

# Data Processing Terms

These Data Processing Terms (“Terms”) is entered into on between Kluster Enterprises Limited, a company registered in the United Kingdom, with registration number 09946422, and whose registered office is at Priory Close, St Mary's Gate, Lancaster, United Kingdom, LA1 1XB (“KEL”) and the company engaging with KEL as a customer, through granting KEL access to data for commercial purposes, or for evaluation and non-commercial purposes (“the Third Party”).

## 1. DEFINITIONS

In these Data Processing Terms:

<b>Appropriate Safeguards</b>	means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time;
<b>Data Controller</b>	has the meaning given to that term (or to the term ‘controller’) in Data Protection Laws;
<b>Data Processor</b>	has the meaning given to that term (or to the term ‘processor’) in Data Protection Laws;
<b>Data Protection Laws</b>	means as applicable and binding on the Third Party, KEL and/or the Services (i) in the United Kingdom the Data Protection Act 2018; and the GDPR, and/or any corresponding or equivalent national laws or regulations; (ii) in member states of the European Union (EU) and/or European Economic Area (EEA): the GDPR and all relevant EU and EEA member state laws or regulations giving effect to or corresponding with any of the GDPR; and (iii) any applicable laws replacing, amending, extending, re-enacting or consolidating any of the above Data Protection Laws from time to time;
<b>Data Subject</b>	has the meaning given to that term in Data Protection Laws;
<b>Data Subject Request</b>	means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;
<b>GDPR</b>	means the General Data Protection Regulation (EU) 2016/679;
<b>International Organisation</b>	means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
<b>International Recipient</b>	has the meaning given to that term in paragraph 6.1;
<b>Personal Data</b>	has the meaning given to that term in Data Protection Laws;
<b>Personal Data Breach</b>	means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;
<b>processing</b>	has the meanings given to that term in Data Protection Laws (and related terms such as <b>process</b> have corresponding meanings);

<b>Processing Instructions</b>	has the meaning given to that term in paragraph 2.1.1;
<b>Protected Data</b>	means Personal Data received from or on behalf of the Third Party to the extent that it is processed by KEL on Customer's behalf in connection with the performance of KEL's obligations under this Agreement;
<b>Services</b>	means the services to be provided under this Agreement.
<b>Sub-Processor</b>	means another Data Processor engaged by KEL for carrying out processing activities in respect of the Protected Data on behalf of the Third Party; and
<b>Supervisory Authority</b>	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws.

## 2. SPECIFIC INTERPRETIVE PROVISION(S)

In these Data Processing Terms:

(a) references to any applicable laws (including to the Data Protection Laws and each of them) and to terms defined in such applicable laws shall be replaced with or incorporate (as the case may be) references to any applicable laws replacing, amending, extending, re-enacting or consolidating such applicable law (including the GDPR and any new Data Protection Laws from time to time) and the equivalent terms defined in such applicable laws, once in force and applicable;

(b) a reference to a law includes all subordinate legislation made under that law; and

(c) references to "paragraph numbers" are to paragraphs of these Data Processing Terms.

## 3. DATA PROCESSING PROVISIONS

### 1 Data Processor and Data Controller

1.1 The parties agree that, for the Protected Data, the Third Party shall be the Data Controller and KEL shall be the Data Processor.

1.2 KEL shall process Protected Data in compliance with:

1.2.1 the obligations of Data Processors under Data Protection Laws in respect of the performance of its obligations under this Agreement; and

1.2.2 the terms of this Agreement.

1.3 The Third Party shall comply with:

1.3.1 all Data Protection Laws in connection with the processing of Protected Data, the Services and the exercise and performance of its respective rights and obligations under this Agreement, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and

1.3.2 the terms of this Agreement.

1.4 The Third Party warrants, represents and undertakes, that:

- 1.4.1 all data sourced by the Third Party for use in connection with the Services, prior to such data being provided to or accessed by KEL for the performance of the Services under this Agreement, shall comply in all respects, including in terms of its collection, storage and processing (which shall include the Third Party providing all of the required fair processing information to, and obtaining all necessary consents from, Data Subjects), with Data Protection Laws;
- 1.4.2 all instructions given by it to KEL in respect of Personal Data shall at all times be in accordance with Data Protection Laws; and
- 1.5 The Third Party shall not withhold, delay or condition its agreement to any Change requested by KEL in order to ensure the Services and KEL (and each Sub-Processor) can comply with Data Protection Laws.

## **2 Instructions and details of processing**

- 2.1 Insofar as KEL processes Protected Data on behalf of the Third Party, KEL:
  - 2.1.1 unless required to do otherwise by applicable law, shall (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Third Party's documented instructions as set out in this paragraph 2 and Schedule 1 (Data processing details), as updated from time to time in accordance with the Change Control Procedure (**Processing Instructions**);
  - 2.1.2 if applicable law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Third Party of any such requirement before processing the Protected Data (unless applicable law prohibits such information on important grounds of public interest); and
  - 2.1.3 shall inform the Third Party if KEL becomes aware of a Processing Instruction that, in KEL's opinion, infringes Data Protection Laws, provided that:
    - (a) this shall be without prejudice to paragraphs 1.3 and 1.4;
    - (b) to the maximum extent permitted by mandatory law, KEL shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any processing in accordance with the Third Party's Processing Instructions following the Third Party's receipt of that information; and
    - (c) this paragraph 2.1.3 shall only apply from the GDPR Date.
- 2.2 The processing of Protected Data to be carried out by KEL under this Agreement shall comprise the processing set out in Schedule 1 (Data processing details), as may be updated from time to time by agreement between the parties.

## **3 Technical and organisational measures**

- 3.1 KEL shall implement and maintain, at its cost and expense, the technical and organisational measures:
  - 3.1.1 in relation to the processing of Protected Data by KEL, as set out in Schedule 1;
  - 3.1.2 to secure all Personal Data accessed or processed by KEL against accidental or unlawful loss; against destruction or damage; against any unauthorized access to and knowledge of the personal data; and against any other processing of the personal data in violation of this Agreement. Updated security documentation is available by request

3.1.3 from the GDPR Date, taking into account the nature of the processing, to assist the Third Party insofar as is possible in the fulfilment of the Third Party's obligations to respond to Data Subject Requests relating to Protected Data.

3.2 Any additional technical and organisational measures shall be at the Third Party's cost and expense.

#### **4 Using staff and other processors**

4.1 Customer acknowledges and agrees that KEL may engage third-party Sub-processors (as set out in Schedule 2) in connection with the provision of the Services. KEL has entered into a written agreement with each Sub-processor containing data protection obligations substantially similar to those in this Agreement with respect to the protection of Protected Data to the extent applicable to the nature of the Services provided by such Sub-processor. KEL shall provide notification by email to the named contact on the Order Form of a new Sub-processor before authorising any new Sub-processor to Process Protected Data in connection with the provision of the Services. Customer may object to KEL's use of a new Sub-processor by notifying KEL promptly in writing within ten (10) business days after receipt of KEL's notice. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, KEL will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Protected Data by the objected-to new Sub-processor without unreasonably burdening the Third Party. If KEL is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate this Agreement for convenience without penalty, by providing written notice to KEL.

4.2 KEL shall remain fully liable for all the acts and omissions of each Sub-Processor, to the extent that they would be breaches of these Data Processing Terms if committed by KEL.

4.3 KEL shall ensure that all persons authorised by it (or by any Sub-Processor) to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data confidential (except where disclosure is required in accordance with applicable law, in which case KEL shall, where practicable and not prohibited by applicable law, notify the Third Party of any such requirement before such disclosure). KEL shall ensure that such obligations survive the termination of the engagement with such persons.

#### **5 Assistance with the Third Party's compliance and Data Subject rights**

5.1 KEL shall refer all Data Subject Requests it receives to the Third Party within *[three]* Business Days of receipt of the request, provided that if the number of Data Subject Requests exceeds 5 per calendar month, the Third Party shall pay KEL's charges calculated on a time and materials basis at KEL's then current rates for recording and referring the Data Subject Requests in accordance with this paragraph 5.1.

5.2 From the GDPR Date, KEL shall provide such reasonable assistance as the Third Party reasonably requires (taking into account the nature of processing and the information available to KEL) to the Third Party in ensuring compliance with the Third Party's obligations under Data Protection Laws with respect to:

5.2.1 security of processing;

5.2.2 data protection impact assessments (as such term is defined in Data Protection Laws);

5.2.3 prior consultation with a Supervisory Authority regarding high risk processing; and

5.2.4 notifications to the Supervisory Authority and/or communications to Data Subjects by the Third Party in response to any Personal Data Breach,

provided the Third Party shall pay KEL's charges for providing the assistance in this paragraph 5.2, such charges to be calculated on a time and materials basis at KEL's then-current rates.

## **6 International data transfers**

6.1 The Third Party agrees that KEL may transfer Protected Data to countries outside the United Kingdom or to any International Organisation(s) (an **International Recipient**), provided all transfers by KEL of Protected Data to an International Recipient shall (to the extent required under Data Protection Laws) be effected by way of Appropriate Safeguards and in accordance with Data Protection Laws. The provisions of this Agreement shall constitute the Third Party's instructions with respect to transfers in accordance with paragraph 2.1.

## **7 Records, information and audit**

7.1 KEL shall maintain, in accordance with Data Protection Laws binding on KEL, written records of all categories of processing activities carried out on behalf of the Third Party.

7.2 KEL shall, in accordance with Data Protection Laws, make available to the Third Party such information as is reasonably necessary to demonstrate KEL's compliance with the obligations of Data Processors under Data Protection Laws, and allow for and contribute to audits by the Third Party (or another auditor mandated by the Third Party) for this purpose, subject to the Third Party:

7.2.1 giving KEL reasonable prior notice of such information request, audit and/or inspection being required by the Third Party;

7.2.2 ensuring that all information obtained or generated by the Third Party or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to the Supervisory Authority or as otherwise required by applicable law);

7.2.3 ensuring that such audit or inspection is undertaken during normal business hours, with minimal disruption to KEL's business, the Sub-Processors' business and the business of other customers of KEL; and

7.2.4 paying KEL's reasonable costs for assisting with the provision of information and allowing for and contributing to inspections and audits.

## **8 Breach management and notification**

8.1 In respect of any Personal Data Breach involving Protected Data, KEL shall, without undue delay:

8.1.1 notify the Third Party of the Personal Data Breach;

8.1.2 provide the Third Party with details of the Personal Data Breach;

8.1.3 make reasonable efforts to identify the cause of such Personal Data Breach and take those steps as KEL deems necessary and reasonable in order to remediate the cause of such a Personal Data Breach to the extent the remediation is within KEL's reasonable control.

8.1.4 keep the Third Party informed of all developments in connection with the Personal Data Breach.

8.1.5 In the case that the Personal Data Breach is caused by the Third Party or the Third Party's users, KEL will assist the Third Party in remediating the cause of the Personal Data Breach on time and material on basis of standard hourly rates, to the extent that it is commercially reasonable to do so.

## **9 Deletion or return of Protected Data and copies**

9.1 KEL shall, at the Third Party's written request, either delete or return all the Protected Data to the Third Party in such form as the Third Party reasonably requests within a reasonable time after the earlier of:

9.1.1 the end of the provision of the relevant Services related to processing; or

9.1.2 once processing by KEL of any Protected Data is no longer required for the purpose of KEL's performance of its relevant obligations under this Agreement,

and delete existing copies (unless storage of any data is required by applicable law and, if so, KEL shall inform the Third Party of any such requirement).

## **10 Survival of data protection provisions**

10.1 Paragraphs 1 to 10 (inclusive) shall survive termination (for any reason) or expiry of this Agreement and continue:

10.1.1 indefinitely in the case of paragraphs 9 to 10 (inclusive); and

10.1.2 until 12 months following the earlier of the termination or expiry of this Agreement in the case paragraphs 1 to 8 (inclusive),

provided always that any termination or expiry of paragraphs 1 to 8 (inclusive) shall be without prejudice to any accrued rights or remedies of either party under any such paragraphs at the time of such termination or expiry.

SCHEDULE 1  
DATA PROCESSING DETAILS

---

**1 Subject-matter of processing:**

The subject-matter of processing of Personal Data by KEL is the provision of the Services to the Controller. The services may contain but are not limited to sales analytics – including forecasting, historic reporting, dashboarding, targeting and KPI engineering; based on sales and related data provided to KEL by the Third Party.

**2 Duration of the processing:**

For the duration of this Agreement as defined on the Order Form.

**3 Nature and purpose of the processing:**

The Third Party is using the Services provided by KEL for the purpose of sales analytics. The sales analytics provided may include features such as revenue forecasting; historic reporting on sales data; dashboarding; target and KPI engineering and mapping to sales data; and pipeline management.

For the purposes of providing the Services, KEL imports copies of the Third Party's data, stores the data, runs analytics on the data, and stores the results of the analytics.

In the provision of the Services, the data delivered to the Third Party through a web browser may contain the Third Party's data, and / or the analytics data, which may be merged with it, and which may be further aggregated, separated and analysed.

The Services are highly configurable, at the Third Party's request. By default, KEL do not import the Third Party's data from fields which are designed to hold personal data of clients, prospects or other third parties in their CRM. Examples of these fields which are excluded by default are first name, last name, email address and telephone number, of a contact or a lead.

However, if the client requests that personal data fields (for example, those listed in the above paragraph) are to be accessed by KEL, this may be done in order to provide the Services.

Personal data from the User object in the CRM is imported so that the sales data can be linked back to the employees of the Third Party. Personal data of employees of the Third Party such as first name, last name and email address are used to configure their user profiles, login information, and contact them by email and through the Intercom messaging service.

The Services provided offer analytics on how the User (an employee of the Third Party) interacts with the Third Party's CRM system (which may or may not be Salesforce, HubSpot CRM, or Microsoft Dynamics). An example could be a report which analyses the number of times, and frequency with which, a CRM user edits a sales opportunity (or deal) within the lifetime of a successful sale. In this example, no personal information of clients, prospects or third parties to the Third Party in the CRM are attributed to this report. However, this report may be attributable to the CRM user (an employee of the Third Party).

The Third Party may use the Services to assist in deciding what targets to set for a given person or team, and input into the Services through the browser. These targets may be based on data attributable to a person, however on a stand-alone basis they are not designed to contain personal data.

As part of the operation of the Services, user accounts with associated profiles and roles may be provisioned and managed. Such user profiles include, may include, but is not limited to, Personal Data such as full name, e-mail address, profile picture, login credentials and login IP address. The Services will maintain an activity log for each user profile.

The Data Controller acknowledges that the Service is not intended or designed for the Processing of Sensitive Information such as the special categories of personal data covered by articles 8, 9 and 10 of the GDPR, and agree not to host any Sensitive Information through the Service without prior agreement with the Data Processor.

#### **4 Type of Personal Data:**

Depending on how the Third Party uses the Services, types of personal data may contain first name, last name, profile photograph, email address, IP address of users and/or third parties whose information is held within the Third Party's data systems.

#### **5 Categories of Data Subjects:**

Data subjects are:

- Users
  - Personal information on the users of Kluster is gathered for purposes such as setting up their profile and monitoring their usage.
- Employees
  - Employees of the Third Party are analysed within Kluster, and may or may not also be users. Personal data such as their first and last names are used to make them identifiable in the platform, and link them to the sales information being analysed.
- Third parties (clients, prospects)
  - Personal information of third parties of the Third Party such as names or email addresses may be used in Kluster when the sales data is imported, updated and processed so the Third Party can link analytics to individuals.



SCHEDULE 2  
SUB-PROCESSORS

---

The Data Processor uses Sub-processors to assist in providing the Services. Sub-processors of Personal Data are as follows:

**Microsoft Azure**

Location: Datacentres around the EEA

The entirety of the core Kluster services are hosted on Microsoft Azure where possible. This includes services which import and analyse data, data storage, code repositories, code hosting, and application hosting.

An extract from the “Processor Confidentiality Commitment” clause within the Licensing Terms with Microsoft agreement is as follows:

“Microsoft will ensure that its personnel engaged in the processing of Customer Data and Personal Data (i) will process such data only on instructions from Customer, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends.”

Full details can be found here:

<http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46>

**Intercom**

Location: Ireland

Intercom is used to collect usage analytics for users logged into the Services. Intercom is also used for both chat and email conversations with KEL support. Intercom processes personal data of logged-in users including name, email address, title, browsing activity and support conversations.

Clause 8.4 of the Subscription Terms of Service explicitly states that section 15 (Confidential Information) will survive any expiration or termination of the agreement. An extract from section 15 is as follows:

“Except as expressly authorized herein, the Receiving Party will (1) hold in confidence and not disclose any Confidential Information to third parties and (2) not use Confidential Information for any purpose other than fulfilling its obligations and exercising its rights under this Agreement.”

Full details can be found here: <https://www.intercom.com/terms-and-policies>