



GDPR CONTRACT ADDENDUM

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.

"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.

"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).

"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.

"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.

"Third Party Suppliers" are companies we engage while processing information.

"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 shall assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR.

3.5 Data Subject Request. sales-i shall, to the extent legally permitted, promptly help customers meet the following rights: right of access, right to rectification, restriction of processing, erasure ("right to be forgotten"), data portability, and object to processing.

3.6 Third Party Suppliers

3.6.1 Appointment of Third Party Suppliers. sales-i may engage third-party suppliers in connection with the provision of the Services. sales-i shall only engage these suppliers with the prior consent of the controller and under a written contract.

4. Obligations

Clause 1

Obligations of the data exporter (Controller)

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law;
- (b) that it will ensure compliance with the security measures;
- (c) 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;
- (d) In the event of using a sub-processor/third-party supplier, the processing activity is carried out with an appropriate level of protection for the personal data and the rights of data subject as the data importer under the clauses.

Clause 2

Obligations of the data importer (processor)

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. If it cannot provide such compliance for whatever reasons, it agrees to inform the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data;
- (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 necessary technical and organizational security measure before processing personal data in its possession;
- (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 unauthorized access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data;
- (f) that, in the event of sub-processing or employing a third-party supplier, it has previously informed the data exporter and obtained its prior written consent;
- (g) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 3 Breaches

- a. sales-i shall take technical and organization measures to prevent the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.
- b. Customer data incident management and notification. sales-i maintains security incident management policies and procedures specified and shall, notify Customer without undue delay (ideally within 24 hours) after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by sales-i or its Sub-processors of which sales-i becomes aware.
- c. sales-i shall make reasonable efforts to identify the cause of such customer data incident and take those steps as sales-i deems necessary and reasonable to remediate the cause of such a Customer Data Incident to the extent the remediation is within sales-i's reasonable control.
- d. The sales-i Incident Response Team is trained on the approaches to take in the event a breach occurs.
- e. The obligations herein shall not apply to incidents that are caused by the Customer or the Customer's Users.

5. 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.

Duration of Processing

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

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

6. Security

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.

sales-i shall take appropriate measures to ensure the security of the data it processes;

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

6.1 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. sales-i shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

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: Wednesday January 9 2019