Gdpr dpa
PEOPLELOGIC DATA PROCESSING ADDENDUM

Last Updated: June 2020

This Data Processing Addendum (this "**Addendum**") is by and between Peoplelogic, Inc. ("**Peoplelogic**") and the organization using the Peoplelogic Service that is accepting this Addendum ("**Customer**").

This Addendum applies only to the extent Customer has determined that it is a data controller subject to GDPR (defined below) and contains agreed terms relating to privacy and security. This Addendum serves as an amendment to the Peoplelogic Terms of Service (the "**Terms**"). Capitalized terms used in this Addendum but not defined have the meaning set forth in the Terms or under GDPR, as applicable.

The parties agree as follows:

1. Definitions. As used herein the following terms shall have the following definitions:

    a. **"controller", "processor", "data subject", "personal data"** and **"processing"** (and **"process"**) shall have the meanings given in Privacy Laws, as applicable to the processing of Customer Personal Data under the Terms.

    b. "**Customer Personal Data**" means personal data supplied by Customer or its Authorized Users to Peoplelogic for use with the Service provided under the Terms.

    c. "**GDPR**" means the General Data Protection Regulation, Regulation (EU) 2016/679.

    d. "**Privacy Laws**" means all applicable U.S. and international laws that regulate the use, disclosure and processing of personal data. "Privacy Laws" include as applicable GDPR and other applicable laws that specify privacy, data protection, security or security breach notification obligations that apply to personal data.

2. Roles of the Parties and Nature of Processing. The parties acknowledge and agree that Customer is the controller and Peoplelogic is a processor with regard to the processing of Customer Personal Data under the Terms. The following provides additional details relating to Peoplelogic's processing:

    - Subject matter. The subject matter of the processing is the provision of the Service and the processing described in the Terms and this Addendum.
    - Duration of processing. The Term of Service.
    - Type of personal data. Employee names, email addresses, and information about employees' use of software and software services made available by Customer to its employees.
    - Categories of data subjects. Employees of Customer.

3. Instructions for Processing. Peoplelogic shall process Customer Personal Data in accordance with the Terms and this Addendum, and as applicable based on Customer's and its Authorized Users' use and configuration of the features of the Service, all of which the parties agree serve as Customer's documented instructions. Customer may provide additional instructions to Peoplelogic to process Customer Personal Data, provided that Peoplelogic shall be obligated to perform such additional instructions only if they are consistent with the terms and scope of the Service and this Addendum.

    Peoplelogic may also process Customer Personal Data to: (a) manage its billing and accounting

functions for Customer; (b) enforce its Terms; (c) enhance and test its products and services; (d) support and maintain its Service; and (e) to deal with a legal process or law, or respond to a subpoena, court order, or government request for information. Unless prohibited by applicable law or a legally-binding request of law enforcement, Peoplelogic will promptly notify Customer of any request or demand by a government agency or law enforcement authority for access to or copy of Customer Personal Data.

4. Peoplelogic Personnel. Peoplelogic shall require its personnel who have access to Customer Personal Data: (a) to receive appropriate training on their responsibilities regarding the handling and safeguarding of Customer Personal Data, and (b) to agree to comply with confidentiality obligations that survive the termination of such personnel's employment.

5. Security Measures. Customer and Peoplelogic each shall maintain (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), appropriate technical and organizational measures to protect against loss, alteration, unauthorized disclosure of, or access to Customer Personal Data. Measures shall include as appropriate:

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

   Peoplelogic's security measures are summarized at https://peoplelogic.zendesk.com/hc/en-us/articles/360044192632. Customer is solely responsible for making an independent determination as to whether the technical and organizational measures for the Service meet Customer's requirements, including any of its security obligations under applicable Privacy Laws.

6. Compliance with Privacy Laws. Peoplelogic will comply with all Privacy Laws applicable to the delivery of the Service. Customer will comply with all Privacy Laws applicable to Customer's use of the Service. As between the parties, Customer shall be solely responsible for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer obtained Customer Personal Data.

7. Rights of Data Subjects. Unless prohibited by law, Peoplelogic will inform Customer of requests to Peoplelogic from data subjects exercising their data subject rights (such as deletion, rectification, and data portability requests) with respect to Customer Personal Data. Customer shall be solely responsible to respond to such requests from data subjects. If the Service does not provide Customer the ability to respond to such requests, then, upon Customer's request, Peoplelogic will provide reasonable assistance to Customer to respond to such requests. Depending on the nature of such assistance, Peoplelogic reserves the right to charge Customer for assistance with such requests.

8. Security Incidents. Peoplelogic shall, unless prohibited by law, notify Customer without undue delay after becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data while processed by Peoplelogic ("**Security Incident**"). Peoplelogic shall promptly: (a) investigate the Security Incident; (b) provide detailed information to Customer about the Security Incident, and (c) take reasonable steps to mitigate the effects and minimize the damage resulting from the Security Incident.

   Peoplelogic shall provide reasonably requested assistance to Customer in dealing with any Security

Incident, taking into account the nature of processing and the information available to Peoplelogic. Peoplelogic shall not make any public announcement about a Security Incident without the prior written consent of Customer, unless required by applicable law.

Customer agrees to notify Peoplelogic promptly about any possible misuse of its accounts or account credentials or any security incident Customer becomes aware of relating to the Service.

9. Customer Personal Data Deletion and Retention. Peoplelogic will maintain Customer Personal Data during the Term and for a period of 90 days after the Term. Within 60 days after such 90-day retention period., Peoplelogic will delete Customer Personal Data in its possession or control, unless otherwise required by applicable law or permitted or authorized under the Terms to retain such data.

10. Audits. Subject to reasonable notice, and at Customer's expense (including fees and expenses as mutually agreed to compensate Peoplelogic for its time and out of pocket costs involved in responding to any audit request), Peoplelogic shall provide Customer an opportunity to conduct a privacy and security audit of Peoplelogic's security program and systems and procedures that are applicable to the Service, as necessary to demonstrate Peoplelogic's compliance with Privacy Laws. Audits will occur at most annually or following notice of a Security Incident and will be subject to reasonable confidentiality procedures. If the audit report generated as a result of Customer's audit includes any finding of material non-compliance, Customer shall share such audit report with Peoplelogic and Peoplelogic shall promptly cure any material non-compliance.

11. Subprocessors Customer grants a general authorization to Peoplelogic to appoint subprocessors to support the performance of the Service, including data hosting providers.

    Peoplelogic maintains a list of subprocessors on its website at <link> and will add the names of new and replacement subprocessors to the list prior to them starting subprocessing of Personal Data. Prior email notice, or notice through the Service, will be provided to Customer of new or replacement subprocessors. If Customer has a reasonable objection to any new or replacement subprocessor, it shall notify Peoplelogic of such objections in writing within ten (10) business days of being notified and the parties will seek to resolve the matter in good faith. If Peoplelogic does not remove the new subprocessor and is unable to satisfy Customer's objections to the subprocessor within sixty (60) days from Customer's notification of objections, Customer may within thirty (30) days following the end of such sixty (60) day period, terminate the Service upon written notice to Peoplelogic.

    Peoplelogic will ensure that any subprocessor it engages on its behalf in connection with this Addendum agrees in a written contract to subprocessor terms substantially as protective of Customer Personal Data as those in this Addendum (the "**Subprocessor Terms**"). Peoplelogic shall be liable to Customer for any breach by a subprocessor of any of the Subprocessor Terms.

12. Data Transfers. Customer Personal Data that Peoplelogic processes on Customer's behalf may be transferred to, and stored and processed in, the United States. Customer appoints Peoplelogic to perform any such transfer of Customer Personal Data to the United States and to store and process Customer Personal Data to provide the Service.

    All transfers of Customer Personal Data out of the European Union, European Economic Area, and Switzerland by the Service shall be governed by the Standard Contractual Clauses in Attachment 1 hereto, unless the Customer has opted out of those clauses.

13. Entire Addendum; Conflict: This Addendum supersedes and replaces all prior and contemporaneous statements, understandings, and communications, oral and written, with regard to the subject matter of this Addendum. If there is any conflict between this Addendum and the Terms, the terms of this Addendum shall control. Except as expressly set forth in this Addendum, the Terms shall remain in place. For the avoidance of doubt, the parties intend that the limitations

on liability clauses in the Terms shall apply to this Addendum.

ATTACHMENT 1 – Standard Contractual Clauses (Processors; for data transfer)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, Customer (as data exporter) and Peoplelogic (as data importer), each a “party,” together “the parties,” agree to the following Contractual Clauses (the “Clauses” or “Standard Contractual Clauses”) 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.

References to various Articles from the Directive 95/46/EC in the Standard Contractual Clauses below will be treated as references to the relevant and appropriate Articles in the GDPR.

Clause 1: Definitions

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2: Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 below which forms an integral part of the Clauses.

Clause 3: Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4: Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 below;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5: Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11; and

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6: Liability

1. The parties agree that any data subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7: Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8: Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9: Governing Law.

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10: Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11: Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12: Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

Data exporter: The data exporter is Customer.

Data importer: The data importer is Peoplelogic.

Data subjects: Data subjects include employees of Customer.

Categories of data: The Peoplelogic service will process employee names, email addresses, and information about employees' use of software and software services (including metadata and content of activities) made available by customer to its employees. For more information, please see "What Events We Process" for each integration (for example GSuite).

Processing operations: The Customer Personal Data transferred will be subject to the following basic processing activities:

- The duration of data processing shall be for the term of the Service. The objective of the data processing is the performance of the Service.
- Additional information regarding data exporter's processing of personal data is described in the "Instructions for Processing" and the "Customer Personal Data Deletion and Retention" sections of the Addendum.
- In accordance with the Addendum, the data importer may hire other companies to provide services on data importer's behalf. Any such subcontractors will be permitted to obtain Customer Personal Data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Customer Personal Data for any other purpose.

Appendix 2 to the Standard Contractual Clauses

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

- The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Personal Data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction, as set forth in data importer's security measures document located at https://peoplelogic.zendesk.com/hc/en-us/articles/360044192632 and incorporated herein by reference.