

Data Processing Addendum EEA (formerly referenced as the GDPR Contract Addendum) (“DPA”)

1. How this addendum applies

This addendum forms part of our terms and conditions and reflects our commitment to the EU General Data Protection Regulation (GDPR).

2. Data processing terms

Definitions

"sales-i" or "us" or "our" means sales-i UK Ltd (registered in England with number 05553047 trading as sales-i).

“Affiliate” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity.

“Controller” means the entity which determines the purposes and means of the Processing of Personal Data.

“Customer Data” means data (including any Personal Data) that Customer or its Users upload into Services.

"Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

“Data Subject” means the identified or identifiable person to whom Personal Data relates.

“EEA” means the European Economic Area and their member states, Switzerland, and the United Kingdom.

“GDPR” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). “UK GDPR” means the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018.

“Personal Data” means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under

applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

“Personal Data Breach” means, an actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by sales-i and/or its Subprocessors in connection with the provision of Services under the Principal Agreement

“Processing” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processor” means the entity which Processes Personal Data on behalf of the Controller.

“Sub-processor” means a natural or legal person, public authority, agency or other body that Processes Personal Data on behalf of the Processor. “Supervisory Authority” means an independent public authority which is established by an EU Member State pursuant to the GDPR.

3. Processing of Personal Data

3.1 Roles of the Parties. The parties acknowledge and agree that related to the Processing of Personal Data, Customer is the Controller, sales-i is the Processor.

3.2. Customers' Processing of Personal Data. Customers shall, in its use of the Services, process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. The Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data.

3.3. sales-i's Processing of Personal Data. sales-i shall treat Personal Data as Confidential Information and shall only act on the written instructions of the Controller for the following purposes:

(i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other reasonable instructions provided by Customer (e.g. via email, telephone) where such instructions are consistent with the terms of the Agreement.

3.4. Rights of Data Subjects

sales-i will provide reasonable assistance to Customer to the extent it is agreed upon by the parties, at Customer's expense, to enable Customer to respond to: (i) any request from a Data Subject to exercise any of its rights under Data Protection Laws (including its rights of access, rectification, erasure, restriction, data portability and objection, as applicable); and (ii) any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third party in connection with the Processing of Personal Data. This will only apply if (x) Customer does not have the technical ability to address such a request itself or migrate Personal Data to another system or service provider; and (y) sales-i is legally permitted to do so and has reasonable access to the relevant Personal Data. If any such request, correspondence, enquiry or complaint is made directly to sales-i and where sales-i is able to correlate the Data Subject to Customer, based on the information provided by the Data Subject, sales-i will refer such Data Subject to Customer. sales-i will not be liable if Customer fails to timely and/or properly respond to the Data Subject's request.

3.5 Sub-processors

Customer consents to sales -i Affiliates being retained as Sub-processors in connection with the provision of Services under the agreement, and to sales-i's use of Sub-processors. A list of sales-i's Sub-processors then in effect is available on <https://sales-i.com/data-policy> or such other URL as is designated by sales-i from time to time.

Furthermore, Customer consents to sales-i engaging additional Sub-processors provided that sales-i imposes data protection terms on any Sub-processor to the materially equivalent standards provided for by this DPA, and sales-i remains fully liable for any breach of this DPA that is caused by its Sub-processor. Customer may object in writing to the appointment of a Sub-processor with legitimate reasons relating to the protection of Personal Data under GDPR within 10 days after the notice was posted by sales-i in writing. If no such written refusal has been made, consent will be deemed granted. If the Customer objects to the appointment of a Sub-processor as set forth herein, Customer and sales-i will work together in good faith to achieve a mutually agreeable solution. In addition, sales-i will have the right in its sole discretion to stop using that Sub-processor for its engagement with Customer, and appoint a new Sub-processor, or suspend or terminate the affected Service.

3.8 International Data Transfer. sales-i may transfer Personal Data outside of the EEA (i) to a recipient in a country that the European Commission has decided provides adequate protection for Personal Data, (ii) to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, including the data privacy framework (iii) to a recipient that has achieved binding corporate rules authorisation in accordance with Data Protection Law, (iv) under any other transfer mechanism provided by Data Protection Laws.

4. Personal Data Breaches

Upon becoming aware of a Personal Data Breach within sales-i's scope of responsibility, sales-i will inform Customer without undue delay. sales-i will implement reasonable measures necessary for securing Personal Data and for mitigating potential negative consequences for the Data Subject and will keep Customer informed about all material developments in connection with the Personal Data Breach. sales-i will not access the contents of Personal Data in order to identify information, subject to any specific legal requirements. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification duties. sales-i's notification of or response to a Personal Data Breach will not be construed as an acknowledgement by sales-i of any fault or liability with respect to the Personal Data Breach.

5. Right to Compensation and Liability.

Where a Data Subject asserts any claims against sales-i in accordance with Article 82 of GDPR, Customer will immediately notify sales-i in writing and will support sales-i in defending against such claims.

6. Details of the processing, Nature and Purpose of Processing

sales-i will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the terms and conditions, and as further instructed by Customer in its use of the Services.

7. Duration of Processing

sales-i will process Personal Data for the duration of the agreement, unless otherwise agreed upon in writing.

8. Categories of Data Subjects

Customer may submit Personal Data may submit personal data relating to the following categories of data subjects:

1. Prospects, customers, business partners and vendors of Customer (who are natural persons).
2. Employees or contact persons of customer's prospects, customers, business partners and vendors.
3. Employees, agents, advisors, freelancers of Customer
4. Customer's Users authorized by Customer to use the Services Type of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

1. First and last name
2. Title
3. Position
4. Employer
5. Contact information (company, email, phone, physical business address)
6. Professional data
7. Localization data

9. Security Measures

sales-i will maintain appropriate technical and organizational measures to protect and secure the confidentiality and integrity of customer datasets. As far as it is reasonably possible, sales-i shall assist the Controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments; sales-i shall submit to audits and inspections, provide the Controller with whatever information it needs to ensure that we are meeting our Article 28 obligations and shall always inform the Controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

10. Deletion of Personal Data

At the end of Services rendered to Customer sales-i will delete or return data sets as stipulated in our terms and conditions.

11. sales-i staff

Confidentiality. sales-i shall ensure that its personnel engaged in the processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements.

Reliability. sales-i shall take commercially reasonable steps to ensure the reliability of all sales-i staff engaged in the processing of Personal Data.

Limitation of Access. sales-i shall ensure that sales-i's staff access to Personal Data is limited to those staff performing Services in accordance with the agreement.

Updated: May 16, 2024