

## LEVER GDPR DATA PROCESSING ADDENDUM AND STANDARD CONTRACTUAL CLAUSES

**Instructions and Effectiveness.** This Addendum has been pre-signed on behalf of Lever. To enter into this Addendum, Customer must:

- Be a customer of the Services;
- Complete the signature block below by signing and providing all items identified (see pages 5, 16, 17, 18, and 19 for signature blocks); and
- Submit the completed and signed Addendum to Lever as instructed.
- This Addendum will only be effective (as of the Effective Date) if executed and submitted to Lever accurately and in full accordance with Section 1 above and this section. If you make any deletions or other revisions to this Addendum, it will be null and void.
- Customer signatory represents to Lever that he or she has the legal authority to bind the Customer and is lawfully able to enter into contracts (e.g., is not a minor).
- This Addendum will terminate automatically upon termination of the Agreement or as earlier terminated pursuant to the terms of this Addendum.

This Data Processing Addendum and Standard Contractual Clauses (“DPA”) supplements the master subscription agreement or terms of service agreement between Lever and Customer (the “Agreement”), when the GDPR applies to Customer’s use of Lever’s Services to Process Customer Data. Except as amended by this DPA, the Agreement will remain in full force and effect.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. **Nothing in this Addendum is intended to alter or have any adverse effect on the Standard Contractual Clauses incorporated into this Addendum in Exhibit A (“Standard Contractual Clauses”). In the event that a competent government authority determines that a conflict exists between the Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.** If there is a conflict between any other agreement between the Parties including the Agreement and this DPA, the terms of this DPA will control.

- 1 Definitions.** Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below.
- 1.1 “Agreement” means any agreement between Lever and a specific customer under which Services are provided by Lever to that customer. Such an agreement may have various titles, including but not limited to “Order Form,” “Sales Order,” or “Master Subscription Agreement.”
  - 1.2 “Customer” means the entity which determines the purposes and means of Processing of Customer Data. Customer may also be referred to as Data Exporter.
  - 1.3 “Customer Data” means any “personal data” (as defined in GDPR) that is provided by or on behalf of Customer and Processed by Lever pursuant to the Agreement.
  - 1.4 “Data Protection Laws” means all laws and regulations, including laws and binding regulations of the European Union, the European Economic Area (“EEA”) and their member states, Switzerland and the United Kingdom, and any amending or replacement legislation from time to time, applicable to the Processing of Customer Data under the Agreement.
  - 1.5 “GDPR” means the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC and the UK GDPR and the Data Protection Act 2018.
  - 1.6 “Permitted Purpose” means the use of the Customer Data to the extent necessary for provision of the Services by Lever to the Customer.
  - 1.7 “Security Incident” means any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of Customer Data.
  - 1.8 “Services” means the Lever services ordered by the Customer from Lever.

- 1.9 "Standard Contractual Clauses" means the agreement, attached at Annex 2, pursuant to the European Commission decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to processors established in third countries.
- 1.10 "Sub-processor" means any entity engaged by Lever to Process Customer Data in connection with the Services.
- 1.11 "Supervisory Authority" means an independent public authority which is established by an EU Member State pursuant to the GDPR and the Information Commissioner. as the UK's independent data protection authority.
- 1.12 Terms such as "Data Subject," "Processing," "Controller," and "Processor" shall have the meaning ascribed to them in the GDPR.
- 1.13 "Third-Party Services" means connections and/or links to third party websites and/or services not included in the core Services offerings identified in the Agreement, including, without limitation, via application programming interfaces.

## 2 Data Processing.

### 2.1 *Data Processing Activities.*

- 2.1.1 Subject Matter. Lever's provision of the Services to the Customer.
- 2.1.2 Nature and Purpose. Lever will process Customer Data for the purposes of providing the Services (including administration, operations, technical and customer support), to Customer in accordance with the Agreement.
- 2.2 *Roles of the Parties.* The Parties acknowledge and agree that Lever will Process the Customer Data in the capacity of a Processor and that Customer will be the Controller of the Customer Data. Customer understands that to the extent Third-Party Services are accessed, Customer serves as the Controller and the Third-Party Services are Processors, and the Third-Party Services are not Sub-processors of Lever.
- 2.3 *Customer Instructions.* The Parties agree this DPA and the Agreement constitute Customer's documented instructions regarding Lever's processing of Customer Data. Lever will process Customer Data only in accordance with these documented instructions.
- 2.4 *Compliance with Laws.* Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR. Lever is not responsible for determining the requirements of laws applicable to Customer's business or that Lever's provision of the Services meet the requirements of such laws.

## 3 Customer Obligations.

- 3.1 *Instructions.* Customer shall provide instructions to Lever pursuant to this DPA comply with the Data Protection Laws.
- 3.2 *Data Subject and Supervisory Authority Requests.* The Customer shall be responsible for communications and leading any efforts to comply with all requests made by Data Subjects under the Data Protection Laws, and all communications from Supervisory Authorities that relate to Customer Data, in accordance with Data Protection Laws. To the extent such requests or communications require Lever's assistance, the Customer shall notify Lever of the Data Subject or Supervisory Authority request.
- 3.3 *Notice, Consent and Other Authorizations.* Customer is responsible for providing the necessary notice to the Data Subjects under the Data Protection Laws. Customer is responsible for obtaining, and demonstrating evidence that it has obtained, all necessary consents, authorizations and required permissions under the Data Protection Laws in a valid manner for Lever to perform the Services.

## 4 Lever's Obligations.

- 4.1 *Scope of Processing.* Lever will Process Customer Data on documented instructions from the Customer, and in such manner as is necessary for the provision of Services except as required to comply with a legal obligation to which Lever is subject. If Lever believes any documented instruction or additional processing instruction from Customer violates the GDPR or other Data Protection Laws, Lever will inform Customer without undue delay and may suspend the performance of the Services until Customer has modified or confirmed the lawfulness of the additional processing instruction in writing. Customer acknowledges and agrees that Lever is not responsible for performing legal research or for providing legal advice to Customer.
- 4.2 *Data Subject Requests.* If Lever receives a request from any Data Subject made under Data Protection relating to Customer Data, Lever will provide a copy of that request to the Customer within two (2) business days of receipt. Lever provides Customer with tools to enable Customer

to respond to a Data Subjects' requests to exercise their rights under the Data Protection Laws. See <https://help.lever.co/hc/en-us/articles/360003802252-How-can-I-collect-respond-to-data-requests-in-Lever->. To the extent Customer is unable to respond to Data Subject's request using these tools, Lever will provide reasonable assistance to the Customer in responding to the request.

- 4.3 *Supervisory Authority Requests.* Lever will assist Customer in addressing any communications and abiding by any advice or orders from the Supervisory Authority relating to the Customer Data.
- 4.4 *Retention.* Lever will retain Customer Data only for as long as the Customer deems it necessary for the Permitted Purpose, or as required by applicable laws. At the termination of this DPA, or upon Customer's written request, Lever will either destroy or return the Customer Data to the Customer, unless legal obligations require storage of the Customer Data.
- 4.5 *Disclosure to Third Parties and Confidentiality.* Lever will not disclose the Customer Data to third parties except as permitted by this DPA or the Agreement, unless Lever is required to disclose the Customer Data by applicable laws, in which case Lever shall (to the extent permitted by law) notify the Customer in writing and liaise with the Customer before complying with such disclosure request. Lever treats all Customer Data as strictly confidential and requires all employees, agents, and Sub-processors engaged in Processing the Customer Data to commit themselves to confidentiality, and not Process the Customer Data for any other purposes, except on instructions from Customer.
- 4.6 *Assistance.* Taking into account the nature of the Processing and the information available, Lever will provide assistance to Customer in complying with its obligations under GDPR Articles 32-36 (inclusive) (which address obligations with regard to security, breach notifications, data protection impact assessments, and prior consultation). Upon request, Lever will provide Customer a list of processing operations.
- 4.7 *Security.* Lever will keep Customer Data confidential and implement and maintain administrative, physical, technical and organizational safeguards for the security (including protection against accidental or unlawful loss, destruction, alteration, damage, unauthorized disclosure of, or access to, Customer Data transmitted, stored or otherwise Processed), confidentiality and integrity of Customer Data as detailed in Appendix 2 to Annex 1.

## 5 **Sub-Processors.**

- 5.1 SCC's. Pursuant to Clause 9 of the Standard Contractual Clauses, Customer acknowledges and expressly agrees Lever may engage new Sub-processors as described in Section 5 of this DPA.
- 5.2 *General Consent.* Customer agrees that Lever may engage third-party Sub-processors in connection with the provision of Services, subject to compliance with the requirements below. As a condition to permitting a Sub-processor to Process Customer Data, Lever will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Customer Data as those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor. Lever will provide copies of any Sub-processor agreements to Customer pursuant only upon reasonable request by Customer. To the extent necessary to protect business secrets or other confidential information, including personal data, Lever may redact the text of the agreement prior to sharing a copy.
- 5.3 *Current Sub-processor List.* Customer acknowledges and agrees that Lever may engage its current Sub-processors listed at [www.lever.co/subprocessors](http://www.lever.co/subprocessors).
- 5.4 *Written Notice Via Mailing List.* Lever will provide Customer with notice ("New Sub-processor Notice") of the addition of any new Sub-processor to the Sub-processor List at any time during the term of the Agreement. Lever will provide Customer with additional information about any Sub-processor on the Sub-processor List that Customer may reasonably request upon receipt of a New Sub-processor Notice
- 5.5 *Customer Objection.* If Customer has a reasonable basis to object to Lever's use of a new Sub-processor, Customer will notify Lever promptly in writing within 15 days after receipt of a New Sub-processor Notice. Lever will use reasonable efforts to make available to Customer a change in the affected Services or recommend a commercially reasonable change to Customer's configuration or use of the affected Services to avoid processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Lever is unable to make available such change within a reasonable period of time, which will not exceed 30 days, Customer may terminate the portion of any Agreement relating to the Services that cannot be reasonably provided without the objected-to new Sub-processor by providing written notice to Lever.

- 5.6 **Responsibility.** Lever will remain responsible for its compliance with the obligations of this DPA and for any acts and omissions of its Sub-processors that cause Lever to breach any of Lever's obligations under this DPA.
- 6 **Security Incident Notification.** Lever shall, to the extent permitted by law, notify Customer without undue delay, but no later than 48 hours after becoming aware of any Security Incident. Lever's notification of a Security Incident to the Customer to the extent known should include: (a) the nature of the incident; (b) the date and time upon which the incident took place and was discovered; (c) the number of data subjects affected by the incident; (d) the categories of Customer Data involved; (e) the measures, such as encryption, or other technical or organizational measures – that were taken to address the incident, including measures to mitigate the possible adverse effects; (f) whether such proposed measures would result in a disproportionate effort given the nature of the incident; (g) the name and contact details of the data protection officer or other contact; and (h) a description of the likely consequences of the incident. The Customer alone may notify any public authority.
- 7 **Transfers Outside of the EEA.** The Parties agree the Standard Contractual Clauses, as identified in Annex 2, will apply to Customer Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing as adequate level of protection for personal data (as described by the GDPR).
- 8 **Third Party Certifications and Audits.**
- 8.1 **Certification/SOC Report.** In addition to the information contained in this DPA, upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement place, Lever will make available the following documents and information regarding the System and Organization Controls (SOC) 2 Report (or the reports or other documentation describing the controls implemented by Lever that replace or are substantially equivalent to the SOC 2), so that Customer can reasonably verify Lever's compliance with its obligations under this DPA.
- 8.2 **Audits.** To the extent the reports provided in Section 8.1 do not verify Lever's compliance with its obligations under this DPA, and subject to the audit requirements described in Clause 8 of the Standard Contractual Clauses, Customer may audit Lever's compliance with this DPA up to once per year, unless requested by a Supervisory Authority or in the event of a Security Incident. Such audit will be conducted by an independent third party ("Auditor") reasonably acceptable to Lever. Lever will work cooperatively with Customer and Auditor to agree on a final audit plan in advance of the audit. The results of the inspection and all information reviewed during such inspection will be deemed Lever's confidential information and shall be protected by Auditor in accordance with the confidentiality provisions to be made between Lever and Auditor. Notwithstanding any other terms, the Auditor may only disclose to the Customer specific violations of the Addendum, if any, and the basis for such findings, and shall not disclose to Customer any of the records or information reviewed during the inspection.
- 9 **Liability.** To the extent permitted by applicable laws, liability arising from claims under this DPA will be subject to the terms of the Agreement.
- 10 **UK GDPR.** References in Exhibit A to the General Data Protection Regulation shall be construed to include the UK GDPR and the Data Protection Act 2018 ("UK GDPR"). References in Exhibit A to the Supervisory Authority shall be construed to include the The Information Commissioner as the UK's independent data protection authority. The governing law for interpretation of claims arising under the UK GDPR shall be the laws of England and Wales.
- 11 **Miscellaneous.**
- 11.1 **Obligations Post-termination.** Termination or expiration of this DPA shall not discharge the Parties from their obligations meant to survive the termination or expiration of this DPA.
- 11.2 **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions hereof, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. The Parties will attempt to agree upon a valid and enforceable provision that is a reasonable substitute and shall incorporate such substitute provision into this DPA.

Accepted and agreed to as of the Effective Date by the authorized representative of each party:

**Lever, Inc. ("Lever")**

**Customer ("Customer")**

DocuSigned by:  
By: David Hollady  
287DF8CD49D5407...

By: \_\_\_\_\_

Name: David Hollady

Name: \_\_\_\_\_

Title: Data Privacy Officer ("DPO")

Title: \_\_\_\_\_

Date: 9/9/2021

Date: \_\_\_\_\_

**Exhibit A:  
STANDARD CONTRACTUAL CLAUSES (CONTROLLER TO PROCESSOR)**

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) (1) for the transfer of personal data to a third country.

(b) The Parties:

- (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
- (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

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 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

- (iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

#### Clause 4

##### Interpretation

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

#### Clause 5

##### Hierarchy

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

#### Clause 6

##### Description of the transfer(s)

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

##### Clause 7 – Optional

##### Docking clause

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

## SECTION II – OBLIGATIONS OF THE PARTIES

#### Clause 8

##### Data protection safeguards

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

#### 8.1 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 Union (4) (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.

### Clause 9

#### Use of sub-processors

(a) **GENERAL WRITTEN AUTHORISATION** 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 thirty (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. (8) 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

(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.

(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.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

#### Clause 12

##### Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) 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

(a) The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

#### Clause 14

##### Local laws and practices affecting compliance with the Clauses

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

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

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

recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(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). For Module Three: The data exporter shall forward the notification to the controller.

(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, if appropriate in consultation with the controller. 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 controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## Clause 15

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

#### 15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible.

The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(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. The data exporter shall make the assessment available to the controller.

(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 and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

#### Clause 17

##### Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

#### Clause 18

##### Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland (specify Member State).

(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.

## ANNEX I

### A. LIST OF PARTIES

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

Name: [REDACTED]  
Address: [REDACTED]  
Contact person's name & position: [REDACTED]  
Contact details: [REDACTED]  
Activities relevant to the data transferred under these Clauses: [REDACTED]  
Role (controller/processor): Controller

**Data importer(s): ]**

Name: Lever, Inc.  
Address: 1125 Mission Street, San Francisco, CA 94103  
Contact person's name & position: David Hollady, DPO  
Contact Details: privacy@lever.co  
Activities relevant to the data transferred under these Clauses: provision of the Services  
Role (controller/processor): Processor

...

### B. DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred*

Data subjects include:

- Natural persons who submit personal data to the data importer via use of the Services (including via online job applications and email communication hosted by the data importer on behalf of the data exporter) ("Applicants").
- The data exporter's users who are authorized by the data exporter to access and use the Services.

*Categories of personal data transferred*

Data relating to individuals provided to Lever via the Services, by or at the direction of Customer. The Customer may submit Customer Data to the Services, and may request for Applicants to submit Customer Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, without limitation:

- Customer Data of all types that may be submitted by Applicants to the Customer via user of the Services (such as via job applications). For example: name, geographic location, age, contact details, IP address, profession, gender, employment history, employment references, salary and other preferences and other personal details that the data exporter solicits or desires to collect from its Applicants.
- Customer Data of all types that Lever may include in forms hosted on the Services for the Customer (such as may be included in a job application or interview feedback forms), or may be requested by Customer via customizable fields.

*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.*

Applicants may submit special categories of Personal Data to the data exporter via the Services, the extent of which is determined and controlled by the data exporter. For clarity, these special categories of Personal Data may include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis). Ongoing during the provision of Services to Customer.*



*Nature of the processing*

The data set out above will be routinely accessed from the data importer's systems, which are based outside of the European Economic Area.

*Purpose(s) of the data transfer and further processing*

For the purposes of delivering the Services (including administration, operations, technical and customer support).

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

During the Service Term identified in the Order Form.

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

During the Service Term identified in the Order Form.

**C. COMPETENT SUPERVISORY AUTHORITY**

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

Irish Data Protection Commission

---

**On behalf of the data exporter:**

Name (written out in full): [REDACTED]

Position: [REDACTED]

Address: [REDACTED]

Signature: [REDACTED]

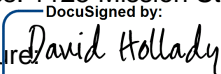
Date: [REDACTED]

**On behalf of the data importer:**

Name (written out in full): David Hollady

Position: Data Privacy Officer

Address: 1125 Mission Street, San Francisco, CA 94103

Signature: DocuSigned by: 

287DF8CD49D5407...  
Date: 9/9/2021

**ANNEX II**

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

Lever will process Customer data in accordance with the security standards identified in the Security Exhibit at [www.lever.co/security-exhibit](http://www.lever.co/security-exhibit)

---

DATA IMPORTER

Name: David Hollady, DPO

DocuSigned by:  
Authorized Signature   
287DF8CD49D5407...

DATA EXPORTER:

Name:

Authorized Signature:

### ANNEX III

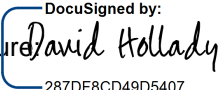
#### LIST OF SUB-PROCESSORS

The controller has authorized the use of the sub-processors identified at [www.lever.co/subprocessors](http://www.lever.co/subprocessors) as updated from time to time.

---

#### DATA IMPORTER

Name: David Hollady, DPO

DocuSigned by:  
Authorised Signature:   
287DF8CD49D5407...

#### DATA EXPORTER:

Name:

Authorised Signature: