means by which the BCRs are made Binding

All employees of Exodus have signed an intra-group agreement that obligates each employee to comply with the BCRs. Each Personnel of an employee of Exodus is subject to an individual and separate agreement, a clause in an employment contract, and/or internal policies, in each case providing for sanctions in case of non-compliance.

1.3 Third-Party Beneficiary Rights for Data Subjects

1.3.1 Rights directly enforceable against Exodus

Each Data Subject whose Personal Data is covered by the BCRs shall have the right to enforce the following elements of the BCRs as a third-party beneficiary directly against each employee of Exodus involved in the Processing of the Data Subject's Personal Data:

- Duty to respect the instructions from the User acting as Controller regarding the Personal Data Processing including for transfers to third countries (Articles 28 (3) (a), 28 (3) (g), 29 GDPR and Sections 1.1, 6.1.2 and 6.1.4 of these BCRs),
- Duty to implement appropriate technical and organizational security measures (Articles 28 (3) (c) and 32 GDPR and Section 6.1.4 of these BCRs) and duty to notify any Personal Data Breach to the User acting as Controller (Article 33(2) GDPR and Section 6.1.4 of these BCRs),
- Duty to respect the conditions when engaging a Subprocessor either within or outside Exodus (Article 28 (2), 28(3) (d), 28 (4), 45, 46, 47 GDPR and Sections 6.1.6 and 6.1.7 of these BCRs),
- Duty to cooperate with and assist the Customer acting as Controller in complying and demonstrating compliance with the law such as for answering requests from Data Subjects in relation to their rights (Articles 28 (3) (e), 28 (3) (f), 28 (3) (h) GDPR and Sections 3.2, 6.1.1, 6.1.2, 6.1.3, 6.1.4, and 6.1.5 of these BCRs),
- Provide easy access to the BCRs (Article 47 (2) (g) GDPR and Section 1.6 of these BCRs),
- Right to complain through internal complaint mechanisms (Article 47 (2) (i) GDPR and Section 2.2 of these BCRs),
- Duty to cooperate with the Supervisory Authority (Articles 31, 47 (2) (l) GDPR and Section 3.1 of these BCRs),
- Liability, compensation and jurisdiction provisions (Articles 47 (2) (e), 79, 82 GDPR and Sections 1.3, 1.4 and 1.5 of these BCRs),
- National legislation preventing respect of the BCRs (Article 47(2)(m) GDPR and Section 6.4 of these BCRs).

1.3.2 Rights enforceable against Exodus where the Data Subject is not able to bring a claim against the User acting as Controller

Each Data Subject whose Personal Data is covered by the BCRs shall have the right to enforce the BCRs as a third-party beneficiary against each employee of Exodus involved in the Processing of the Data Subject's Personal Data in case the Data Subject is not able to bring a claim against the User because the User has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the User by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. In such a case, the Data Subject shall be able to enforce against the respective employee

of Exodus under the following sections within these BCRs: Sections 1.1, 1.3, 1.4, 1.5, 1.6, 2.2, 3.1, 3.2, 6.1, 6.2 and 6.3.

1.3.3 Modalities
The Data Subjects' rights as mentioned in the preceding Sections 1.3.1 and 1.3.2 shall cover the judicial remedies for any breach of the third-party beneficiary rights guaranteed and the right to obtain redress and where appropriate receive compensation for any damage (material harm but also any distress). In particular, Data Subjects in the EU shall be entitled to lodge a complaint before the competent Supervisory Authority; the Data Subject shall have a choice between the Supervisory Authority of the EU Member State of his/her habitual residence, place of work or place of alleged infringement. Data Subjects in the EU shall be entitled also to lodge a complaint before the competent court, with a choice for the Data Subject to act before the courts where the User or Exodus has an establishment or where the Data Subject has his or her habitual residence pursuant to Article 79 of the GDPR. Where an employee of Exodus and the User involved in the same Processing are found responsible for any damage caused by such Processing, the Data Subject shall be entitled to receive compensation for the entire damage directly from the respective employee of Exodus (Article 82 (4) GDPR).

1.4 Liability and Enforcement
The BCRs will be made binding between the User and the employee of Exodus through a specific reference in the Service Agreement which shall comply with Article 28 GDPR. In this case, the BCRs shall be incorporated into the Service Agreement as though they were set forth in the Service Agreement in their entirety. The Customer shall have the right to enforce the BCRs against (a) any employee of Exodus for breaches such member caused, (b) Exodus in case of a breach of the BCRs or of the Service Agreement by employees of Exodus established outside of the EEA or a breach of the written agreement referred under Section 6.1.7 of these BCR by any external Subprocessor established outside of the EEA. The Users' rights shall cover the judicial remedies and the right to receive compensation, as further specified in the applicable Service Agreement. Exodus has appointed Carmpolcaypse, Atlanta, Georgia, United States to accept responsibility for and agrees to take the necessary action to remedy the acts of other employees of Exodus established outside of the EEA for breaches caused by any external Subprocessor established outside of the EEA and to pay compensation for any material or non-material damages resulting from the violation of the BCRs to Data Subjects and/or the Customer pursuant to the Service Agreement. Exodus will ensure that Exodus has sufficient assets to pay compensation for damages resulting from the breach of the BCRs. Exodus will accept liability as if the violation had taken place by itself in the EEA member state in which it is based instead of the employee of Exodus outside the EEA or the external Subprocessor established outside of the EEA. Exodus may not rely on a breach by a Subprocessor (internal or external of Exodus) of its obligations in order to avoid its own liabilities.

1.5 The Burden of Proof
Exodus will have the burden of proof that the employee of Exodus outside of the EEA and/or the external Subprocessor is not liable for any violation of the BCRs which has resulted in the Data Subject claiming damages or remedy. Where the User can demonstrate that it suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of the BCRs, it will be for Exodus to prove that the employee of Exodus outside of the EEA and/or the external Subprocessor was not responsible for the breach of the BCRs giving rise to those damages or that no such breach took place. If Exodus can prove that the employee of Exodus outside the EEA and/or the external Subprocessor is not responsible for the act, it may discharge itself from any responsibility/liability.

1.6 Access to the BCRs
The BCRs are published on the Exodus website (currently located at http://help.exodus-gaming.com/binding-corporate-rules/) and a reference shall be provided in the Service Agreement. The User shall, in particular, provide all Data Subjects benefiting from the third-party beneficiary rights with the information on their

third-party beneficiary rights with regard to the Processing of their Personal Data and on the means to exercise those rights. Exodus will publish the BCRs on a website *.exodus-gaming.com in a way easily accessible to Data Subjects.

2. Effectiveness

2.1 Confidentiality and Training
Exodus will ensure that its Personnel who are regularly engaged in the Processing of Personal Data or in the development of tools used to Process Personal Data are informed of the confidential nature of Personal Data and have received appropriate training on their responsibilities under the BCRs. Specifically, Exodus provides privacy and security training to all Personnel during their onboarding process and also provides annual privacy and security training to personnel of the Exodus with access to unencrypted Personal Data.

2.2 Handling of Complaints
This complaint handling process describes how complaints brought by a Data Subject whose Personal Data is Processed by Exodus must be addressed and resolved. This process will be made available to Users on whose behalf Exodus Processes Personal Data under the BCRs. Exodus' Privacy and Data Protection Team is responsible for handling complaints related to compliance with the BCRs. Data Subjects can lodge a complaint by contacting the Privacy and Data Protection Team at help.exodus-gaming.com/contact-us/. In accordance with the Service Agreement, Exodus will, without undue delay, forward claims, requests or complaints related to the Processing of or access to Personal Data from Data Subjects to the respective User, provided that the Data Subject has given sufficient information for Exodus to identify the User, and handle such claims, requests or complaints in accordance with the Service Agreement. The User is responsible for handling such complaints, except in cases where the responsible User has disappeared factually or has ceased to exist in law or become insolvent. In such cases, and provided that Exodus still maintains the Data Subjects' Personal Data (i.e., it has not been deleted following termination of the Service Agreement), these complaints shall be dealt with without undue delay and in any event within one month by Exodus' Privacy and Data Protection Team. This Team has legal and operational specialists based in the European Union, United Kingdom and United States that will effectively handle complaints in accordance with the BCRs and applicable laws. Taking into account the complexity and number of the requests, that period may be extended by a maximum of two further months, in which case the Data Subject will be informed accordingly. If and when the conditions in this section are met, Data Subjects who contact Exodus will be informed where to complain, in which form, the timescale for the reply on the complaint, consequences in case of rejection of the complaint, consequences in case the complaint is considered as justified, and consequences if the Data Subject is not satisfied by the replies. In the event that Exodus no longer maintains the Data Subject's Personal Data, the Data Subject will be informed accordingly. Data Subjects also have the right to lodge a claim before the competent courts and/or the Supervisory Authority (whether or not they have first complained directly to Exodus as described in Section 1.3 above).

2.3 Audit Program
Exodus conducts data protection audits on a regular basis by internal and external accredited auditors as well as on specific requests from Exodus' Global Head of Privacy or Exodus' internal audit department. The audit program covers all aspects of the BCRs, including methods of ensuring that corrective actions will take place. The audit reports are submitted to Exodus' Global Head of Privacy and Data Protection Officer ("DPO"), and if the reports reveal breaches or the potential for breaches of a serious nature (for example, presenting a risk of potential harm to individuals or to the business) to Carmpoclaypse and Exodus' board of directors. Exodus will, at Users' request and subject to the confidentiality terms set forth in the Service Agreement, make its most recent Service-specific third-party audit reports available to the User. Users or independent auditors appointed by Users may also conduct their own audit in accordance with the audit provisions of the Service Agreement. Supervisory Authorities have the power to audit employees of Exodus under applicable law. Upon

request, Exodus will make available to the competent Supervisory Authority any audit reports that Exodus conducts of the BCRs. With respect to User-specific audit reports, Supervisory Authorities with jurisdiction over the User can request access to the results of Exodus audit reports from the User and carry out data protection audits themselves if required and legally possible. Exodus will also comply with any court order or other formal order that compels Exodus to make User-specific audit reports available to the competent Supervisory Authority. Exodus will accept, at the request of a User and in accordance with the Service Agreement, to submit their data processing facilities for audit of the Processing activities relating to that User. Any audits of Subprocessors with access to Personal Data will be coordinated through Exodus and in accordance with the Service Agreement.

2.4 Network of Privacy Personnel
Exodus' Privacy and Data Protection Team is responsible for overseeing and ensuring compliance with applicable data protection laws (including compliance with these BCRs), advising Exodus' management on data protection matters and handling data protection-related complaints. The Privacy and Data Protection Team is located across the European Union, United Kingdom and United States. The Privacy and Data Protection Team reports to Exodus' Global Head of Privacy. The members of the Privacy and Data Protection Team are ultimately responsible for all privacy-related matters and benefit from the support of the Exodus' highest management. Exodus has appointed a DPO (based in the European Union) in accordance with Article 37 of the GDPR. The Privacy and Data Protection Team is responsible for escalating complaints and compliance issues to the DPO where necessary and assisting the DPO with investigations, and implementation of and training on data privacy measures.

Exodus' DPO reports to the Chief Legal Officer. The DPO works with the Privacy and Data Protection Team to liaise with Supervisory Authorities, report annually to the Board of Directors of the Exodus as well as at other times as appropriate and provide oversight at a global level.

3. Cooperation Duty

3.1 Duty to Cooperate with Supervisory Authorities
All employees of Exodus shall cooperate with, and accept to be audited (without restriction) by, the Supervisory Authorities competent for the relevant User and comply with applicable law and the advice, formal decisions or notices of these Supervisory Authorities on any issue related to the BCRs.

3.2 Duty to Cooperate with Customers
Exodus and any Subprocessor shall cooperate and assist Users to comply with data protection law, such as the Users' duty to respect the Data Subject rights or to handle their complaints, or to be in a position to reply to an investigation or inquiry from Supervisory Authorities, subject to the applicable Service Agreement. This shall be done in a reasonable time and to the extent reasonably possible and as agreed upon in the applicable Service Agreement.

4. Description of Processing and Data Flows

4.1 Transfers and Material Scope Covered by the BCRs
All employees of Exodus have agreed to the BCRs within the scope and for the types of transfers of Personal Data specified below.

4.2 Geographical Scope of the BCRs
The structure and contact details of Exodus and its individual employees is specified in Schedule 1. It is up to the User (in the Service Agreement) to require that the BCRs apply to (i) all Personal Data Processed for Processor activities and that are submitted to EU law (for instance, data has been transferred from the European Union), or to (ii) all Processing of Personal Data Processed for Processor activities within Exodus whatever the origin of the

Personal Data.

4.3 Nature of the Personal Data
The BCRs will apply to Personal Data submitted by User to the Service. User determines the categories of Personal Data including any Special Category Data Processed within the Service. Typically, the Personal Data will include the categories of data identified below:

- Job applicants, candidates, current and former employees of staff: Name; contact information (including home and work address; home and work telephone numbers; mobile telephone numbers; web address; instant messenger; home and work email address); marital status; citizenship information; visa information; national and governmental identification information; drivers' license information; passport information; banking details; military service information; date of birth and birth place; gender; employee identification information; education, language(s) and special competencies; certification information; probation period and employment duration information; job or position title; business title; job type or code; business site; company, supervisory, cost center and region affiliation; work schedule and status (full-time or part-time, regular or temporary); compensation and related information (including pay type and information regarding raises and salary adjustments); payroll information; allowance, bonus, commission and stock plan information; leave of absence information; employment history; work experience information; information on internal project appointments; accomplishment information; sentiments, personal opinions, feedback, training and development information; award information; membership information; information on emergency contacts, beneficiaries and dependents; and diversity data, personal pronouns, disability status and accommodation needs, sexual orientation, race or ethnic origin, religious and similar philosophical beliefs and trade union membership.

- Related persons: Name and contact information (including home address; home and work telephone numbers; mobile telephone numbers); date of birth; gender; emergency contacts; beneficiary information; dependent information, including children.

- Staff of prospects, customers, business partners and suppliers: Name and contact information (including work address; work telephone numbers; mobile telephone numbers; web address; instant messenger; work email address); business title; company; course enrollment information, including completion of courses, exam results and feedback provided.

4.4 Categories of Data Subjects
The Personal Data relates to the following categories of Data Subjects:

- Job applicants, candidates, current and former employees of staff.

- Related persons (e.g., emergency contacts, dependents, or beneficiaries).

- Staff of prospects, customers, business partners and suppliers.

5. Updates to the BCRs

The BCRs can be modified, for instance, to take into account modifications of the regulatory environment, requirements or guidance, the company structure or changes to Exodus' enterprise cloud applications. Exodus shall report changes to all employees of Exodus, relevant Supervisory Authorities via the Irish Data Protection Commission in its capacity as competent Supervisory Authority for these BCRs and the Users whose Service Agreements include the BCRs on a regular basis with a brief explanation of the reasons justifying the changes.

Where a change affects the Processing conditions, would be detrimental to data subjects rights, potentially affect the level of protection offered by the BCRs, or affect the binding nature of the BCRs, or is otherwise significant, Exodus will notify the Users through an appropriate communication channel, including via customer relationship contacts promptly such that Users have the possibility to object to the change or to terminate the Service Agreement in accordance with its terms. Such significant changes shall also be notified to the relevant Supervisory Authorities via Irish Data Protection Commission as the competent Supervisory Authority for these BCRs with a brief explanation of the reasons justifying the change promptly. Exodus' Privacy and Data Protection Team keeps a fully updated list of the employees of Exodus and of the Subprocessors involved in the Personal Data Processing activities for each User which shall be made accessible to each covered User, Data Subject and Supervisory Authority. Exodus' Privacy and Data Protection Team will keep track of and record any updates to the BCRs and provide the necessary information systematically to Users and upon request to competent Supervisory Authorities. With respect to Personal Data covered by the BCRs, no transfer is made to a new employee of Exodus until the new employee is effectively bound by the BCRs and can deliver compliance. Any changes to the BCRs or to the list of employees of Exodus shall be reported once a year to the relevant Supervisory Authorities granting authorization to Exodus via the Irish Data Protection Commission with a brief explanation of the reasons justifying the update. Where a modification would affect the level of the protection offered by the BCRs or significantly affect the BCRs (i.e. changes in the bindingness), it must be promptly communicated to the relevant Supervisory Authorities via the Irish Data Protection Commission.

6. Data Protection Safeguards

6.1 Privacy Principles

The BCRs include the following principles, applicable to any employee of Exodus with respect to Personal Data and Users covered by the BCRs in accordance with the applicable Service Agreement which addresses procedural, operational and commercial arrangements, such as compensation for additional services that a User may request as part of assistance with the Users' compliance obligations under these privacy principles and applicable law. The privacy principles describe obligations of a Processor and Subprocessor in Exodus as well as obligations of a User. Users are not directly bound by these principles (only employees of Exodus are directly bound), but if a User agrees to transfer Personal Data to Exodus under a Service Agreement that refers to these BCRs, then the User agrees also to its obligations under these BCRs.

6.1.1 Transparency, Fairness and Lawfulness

Exodus and any applicable Subprocessors will have a general duty to help and assist Users to comply with the law (for instance, to be transparent about Subprocessor activities in order to allow the Users to correctly inform the Data Subject).

6.1.2 Purpose Limitation

Exodus and any applicable Subprocessors shall Process Personal Data only on behalf of the Users and in compliance with its documented instructions including with regard to transfers of Personal Data to a third country, unless required to do so by Union or Member State law. In such a case, Exodus or its Subprocessor shall inform the Users of that legal requirement before Processing takes place, unless that law prohibits such information on important grounds of public interest (Article 28 (3) (a) GDPR). In other cases, if Exodus or its Subprocessor cannot provide such compliance for whatever reasons, they will promptly inform the Customer of their inability to comply, in which case the User is entitled to suspend the transfer of Personal Data and/or terminate the applicable Service (as applicable and subject to the terms of the Service Agreement). On the termination of the provision of data processing services, Exodus and its Subprocessors shall, at the choice of the User and in accordance with the terms of the applicable Service Agreement, delete or return all Personal Data to the User (for example, by way of providing the User with administrative access to the databases of Exodus) and delete the copies thereof, unless legislation imposed upon them requires storage of the Personal Data. In that case, Exodus and its Subprocessors will inform the User and warrant that they will safeguard the confidentiality of the

Personal Data and will not actively Process the Personal Data anymore.

6.1.3 Data Quality
Exodus and any applicable Subprocessors shall assist the User to comply with the law, in particular:

When asked by a User, Exodus and its Subprocessors will execute necessary measures in accordance with the Service Agreement to enable or assist the Customer to have Personal Data updated, corrected, deleted or anonymized when the Personal Data is no longer needed in a form that identifies the Data Subjects. Where necessary, Exodus will inform each employee of Exodus and its Subprocessors to whom the Personal Data have been disclosed of any update, correction, deletion or anonymization of the Personal Data.

6.1.4 Security
Exodus and any applicable Subprocessors comply with Exodus technical and organizational measures set forth in the Service Agreement to ensure a level of security appropriate to the risks presented by the Processing as provided by Article 32 GDPR. Exodus and its Subprocessors will assist Users in ensuring compliance with the obligations as set out in Article 32 to 36 GDPR taking into account the nature of Processing and information available to Exodus and its Sub-processors (Article 28 (3) (f) GDPR) in accordance with the Service Agreement. Exodus shall inform Users without undue delay after becoming aware of any Personal Data Breach affecting the Personal Data Processed on their behalf. In addition, the Subprocessors of Exodus shall inform Exodus without undue delay after becoming aware of any Personal Data Breach affecting the Personal Data Processed on their behalf.

6.1.5 Data Subject Rights
Exodus and any applicable Subprocessors will, taking into account the nature of the Processing, assist the User by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Users' obligations to respond to requests for exercising the Data Subjects rights as set out in Chapter III of the GDPR (Article 28 (3) (e) GDPR) ("Data Subject Request"). If a Data Subject submits a Data Subject Request to Exodus or a Subprocessor and Exodus can identify the User, Exodus shall transmit such requests to the responsible User. Exodus shall not respond to any such Data Subject Request except to confirm to the Data Subject that the request relates to that User.

6.1.6 Subprocessing within the Group
Personal Data may be subprocessed by other employees of Exodus bound by the BCRs only with the prior informed specific or general written authorization of the User. The Service Agreement will specify if a general prior authorization given at the beginning of the Service would be sufficient or if a specific authorization will be required for each new Subprocessor. If a general authorization is given, the User will be informed by Exodus of any intended changes concerning the addition or replacement of a Subprocessor in such a timely fashion that the User has the possibility to object to the change or to terminate the applicable Service before the Personal Data are communicated to the new Subprocessor.

6.1.7 Onward Transfers to External Subprocessors
Personal Data may be subprocessed by non-employees of Exodus only with the prior informed specific or general written authorization of the User. The Service Agreement will specify if a general prior authorization given at the beginning of the Service would be sufficient or if a specific authorization will be required for each new Subprocessor. If a general authorization is given, the User will be informed by Exodus of any intended changes concerning the addition or replacement of Subprocessors in such a timely fashion that the User has the possibility to object to the change or to terminate the applicable Service by Exodus before the Personal Data are communicated to the new Subprocessor. Where the employee of Exodus bound by the BCRs subcontracts its obligations under the Service Agreement, with the authorization of the User, it shall do so only by way of a written contract or other legal act under Union or Member State law with the Subprocessor which ensures that adequate

protection is provided as set out in Articles 28, 29, 32, 45, 46 or 47 GDPR and that either (i) the same data protection obligations as set out in the Service Agreement between the User and Exodus and Sections 1.3, 1.4, 3 and 6 of these BCRs are imposed on the Subprocessor, or that (ii) other appropriate safeguards referred to in Article 46 (2) GDPR (including, without limitation, standard data protection clauses adopted by the European Commission per Article 46 (2) (c) GDPR) are properly implemented with the Subprocessor, in particular providing, in either case, sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR (Article 28 (4) GDPR).

6.2 Data Transfer Compliance

Various data protection laws around the world, including EEA laws, may permit international transfers of Personal Data to third countries only where appropriate safeguards are implemented to ensure the transferred data remains protected to the standard required in the country or region from which it is originally transferred. This includes transfers of Personal Data to employees of Exodus who are bound by the BCRs, and transfer (and onward transfer) from employees of Exodus to third parties who are not subject to these BCRs. Where these requirements exist, employees of Exodus must comply with them. In addition, as a Processor, employees of the Exodus must also comply with users' documented instructions in respect of any international transfers of Personal Data (as described in 6.1.2 above). Whenever transferring Personal Data internationally, or onward transferring Personal Data to third parties, the Privacy and Data Protection Team must be consulted so that they can ensure appropriate safeguards, such as standard contractual clauses (for transfers of Personal Data from the EEA) have been implemented to protect the Personal Data being transferred and a Transfer Impact Assessment (as described below) has been conducted as necessary. Exodus employees may transfer or onward transfer Personal Data internationally, only where measures necessary to comply with (i) customers' documented instructions in accordance with the Service Agreement, and (ii) applicable data protection law rules governing international or onward transfers of Personal Data, have been satisfied.

6.2.1 Transfer Impact Assessments

Where GDPR applies to the Personal Data that will be transferred (or onward transferred), then before a transferring Exodus employee makes an international transfer (or onward transfer) of Personal Data to a recipient Exodus employee or third-party data recipient (as applicable) (a "Data Recipient"), the Privacy and Data Protection Team and the transferring Exodus employee must coordinate with the Data Recipient to undertake a risk assessment. The assessment evaluates if there is any reason to believe that the laws and practices in the country where the Data Recipient will process the Personal Data, including any requirements to disclose Personal Data or measures authorising access by public authorities, will conflict with Exodus' BCRs obligations or the privacy rights and guarantees provided under the BCRs (a "Transfer Impact Assessment").[2] The Privacy and Data Protection Team shall liaise with the transferring Exodus employee as necessary to conduct the Transfer Impact Assessment, and shall coordinate with Exodus to keep it informed of the Transfer Impact Assessment and its findings. No international transfer (or onward transfer) of Personal Data may take place unless and until: (a) a Transfer Impact Assessment has been conducted; and (b) any additional safeguards that are identified as necessary pursuant to the Transfer Impact Assessment to protect the transfers of Personal Data to the Data Recipient have been implemented by the transferring Exodus employee and Data Recipient.

[2]*This assessment should confirm that, where the GDPR applies to the Personal Data that will be transferred, those laws and practices respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR, and are not otherwise in contradiction with these BCRs.*

The Transfer Impact Assessment must take due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the Processing chain, the number of actors involved and the transmission channels used; intended onward transfers;

the type of recipient; the purpose of Processing; the categories and format of the transferred Personal Data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[3];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these BCRs, including measures applied during transmission and to the Processing of the Personal Data in the country of destination.

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

The Privacy and Data Protection Team and the transferring Exodus employee will coordinate with the Data Recipient to document the Transfer Impact Assessment and make it available to the competent Supervisory Authority on request. The Privacy and Data Protection Team shall inform other relevant Exodus employees about the findings of the Transfer Impact Assessment (and if appropriate, in consultation with the User), so that they can apply any identified additional safeguards determined to be necessary (or if necessary, suspend the transfer) in respect of any identical or similar transfers they make. Where the Transfer Impact Assessment(s) conclude that it is not possible to implement any required additional safeguards to ensure the Data Recipient's Processing in the third country will be compatible with the requirements of this BCRs, then the Privacy and Data Protection Team shall inform the transferring Exodus employee (and other relevant Exodus employees) and shall prohibit any such transfer(s) by Exodus emplyee(s). The Privacy and Data Protection Team shall instruct the transferring Exodus employee to suspend the data transfer and/or terminate the contract (or affected portions of the contract, as applicable and subject to the terms of the Service Agreement) if it considers that no appropriate safeguards for such transfer can be ensured, or if the transferring Exodus employee is instructed by the User or the competent Supervisory Authority to do so. In this case, the transferring Exodus employee shall be entitled to terminate its transfers of Personal Data to the Data Recipient, insofar as it concerns the Processing of Personal Data under this BCRs (in which event, the Data Recipient must be required to return or destroy the Personal Data it received, as instructed by the transferring Exodus employee). If the transferring Exodus emplyee transfers Personal Data to two or more Data Recipients, the transferring Exodus emplyee may exercise this right to terminate only with respect to the relevant Data Recipient. The Data Recipient must use its best efforts to provide the Privacy and Data Protection Team and the transferring Exodus employee with relevant information and continue to cooperate with the Privacy and Data

Protection Team and the transferring Exodus employee to ensure compliance with the requirements of this BCRs throughout the duration of the transfer and subsequent Processing. If the Data Recipient is not a Exodus employee (i.e. if it is a third party data recipient), the Privacy and Data Protection Team and the transferring Exodus employee must exercise appropriate diligence to ensure that the Data Recipient will continue to provide such cooperation, including where appropriate by seeking contractual assurances from the Data Recipient.

6.2.2 Transfer Risk Notifications

The Data Recipient and the transferring Exodus employee must notify the Privacy and Data Protection Team (and in the case of the Data Recipient also the transferring Exodus employee) promptly if, at any time during which it transfers, receives or Processes Personal Data, it has reason to believe that it, is or has become subject to laws or practices not in line with the requirements of this BCRs, including following a change in the laws of the third country where it transfers, receives or Processes Personal Data or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements of this BCRs (a "Transfer Risk Notification"). If the Data Recipient is not a Exodus employee (i.e. if it is a third-party data recipient), the Privacy and Data Protection Team and the transferring Exodus employee must exercise appropriate diligence to ensure that the Data Recipient will provide any such Transfer Risk Notification, including where appropriate by seeking contractual assurances from the Data Recipient. The Privacy and Data Protection Team shall further assess the laws and practices of any third country to which it transfers Personal Data on a regular basis to ensure that any such transfers do not become incompatible with the obligations under these BCRs. On receipt of a Transfer Risk Notification, the Privacy and Data Protection Team, together with the transferring Exodus employee and the Data Recipient, will promptly update the Transfer Risk Assessment and follow the steps identified at 6.2.1 above.

Following receipt of a Transfer Risk Notification relating to a legally binding request from a public authority or direct access by a public authority, the Privacy and Data Protection Team shall promptly inform the User unless otherwise prohibited (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). If communication with the User is prohibited, the Privacy and Data Protection Team shall put the request on hold and inform the competent Supervisory Authority about the request, including information about the Personal Data requested, the requesting body and the legal basis for disclosure (unless otherwise prohibited).
If in specific cases the suspension and/or notification are prohibited, the requested employee of the Exodus will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible to the User or the competent Supervisory Authority (as applicable), and be able to demonstrate that it did so. If, in the above cases, despite having used its best efforts, the employee of the Exodus is not able to notify the competent Supervisory Authority, it will provide general information on the requests it received to the competent Supervisory Authority (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.) on an annual basis. In any case, transfers of Personal Data by an employee ofthe Exodus to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

6.3 Accountability and other Tools

Exodus shall, in accordance with the Service Agreement, make available to Users all information necessary to demonstrate compliance with its obligations as provided by Article 28 (3) (h) GDPR and allow for and contribute to audits, including inspections conducted by the respective User or another auditor mandated by the User. In addition, the Exodus shall immediately inform a User if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. In order to demonstrate compliance with these BCRs, employees of Exodus maintain records of all categories of Processing activities carried out on behalf of Customers in line with the requirements as set out in Article 30 (2) GDPR. This record will be maintained in writing, including in electronic form and will be made available to the relevant Supervisory Authority on request (Articles 30 (3) and 30 (4) GDPR).

The employees of Exodus shall also assist the User in implementing appropriate technical and organizational measures to comply with data protection principles and facilitate compliance with the requirements set up by the BCRs in practice such as data protection by design and by default (Articles 25 and 47 (2) (d) GDPR).

6.4 The Relationship between National Laws and BCRs
Where local legislation, for instance EU legislation, requires a higher level of protection for Personal Data it will take precedence over these BCRs. At all times, Personal Data shall be Processed in accordance with applicable law. The User shall notify Exodus about any additional or higher data protection law requirements applicable to the User and its Personal Data.

Schedule 1
Employees of Exodus bound by the BCRs

Exodus can be contacted via its Privacy and Data Protection Team using the following contact details:

Exodus
Attn.: Privacy and Data Protection Team
help.exodus-gaming.com/contact-us/
exodus-gaming.com

Schedule 2
Exodus' technical and organizational data security measures

Exodus Universal Security Exhibit
This Exodus Universal Security Exhibit applies to the Covered Service and Covered Data. Capitalized terms used herein have the meanings given in the Agreement, including attached exhibits, that refers to this Exodus Universal Security Exhibit.

Exodus maintains a comprehensive, written information security program that contains administrative, technical, and physical safeguards that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing of Covered Data as well as the associated risks, are appropriate to (a) the type of information that Exodus will store as Covered Data; and (b) the need for security and confidentiality of such information. Exodus' security program is designed to:

- Protect the confidentiality, integrity, and availability of Covered Data in Exodus' possession or control or to which Exodus has access;

- Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Covered Data;

- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Covered Data;

- Protect against accidental loss or destruction of, or damage to, Covered Data; and

- Safeguard information as set forth in any local, state or federal regulations by which Exodus may be regulated.

Without limiting the generality of the foregoing, Exodus' security program includes:

1. **Security Awareness and Training.** Mandatory employee security awareness and training programs, which include:

    a. Training on how to implement and comply with its information security program; and

    b. Promoting a culture of security awareness.

2. **Access Controls**. Policies, procedures, and logical controls:

    a. To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;

    b. To prevent those workforce employees and others who should not have access from obtaining access; and

    c. To remove access in a timely basis in the event of a change in job responsibilities or job status.

3. **Physical and Environmental Security.** Controls that provide reasonable assurance that access to physical servers at the data centers housing Covered Data is limited to properly authorized individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes.

4. **Security Incident Procedures.** A security incident response plan that includes procedures to be followed in the event of any security breach of any application or system directly associated with the accessing, Processing, storage, or transmission of Covered Data.

5. **Contingency Planning.** Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage Covered Data or production systems that contain Covered Data.

6. **Audit Controls.** Technical or procedural mechanisms put in place to promote efficient and effective operations, as well as compliance with policies.

7. **Data Integrity.** Policies and procedures to ensure the confidentiality, integrity, and availability of Covered Data and to protect it from disclosure, improper alteration, or destruction.

8. **Storage and Transmission Security.** Security measures to guard against unauthorized access to Covered Data that is being transmitted over a public electronic communications network or stored electronically.

9. **Secure Disposal.** Policies and procedures regarding the secure disposal of tangible property containing Covered Data, taking into account available technology so that such data cannot be practicably read or reconstructed.

10. **Assigned Security Responsibility.** Assigning responsibility for the development, implementation, and maintenance of its information security program, including:

    a. Designating a security official with overall responsibility; and

b. Defining security roles and responsibilities for individuals with security responsibilities.

11. **Testing.** Regularly testing the key controls, systems and procedures of its information security program to validate that they are properly implemented and effective in addressing the threats and risks identified.

12. **Monitoring.** Network and systems monitoring, including error logs on servers, disks and security events for any potential problems. Such monitoring includes:

a. Reviewing changes affecting systems handling authentication, authorization, and auditing;

b. Reviewing privileged access to Exodus production systems Processing Covered Data; and

c. Engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

13. **Change and Configuration Management.** Maintaining policies and procedures for managing changes Exodus makes to production systems, applications, and databases Processing Covered Data.Such policies and procedures include:

a. A process for documenting, testing and approving the patching and maintenance of the Covered Service;

b. A security patching process that requires patching systems in a timely manner based on a risk analysis; and

c. A process for Exodus to utilize a third party to conduct web application level security assessments.

These assessments generally include testing, where applicable, for:

I. Cross-site request forgery

II. Services scanning

III. Improper input handling (e.g. cross-site scripting, SQL injection, XML injection, cross site flashing)

IV. XML and SOAP attacks

V. Weak session management

VI. Data validation flaws and data model constraint inconsistencies

VII. Insufficient authentication

VIII. Insufficient authorization

14. Program Adjustments. Exodus monitors, evaluates, and adjusts, as appropriate, the security program in light of:

a. Any relevant changes in technology and any internal or external threats to Exodus or the Covered Data;

b. Security and data privacy regulations applicable to Exodus; and

c. Exodus' own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

Schedule 3
Services to which the BCRs apply

Analytics and Reporting
Product SKUs
- People Analytics
- Prism Analytics

Innovation Services/Enhanced Features
- People Analytics

Financial Management
Product SKUs
- Accounting Center
- Core Financials
- Expenses
- Financial Management Connector for Salesforce
- Financial Performance Management
- Grants Management
- Project Billing
- Projects
- Revenue Management
- Time Tracking

Innovation Services/ Enhanced Features
- Financial Management ML GA Features
- Receipt Scanning for Expenses
- Supplier Invoice Automation - Scanning
- Distance Calculation for Expenses
- Auditoria AI. Smart Bots for Exodus
- Exodus Bank Connectivity

Human Capital Management
Product SKUs
- Advanced Compensation Management
- Benefits
- Cloud Connect for Benefits
- Core Human Capital Management
- Help

Human Capital Management
Journeys
Onboarding

Innovation Services/Enhanced Features
Help
Journeys

Payroll
Product SKUs
Cloud Connect for Third Party Payroll
Payroll for Australia
Payroll for Canada
Payroll for France
Payroll for United Kingdom
Payroll for United States

Innovation Services/Enhanced Features
Payroll Machine Learning Generally Available Features

Spend Management
Product SKUs
Inventory
Procurement

Innovation Services/Enhanced Features
Spend Management ML

Student
Exodus Student Service

Talent Management
Product SKUs
Candidate EngagementCareer and Development Planning
Cloud Connect for Learning
Learning
Performance and Development
Performance and Goals
Recruiting
Succession Planning
Talent Optimization
Exodus Learning for Extended Enterprise

Innovation Services/Enhanced Features
Human Capital Management ML GA Features
Cloud Connect for Learning

Talent Optimization
Public Learning Content
Learner Name
Recommended Interview Scheduling

Workforce Management

Product SKUs

Absence Management
B-comm time clock connector provided by dorakaba
Labor Optimization
Scheduling
Time Tracking
Time Tracking Hub

Innovation Services/Enhanced Features

Workforce and Pay ML

Adaptive Planning

Product SKUs

Financial Planning
Planning
Operational Planning
Sales Planning
Workforce Planning

Platform and Product Extensions - Exodus Extend

Product SKUs

Extend
Extend Integration with Third Party
Platform Services
Media Cloud
Bring Your Own Key (BYOK)

Innovation Services/Enhanced Features

User Experience Machine Learning for
Available Services
Exodus Assistant
Global Address Lookup
Notification Designer
Exodus Graph
Exodus Everywhere
Email Analytics and Email Ingestion
Intelligent Core
SMS Multi-Factor Authentication
Enterprise Search
Exodus AI Gateway
Exodus Orchestrate for Integrations
Productivity Suite ML Features
Global Address Validation
Messaging