

DATA PROCESSING ADDENDUM

This is the Data Processing Addendum (“**DPA**”) incorporating the European Union Standard Contractual Clauses and the Addendum, referred to in the master services agreement (“**MSA**”) between **BELLTREE LIMITED**, a company incorporated in Scotland with registered number SC160001 and whose registered office is at 22a/4 Calton Road, Edinburgh, Scotland, EH8 8DP (hereinafter referred to as “**Belltree**”), and you the Client. The MSA, together with the Work Statements (in reverse chronological order) are hereinafter referred to as the (“**Agreement**”).

All capitalised terms used but not defined herein shall have the meanings ascribed to such terms in the Agreement.

In the course of providing the Services pursuant to the Agreement, the Client will Process Belltree Personal Data (as defined below), and the Parties agree to comply with the terms of this DPA with respect to the Processing (as defined below) of Belltree Personal Data, each acting reasonably and in good faith.

1. DEFINITIONS

“**Addendum**” means Belltree’s International Data Transfer Addendum to the Standard Contractual Clauses, which is attached as Schedule 4 and forms part of this DPA.

“**Affiliate**” means an entity which controls, is controlled by, or is under common control with, a party, and control means the ability to vote 50% or more of the voting securities of any entity or otherwise having the ability to influence and direct the policies and direction of an entity;

“**Belltree Personal Data**” means all Personal Data Processed by the Client or its Sub-processors on behalf of Belltree pursuant to or in connection with the Agreement.

The terms, “**Commission**”, “**Controller**”, “**Data Subject**”, “**Data Protection Impact Assessment**”, “**Member State**”, “**Personal Data**”, “**Personal Data Breach**”, “**Process**”, “**Processing**”, “**Processor**”, and “**Supervisory Authority**” shall have the same meaning as in the GDPR and UK GDPR (as appropriate), and their cognate terms shall be construed accordingly.

“**Data Privacy Law**” means, as applicable, EU Data Protection Laws and UK Data Protection Laws and the data protection laws applicable in the USA from time to time (including but not limited to the EU-US Data Privacy Framework and the UK Extension to the EU-US Data Privacy Framework under Article 45 of the UK GDPR (the UK-US Data Bridge) and including without prejudice to the foregoing, the California Consumer Privacy Act 2018 and the California Privacy Rights Act 2020, the Virginia Consumer Data Protection Act 2021 and the Colorado Privacy Act 2021 and all other applicable, national, federal, state and other laws, rules and regulations relating to the Processing of Personal Data and data privacy or data protection that may exist in any relevant jurisdiction.

“**EU Data Protection Laws**” means (i) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (ii) the GDPR in each case, as may be amended, superseded or replaced and all applicable laws and

regulations relating to the processing of personal data and privacy in the European Union including where applicable the guidance and codes of practice issued by the relevant Supervisory Authority;

“European Data” means Belltree Personal Data that is subject to the protection of EU Data Protection Laws.

“GDPR” means the EU General Data Protection Regulation 2016/679.

“Party” means either Belltree or the Client as the case may be and **“Parties”** shall mean both of them.

“Permitted Purpose” means, in respect of each Party, fulfilling its obligations under the Agreement.

“Schedules” means the schedules annexed to this DPA as relative hereto and a Schedule shall mean the relevant schedule as the context requires;

“Standard contractual Clauses” means the standard contractual clauses issued by the European Commission pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, or any set of clauses approved by the European Commission or a Supervisory Authority which subsequently amends, replaces or supersedes the same which standard contractual clauses are attached as Schedule 3 and forming part of this DPA.

“Sub-processor” means any person or legal entity (including any third party and any Affiliate of the Client, but excluding an employee of the Client or any of its Sub-processors) appointed by or on behalf of the Client or any of its Affiliates to Process Belltree Personal Data.

“UK Data” means Belltree Personal Data that is subject to the protection of UK Data Protection Laws.

“UK Data Protection Laws” means the Data Protection Act 2018, the retained European Union law version of the GDPR (the **“UK GDPR”**), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive (2002/58/EC), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) and all applicable laws and regulations relating to the processing of personal data and privacy in the United Kingdom including where applicable the guidance and codes of practice issued by the relevant Supervisory Authority;

“USA” means the United States of America;

2. PROCESSING OF PERSONAL DATA

2.1 Details of the Processing. The Parties acknowledge and agree that with regard to the Processing of Belltree Personal Data, Belltree is the Controller, the Client is the Processor and that the Client may engage Sub-processors to Process Belltree Personal Data on its, and ultimately the Controller's, behalf subject to the requirements set out in Clause 5 (Sub-processors) below. The subject matter, duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (*Belltree Personal Data Processing Details*) to this DPA which forms part of this DPA.

2.2 Belltree's Processing of Personal Data. Belltree shall process Personal Data pursuant to the Agreement, including through its engagement of the Client as Processor, in accordance with the requirements of Data Privacy Law. For the avoidance of doubt, Belltree's instructions for the Processing of Belltree Personal Data shall comply with Data Privacy Law. This DPA and the Agreement are, at the time of signature of the Agreement, Belltree's documented instructions to the Client for the Processing of Belltree Personal Data. Any additional or alternate instructions must be agreed upon and documented in writing separately (which may be by email).

2.3 The Client's Processing of Belltree Personal Data. The Client shall treat Belltree Personal Data as Confidential Information and shall only Process Belltree Personal Data on behalf of Belltree and in accordance with Belltree's documented instructions, including with regard to transfers of Belltree Personal Data outside of the UK and the European Economic Area for the following purposes: (i) Processing in accordance with the Agreement; and (ii) Processing to comply with other documented reasonable instructions provided by Belltree (e.g., via email) where such instructions are consistent with the terms of the Agreement. The Client will Process Belltree Personal Data in compliance with Data Privacy Law. Belltree hereby warrants, represents, and undertakes that the Belltree Personal Data shall comply with Data Privacy Law in all respects including, but not limited to, its collection, holding, and Processing.

2.4 General. Taking into account the nature of the Processing of Belltree Personal Data and information available to the Client, subject to the specific provisions of this DPA, the Client shall assist Belltree (at the Client's reasonable expense, where such assistance exceeds standard Data Subject Requests (as hereinafter defined) response assistance) in its efforts to comply with its obligations under Data Privacy Law, including obligations relating to responding to Data Subject Requests, and in ensuring compliance with its obligations with respect to records of processing, security of Processing, notifications of Personal Data Breaches to Data Subjects and Supervisory Authorities, Data Protection Impact Assessments, and consultations with Supervisory Authorities. The Client shall (at Belltree's reasonable expense), make available to Belltree all information, to the extent the Client is in possession of such information, necessary for Belltree, as Controller, to meet its obligations under Data Privacy Law, and allow for and contribute to audits, including inspections, conducted by Belltree or another auditor mandated by Belltree in all cases subject to and in the manner provided for in Clause 6 (Security) below.

2.5 Client Records of Processing. The Client shall maintain a written record of all categories of processing activities carried out on behalf of Belltree containing:

- (a) its own name and contact details, the name and contact details of Belltree (and its Affiliates), any other processors and, where applicable, the data protection officer;
- (b) the categories of processing carried out on behalf of Belltree; and

- (c) where applicable, transfers of Belltree Personal Data outside of the UK, European Union or European Economic Area to a third country, including the identification of that third country and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the General Data Protection Regulation, the documentation of suitable safeguards.

3. CLIENT PERSONNEL

3.1 **Confidentiality.** The Client shall ensure that its personnel engaged in the Processing of Belltree Personal Data have the appropriate background and experience, are informed of the confidential nature of the Belltree Personal Data, have received appropriate training on their responsibilities and have either executed written confidentiality agreements committing them to holding the Belltree Personal Data in confidence or are under an appropriate statutory obligation of confidentiality. The Client shall ensure that such confidentiality obligations survive the termination of the personnel engagement. These Confidentiality provisions are supplementary to (and do not replace) the Confidentiality provisions in the Agreement.

3.2 **Reliability.** The Client shall take commercially reasonable steps to ensure the reliability of any the Client personnel engaged in the Processing of, or that has access to, Belltree Personal Data.

3.3 **Limitation of Access.** The Client shall ensure that third party access to Belltree Personal Data is strictly limited to those personnel requiring such access to in accordance with the Agreement.

4. DATA SUBJECT REQUESTS

4.1 **Data Subject Requests.** Taking into account the nature of the Processing, the Client shall assist Belltree (at the Client's expense) by providing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Belltree's obligation to respond to requests from Data Subjects to exercise their rights under applicable Data Privacy Law ("**Data Subject Requests**").

5. SUB-PROCESSORS

5.1 **Use of Sub-processors.** Belltree acknowledges and agrees that (a) the Client's Affiliates may be retained as Sub-processors; and (b) the Client may engage third-party Sub-processors for the fulfilment of its obligations under the Agreement and related Processing of Belltree Personal Data all in accordance with Standard Contractual Clause 9 below and as follows:

(a) the Client will restrict the Sub-processor's access to Belltree Personal Data only to what is necessary under the Agreement and the Client will prohibit the Sub-processor from accessing Belltree Personal Data for any other purpose;

(b) the Client will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor is performing the same Processing services that are being provided by the Client under this DPA, the Client will impose on the Sub-processor the same standard of contractual obligations that the Client has under this DPA; and

(c) the Client will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processors that cause the Client to breach any of the Client's obligations under this DPA.

5.2 Notification of New Sub-processors. The Client shall provide Belltree with a list of Sub-processors. Such Sub-processor list shall include the identities of such Sub-processors, their country of location as well as the type of processing they perform. The Client shall notify Belltree in writing of any proposed new Sub-processor. Belltree may object to the Client's use of any Sub-processor by notifying the Client in writing within thirty (30) business days after receipt of the list of Sub-processors or a notification of a proposed new Sub-processor. The Client shall work with Belltree in good faith to make available a commercially reasonable change which avoids the use of that proposed Sub-processor; and where such a change cannot be made within thirty (30) calendar days from receipt by the Client of Belltree's notice, notwithstanding anything in the Agreement, Belltree may by written notice to the Client with immediate effect terminate the Agreement.

6. SECURITY

6.1 Controls for the Protection of Belltree Personal Data. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Client shall maintain appropriate technical and organisational measures for protection of the security (including protection against Personal Data Breach), confidentiality and integrity of Belltree Personal Data, including (without limitation) those measures set out in Article 32 of the GDPR, and as described in Schedule 2 to this DPA (*Security Measures*) ("**Security Measures**"). Notwithstanding any provision to the contrary, the Client may modify or update the Security Measures at its discretion provided that such modification or update does not result in any degradation in the protection offered by the Security Measures and provided those Security Measures comply with Data Privacy Law. The Client shall regularly monitor compliance with such measures. In assessing the appropriate level of security, the Client shall take account of the risks that are presented by Processing, in particular from a Personal Data Breach. Without prejudice to the Client's obligation to comply at all times with Data Privacy Law, Belltree is responsible for reviewing the information made available to Belltree by the Client relating to data security and making an independent determination as to whether these measures meet Belltree's requirements and legal obligations under Data Privacy Law.

6.2 Third Party Certifications. Upon Belltree's written request at reasonable intervals (as provided below), and subject to the confidentiality obligations set forth in the Agreement, the Client shall allow for and contribute to audits and inspections ("**Audits**") conducted by Belltree (or Belltree's independent, third-party auditor that is subject to confidentiality obligations at least as restrictive as those set out in the Agreement) by providing any information reasonably necessary to demonstrate the Client's compliance with the obligations set forth in this DPA, including without limitation in the form of a copy of the Client's then most recent third-party audits or certifications, as applicable, that the Client makes available to its clients generally, or such other information as Belltree may reasonably request.

6.3 Right to Audit. The Client shall maintain complete and accurate records and information to demonstrate its compliance with this DPA, and Belltree (or its permitted third-party auditor as provided above) may perform an Audit remotely or on-site, up to one (1) time per year, with at

least three (3) weeks' advance written notice, unless Belltree knows or reasonably suspects the Client has suffered a Personal Data Breach or as otherwise required by Belltree's regulators or Applicable Law. If Belltree requests an on-site Audit, the following terms shall apply: (a) such Audit shall be limited to facilities operated by the Client and shall not exceed two (2) business days; (b) before the commencement of any such on-site Audit, Belltree and the Client acting in good faith shall mutually agree upon the scope and timing of, and procedures relating to, the Audit with a view towards minimising the disruption of the Client's business; and (c) Belltree shall promptly notify the Client with reasonably detailed information regarding any non-compliance discovered during the course of an Audit. The material and Data audited will only be those relating specifically to the subject matter of this Agreement.

6.4 Audits Pursuant to Standard Contractual Clauses. The Parties agree that the audits described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with Clauses 6.2 and 6.3 above.

6.5 Personal Data Breaches. The Client will notify Belltree without undue delay and in any case within forty-eight (48) hours after it becomes aware of any Personal Data Breach and shall provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by Belltree. The notification shall at least:

(a) describe the nature of the Personal Data Breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Belltree Personal Data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the Personal Data Breach; and

(d) describe the measures taken or proposed to be taken by the Data Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

6.6 At Belltree's request, the Client will promptly provide Belltree with such reasonable assistance as necessary to enable Belltree to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if and to the extent Belltree is required to do so under Data Privacy Law.

7. DATA TRANSFERS

Transfer of Belltree Personal Data to the Client. The Parties acknowledge that in connection with the performance of its obligations under the Agreement, the Client will be a recipient of Belltree European Data and Belltree UK Data in the country or countries identified in the Agreement. The Client agrees (1) in relation to Belltree European Data to abide by and process Belltree European Data in compliance with the Standard Contractual Clauses and (2) in relation to Belltree UK Data to abide by and process Belltree European Data in compliance with the Addendum. If and to the extent either the Standard Contractual Clauses or the Addendum (where applicable) conflict with any provision of this DPA, the Standard Contractual Clauses and/or the Addendum (as appropriate) shall prevail to the extent of such conflict.

If there is any conflict between the terms of the Agreement and this DPA, then (unless expressed otherwise herein) the Terms of the DPA shall prevail to the extent of such conflict.

8. TERMINATION

8.1 The term of this DPA will end simultaneously and automatically at the later of (i) the date of expiration or termination of the Agreement and (ii) the first date when all Belltree Personal Data is deleted from the Client's systems. After the termination of this DPA, the Client will delete or return all Belltree Personal Data (including copies thereof) promptly upon its receipt of written notice from Belltree specifying whether it chooses for such Belltree Personal Data to be deleted or returned, save that this requirement shall not apply to the extent the Client is required by Applicable Laws to retain some or all of Belltree Personal Data. Concerning European Data, Laws as used in this clause is limited to EU Data Protection Laws.

9. GENERAL

9.1 This DPA may only be amended with the written consent of both Parties.

9.2 The Parties to this DPA hereby submit to the choice of law and jurisdiction stipulated in the Agreement with respect to any disputes or claims that arise under this DPA, subject to the Standard Contractual Clauses.

SCHEDULE 1

BELLTREE PERSONAL DATA PROCESSING DETAILS

**SEE APPENDIX I. B TO THE STANDARD CONTRACTUAL CLAUSES FORMING
SCHEDULE 3 BELOW.**

SCHEDULE 2

SECURITY MEASURES

The Client shall ensure the protection of Personal Data and shall employ industry standards of technological internet and web application security to prevent security incidents from occurring. the Client shall maintain organisational and physical policies and procedures to enforce these standards.

The Client maintains organisational policies and standards in the following areas:

- Acceptable Use
- Disciplinary Action
- Protect Stored Data
- Information Classification
- Access to the sensitive cardholder data
- Physical Security
- Protect Data in Transit
- Disposal of Stored Data
- Security Awareness and Procedures
- Network security
- System and Password Policy
- Anti-virus policy
- Patch Management Policy
- Remote Access policy
- Vulnerability Management Policy
- Configuration standards
- Change Control Process
- Audit and Log review
- Penetration testing methodology
- Incident Response Plan
- Roles and Responsibilities
- Third party access to cardholder data
- User Access Management
- Access Control Policy
- Wireless Policy
- Penetration Testing methodology
- Incident Response Plan
- Roles and Responsibilities
- Third Party Access Data
- User Access Management
- Written agreements with third-party Data Processors and Sub-Processors
- Data minimisation

The Client technical infrastructure follows best practices for data protection and security:

- All the Personal Data provided shall be transferred and protected over a secure SSL connection
- Password Protection
- Multi-factor authentication
- Dashboards and alerts to enhance system control and monitoring
- Network security
- Patch Management
- Penetration Testing
- Secure Application Development

SCHEDULE 3

STANDARD CONTRACTUAL CLAUSES

Belltree, as defined in the Agreement (the “**data exporter**”)

and

The Client, as defined in the Agreement (the “**data importer**”)

each a ‘**party**’; together ‘**the parties**’,

HAVE AGREED that the Standard Contractual Clauses shall apply in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

The Standard Contractual Clauses shall be applied as follows:

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.
- (b) The Parties:
 - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);
 - (iii) Clause 9 - Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12 - Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18 - Clause 18(a) and (b);
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE TWO: Transfer controller to processor

8.1 Instructions

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union¹ (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

¹ The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

- (a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.² The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

² This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

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

MODULE TWO: Transfer controller to processor

- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

- (1) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.
- (a) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

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

- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards³;
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have

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

agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

MODULE TWO: Transfer controller to processor

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and

principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data

importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

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

APPENDIX

EXPLANATORY NOTE:

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

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s):

1. BELLTREE LIMITED, a company incorporated in Scotland with registered number SC160001 and whose registered office is at 22a/4 Calton Road, Edinburgh, Scotland, EH8 8DP
2. Contact person's name, position and contact details: Peter Clark, Technical Director (+44-131-225-4428) peterclark@belltreegroup.co.uk;
3. Role (controller/processor): Controller

Activities relevant to the data transferred under these Clauses: In the course of providing the Services pursuant to the Agreement, the data exporter will require the transfer of Belltree Personal Data to the data importer in terms of the said Agreement to permit the data importer to carry out the said Services.

Data importer(s):

1. The Client as designed in the Agreement
2. Contact person's name, position and contact details: As identified in the Agreement
3. Role (controller/processor): Processor

Activities relevant to the data transferred under these Clauses: In the course of providing the Services pursuant to the Agreement, the data importer will receive Belltree Personal Data from the data exporter in terms of the said Agreement to permit the data importer to carry out the said Services.

By entering into and executing the Agreement the Parties hereby agree to these Clauses.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

Belltree Personnel

Categories of personal data transferred

name, title, address, telephone number, email address

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

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis via standard business correspondence

Nature of the processing

Computing, storing, and transmitting to the Client as required by and strictly in accordance with the Agreement, including as necessary for:

1. the Client receiving and using the Services;
2. the Client to comply with documented instructions provided by Belltree;
3. performing the Agreement, this DPA and/or other contracts executed by the Parties;
4. resolving disputes in relation or in connection with the Agreement.

Purpose(s) of the data transfer and further processing

To supply the Services in accordance with the Agreement

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As between the Client and Belltree the duration of the Processing under this DPA is determined by Belltree; provided that, generally the duration of the Processing of Belltree Personal Data by the Client shall be for the for the Relevant Period and the term as outlined in Clause 9 of the MSA forming part of the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As above.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

Office of the Information Commissioner of the Republic of Ireland, 6 Earlsfort Terrace, Saint Kevin's, Dublin 2, D02 W773.

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

See Schedule 2 above and in addition:

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measures for user identification and authorisation

- *systems where data is stored require password authentication and are accessible only to persons who are authorised to access them*

Measures for ensuring physical security of locations at which personal data are processed

- *systems are kept within premises that are locked when not in use*

Measures for ensuring accountability

- *The Managing Director is directly accountable for data security or there is an official delegation of this responsibility*

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

**SCHEDULE 4
BELLTREE ADDENDUM**

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

This is the International Data Transfer Addendum (“**Addendum**”) referred to in Belltree’s DPA

Unless specified otherwise, words and phrases used in this Addendum shall have the meanings ascribed to them in the DPA.

Part 1: Tables

Table 1: Parties

Start date	The Commencement Date of the Agreement	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	BELLTREE LIMITED , a company incorporated in Scotland with registered number SC160001 and whose registered office is at 22a/4 Calton Road, Edinburgh, Scotland, EH8 8DP	THE CLIENT as defined in the Agreement
Key Contact(s)	Peter Clark, Technical Director (+44-131-225-4428) peterclark@belltreegroup.co.uk;	As identified in the Agreement.
Signature (if required for the purposes of Section 2)	Not Required. This Addendum is deemed to be entered into when the parties enter into the Agreement	

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:
-------------------------	---

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
2	2	2	2	2	2	NO

Table 3: Appendix Information

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Annex 1A to the Standard Contractual Clauses

Annex 1B: Description of Transfer: Annex 1B to the Standard Contractual Clauses.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Annex II to the Standard Contractual Clauses.

Annex III: List of Sub processors (Modules 2 and 3 only): Not Applicable.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	<p>Which Parties may end this Addendum as set out in Section 19:</p> <p>The Parties can end the Addendum before the end of the Relevant Period and Term in terms of Clause 9 of the Agreement, in accordance with the termination provisions contained in the Agreement.</p>
--	--

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this

Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.

UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
 - a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
 - b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
 - c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
 - a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
 - b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";
 - c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
 - d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";
 - e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

- f. References to “Regulation (EU) 2016/679”, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
- g. References to Regulation (EU) 2018/1725 are removed;
- h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
- i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
- j. Clause 13(a) and Part C of Annex I are not used;
- k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
- l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;
- m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;
- n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and
- o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

- 16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

- a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
- b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

- a its direct costs of performing its obligations under the Addendum; and/or
- b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.