Alliants Limited,
Office 4, Universal Marina,
Southampton, Hants, SO31 7ZN
United Kingdom

Reg. number: 6868886
info@alliants.com
www.alliants.com

Alliants AXP Data Processing Agreement

Last Modified: 12/09/2025

BETWEEN:

1) Customer listed within the Alliants Order Form and/or Statement of Work ("you" or "Data Controller") and

2) Alliants Limited, a company registered in England under number 6868886, whose registered office is at Fleming Court Leigh Road, Eastleigh, Southampton, Hampshire, United Kingdom, SO50 9PD ("us""Data Processor").

This Alliants Data Processing Agreement and its Schedules ("Agreement") reflects the Parties' agreement with respect to the Processing of Personal Data by us on behalf of you in connection with the Alliants Experience Platform ("AXP") under the Alliants Order Form and/or Statement of Work between you and us.

Alliants Limited acts as a Data Processor and Customer as a Data Controller under this Agreement and any required International Data Transfer Agreement.

This Agreement will be updated from time to time. If you require previous versions of the Agreement, please request them by emailing support@alliants.com

This Data Processing Agreement includes:

1) The Parties to this Agreement, attached hereto at Schedule 1.

2) Details of the subject matter of the Processing, duration of the Processing, the nature and purpose of the Processing, the type of Personal Data, the categories of Data Subjects and the arrangements for the destruction of the Personal Data upon termination of the SOW, set out here at Schedule 2.

3) List of approved Sub-Processors, attached hereto at Schedule 3.

4) List of technical and organisational measures to ensure the security of Personal Data, attached hereto at Schedule 4.

5) The mandatory clauses required under an International Data Transfer Agreement, attached hereto at Schedule 5.

6) List of jurisdictions to which transfers of Personal Data can be made without requiring an International Data Transfer Agreement, attached hereto at Schedule 6.

WHEREAS:

1) As set out within the Alliants Order Form between the Data Controller and the Data Processor, entered into on the "effective date" found within "Effective Date, Terms and Renewal" Section of the Alliants Order Form, the Data Processor provides to the Data Controller the Services described in the Statement of Work.

2) The provision of the Services by the Data Processor involves processing the Personal Data described in Schedule 2 on behalf of the Data Controller.

3) Under Article 28, paragraph 3 of the UK and EU GDPR, the Data Controller is required to put in place an agreement in writing with any organisation which processes Personal Data on its behalf. This agreement shall govern the processing of that Personal Data.

4) The Parties have agreed to enter into this Agreement to ensure compliance with the said provisions of the UK and EU GDPR in relation to all processing of the Personal Data by the Data Processor for the Data Controller.

5) The terms of this Agreement are to apply to all processing of Personal Data carried out for the Data Controller by the Data Processor and to all Personal Data held by the Data Processor in relation to all such processing.

IT IS AGREED as follows:

1.   Definitions and Interpretation

1.1.   In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

"Californian Data Protection Laws"	means the California Consumer Privacy Act of 2018 (CCPA) and the California Privacy Rights Act (CPRA);
"Data Privacy Laws"	means (i) the EU GDPR (ii) the UK Data Protection Laws (iii) the Californian Data Protection Laws;

alliants

"Data Controller", "Data Processor", "Processing", "Data Subject" and "Supervisory Authority"	shall have the meanings given to the terms "controller", "processor", "processing", "data subject" and "supervisory authority" respectively in Article 4 of the EU and UK GDPR;
"EU GDPR"	means the EU Regulation 2016/679 General Data Protection Regulation, as amended or replaced from time to time;
"ICO"	means the UK's Supervisory Authority, the Information Commissioner's Office;
"IDTA"	means International Data Transfer Agreement VERSION A1.0, in force 21 March 2022, issued by the Information Commissioner's Office, as may be amended, superseded or replaced;
"IDT Addendum"	means International Data Transfer Addendum to the EU Commission Standard Contractual Clauses VERSION B1.0, in force 21 March 2022, issued by the Information Commissioner's Office, as may be amended, superseded or replaced;
"Personal Data"	means all such "personal data", as defined in Article 4 of the UK and EU GDPR, as is, or is to be, processed by the Data Processor on behalf of the Data Controller, as described in Schedule 2;
"Services"	means those services described in the SOW which are provided by the Data Processor to the Data Controller and which the Data Controller uses for the purposes described in the SOW;
"Standard Contractual Clauses"	means the clauses issued by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as may be amended, superseded or replaced;
"Sub-Processor"	means any processor appointed by the Data Processor to process the Personal Data;
"SOW"	Statement of Work and/or Alliants Order Form;
"Supervisory Authority"	means an independent public authority regulating the processing of Personal Data; and
"UK Data Protection Laws"	means the UK General Data Protection Regulation, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations and all other applicable UK national laws and regulations, as amended or replaced from time to time.
"UK GDPR"	UK General Data Protection Regulation, as amended or replaced from time to time.

alliants

For clarity, this Data Processing Agreement covers any processing that takes place pursuant to the CCPA and the CPRA. Therefore, the following references in the CCPA and CPRA have the following meanings in this DPA:

"Business"   means **"Controller"**

"Service Provider"   means **"Processor"**

"Third Party"   means **"Sub-Processor"**

"Personal Information"   means **"Personal Data"**

"Consumer"   means **"Data Subject"**

1.2.   Unless the context otherwise requires, each reference in this Agreement to:

1.2.1.   "writing", and any cognate expression, includes a reference to any communication affected by electronic or facsimile transmission or similar means;

1.2.2.   a statute or a provision of a statute is a reference to that statute or provision as amended or re-enacted at the relevant time;

1.2.3.   "this Agreement" is a reference to this Agreement and each of the Schedules as amended or supplemented at the relevant time;

1.2.4.   a Schedule is a schedule to this Agreement; and

1.2.5.   a Clause or paragraph is a reference to a Clause of this Agreement (other than the Schedules) or a paragraph of the relevant Schedule.

1.2.6.   a "Party" or the "Parties" refer to the parties to this Agreement.

1.3.   The headings used in this Agreement are for convenience only and shall have no effect upon the interpretation of this Agreement.

1.4.   Words imparting the singular number shall include the plural and vice versa.

1.5.   References to any gender shall include all other genders.

1.6.   References to persons shall include corporations.

2.   Scope and Application of this Agreement

2.1.   The provisions of this Agreement shall apply to the processing of the Personal Data described in Schedule 2, carried out for the Data Controller by the Data Processor, and to all Personal Data held or accessed by the Data Processor in relation to all such processing whether such Personal Data is held at the date of this Agreement or received afterwards.

alliants

2.2.   The provisions of this Agreement supersede any other arrangement, understanding, or agreement including, but not limited to, the SOW made between the Parties at any time relating to the Personal Data.

2.3.   This Agreement shall continue in full force and effect for so long as the Data Processor is processing Personal Data on behalf of the Data Controller, and thereafter as provided in Clause 9.

3.   Provision of the Services and Processing Personal Data

The Data Processor is only to carry out the Services, and only to process the Personal Data received from the Data Controller:

3.1.   for the purposes of those Services and not for any other purpose;

3.2.   to the extent and in such a manner as is necessary for those purposes; and

3.3.   strictly in accordance with the express written authorisation and instructions of the Data Controller (which may be specific instructions or instructions of a general nature or as otherwise notified by the Data Controller to the Data Processor).

4.   Data Protection Compliance

4.1.   All instructions given by the Data Controller to the Data Processor shall be made in writing and shall at all times be in compliance with the Data Privacy Laws and other applicable laws. The Data Processor shall act only on such written instructions from the Data Controller unless the Data Processor is required by law to do otherwise (as per Article 29 of the UK and EU GDPR).

4.2.   The Data Controller acknowledges and agrees to be solely responsible for: (i) the accuracy, quality and legality of Personal Data processed under this Agreement, and the means by which the Data Controller has acquired this Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Privacy Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorisations; (iii) ensuring you have the right to transfer, or provide access to, the Personal Data to the Data Processor for Processing in accordance with the SOW related to this Agreement.

4.3.   The Data Controller acknowledges and agrees that, in connection with the performance of the services under the SOW, Personal Data will be transferred from the Data Processor to the Data Controller.

4.4.   The Data Processor shall promptly comply with any request from the Data Controller requiring the Data Processor to amend, transfer, delete, or otherwise dispose of the Personal Data, in accordance with Clause 11 of this Agreement.

alliants

4.5.   The Data Processor shall transfer all Personal Data to the Data Controller on the Data Controller's request in the formats, at the times, and in compliance with the Data Controller's written instructions.

4.6.   Both Parties shall comply at all times with the Data Privacy Laws and other applicable laws and shall not perform their obligations under this Agreement or any other agreement or arrangement between themselves in such a way as to cause either Party to breach any of its applicable obligations under the Data Privacy Laws.

4.7.   The Data Processor agrees to comply with any reasonable measures required by the Data Controller to ensure that its obligations under this Agreement are satisfactorily performed in accordance with any and all applicable legislation from time to time in force (including, but not limited to, the Data Privacy Laws) and any best practice guidance issued by the ICO or other relevant Supervisory Authority.

4.8.   The Data Processor shall provide all reasonable assistance to the Data Controller in complying with its obligations under the Data Privacy Laws with respect to the security of processing, the notification of personal data breaches, the completion of data protection impact assessments, and in dealings with the ICO or other relevant Supervisory Authority.

4.9.   When processing the Personal Data on behalf of the Data Controller, the Data Processor shall:

4.9.1.   not transfer any of the Personal Data to any third party without the written consent of the Data Controller and, in the event of such consent, the Personal Data shall be transferred strictly subject to the terms of a suitable agreement, as set out in Clause 10;

4.9.2.   process the Personal Data only to the extent, and in such manner, as is necessary in order to comply with its obligations to the Data Controller or as may be required by law (in which case, the Data Processor shall inform the Data Controller of the legal requirement in question before processing the Personal Data for that purpose unless prohibited from doing so by law);

4.9.3.   implement appropriate technical and organisational measures and take all steps necessary to protect the Personal Data against any unauthorised processing, including any accidental or unlawful loss, destruction, damage, alteration, disclosure or access. In assessing the appropriate level of security, the Parties shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks for Data Subjects. The Data Processor shall at least implement the technical and organisational measures specified in Schedule 4 and shall inform the Data Controller in advance of any changes to such measures;

4.9.4.   if so requested by the Data Controller (and within the timescales required by the Data Controller) supply further details of the technical and organisational systems in place to safeguard the security of the Personal Data held and to prevent unauthorised access;

alliants

4.9.5.   keep detailed records of all processing activities carried out on the Personal Data in accordance with the requirements of Article 30(2) of the UK and EU GDPR;

4.9.6.   make available to the Data Controller any and all such information as is reasonably required and necessary to demonstrate the Data Processor's compliance with the UK and EU GDPR;

4.9.7.   on reasonable prior notice and the Data Controller paying our reasonable costs, submit to audits and inspections and provide the Data Controller with any information reasonably required in order to assess and verify compliance with the provisions of this Agreement and both Parties' compliance with the requirements of the UK and EU GDPR. The requirement to give notice will not apply if the Data Controller believes that the Data Processor is in breach of any of its obligations under this Agreement or under the law; and

4.9.8.   inform the Data Controller without undue delay if it is asked to do anything that infringes the UK and EU GDPR or any other applicable data protection legislation.

5.   International Processing

5.1.   Conditions for international processing:

5.1.1.   the Data Processor shall only process Personal Data on behalf of the Data Controller (including a return of Personal Data to the Data Controller) where the transfer is:

5.1.1.1.   to a jurisdiction deemed by the UK Secretary of State to have an adequate level of protection (an adequacy regulation); or

5.1.1.2.   made pursuant to a transfer framework deemed adequate and approved by the UK Secretary of State.

5.1.1.3.   Please see Schedule 6 for a list of approved jurisdictions and frameworks.

5.1.2.   Where one of the above cannot be achieved, as the Data Controller is established outside of the jurisdictions or cannot rely upon the frameworks listed within Schedule 6, the transfer shall be made subject to the IDTA.

5.2.   UK International Data Transfer Agreement:

5.2.1.   where the transfer must proceed on the basis of 5.1.2. above, the Data Controller and Data Processor hereby agree to enter into the IDTA. For this purpose the Data Controller shall act as the "Data Importer" and the Data Processor shall act as the "Data Exporter". Within Clause 5.2.1, where Tables 1-4 are referred to, this is with reference to the Tables of the same name within the IDTA. On the basis that the IDTA is incorporated into this DPA:

5.2.1.1.   For the purposes of Table 1, the required details are set out within Schedule 1.

alliants

5.2.1.2.   For the purposes of Table 2:

5.2.1.2.1.   the law of England and Wales shall govern the IDTA and be the primary place for legal claims to be made;

5.2.1.2.2.   the Data Importer and Data Exporter and their statuses are set out within Schedule 1;

5.2.1.2.3.   the "Linked Agreement" is this Data Processing Agreement and shall remain in place for the duration of the SOW between the Data Controller and the Data Processor.

5.2.1.3.   For the purposes of Table 3, the details of the "Transferred Data" are set out in Schedule 2. Additionally, any update to the Linked Agreement shall result in an automatic update to the content of the IDTA.

5.2.1.4.   For the purposes of Table 4, the details of the "Security Requirements" are set out in Schedule 4.

5.2.2.   Relation of the IDTA to this Agreement - nothing in the Agreement shall be construed to prevail over any conflicting clause of the IDTA. For the avoidance of doubt, where this Agreement further specifies audit and Sub-Processor rules, such specifications also apply in relation to the IDTA.

6.   Data Subject Requests, Complaints and Breaches

6.1.   The Data Processor shall assist the Data Controller in complying with its obligations under the UK and EU GDPR. In particular, the following shall apply to data subject requests, complaints, and data breaches.

6.2.   The Data Processor shall notify the Data Controller without undue delay if it receives:

6.2.1.   a request from a data subject to exercise their rights under applicable data protection legislation; or

6.2.2.   any other complaint or request relating to the processing of the Personal Data.

6.3.   The Data Processor shall cooperate fully with the Data Controller and assist as required in relation to any data subject request, complaint, or other request, including by:

6.3.1.   providing the Data Controller with full details of the complaint or request;

6.3.2.   providing the necessary information and assistance in order to comply with a data subject request;

6.3.3.   providing the Data Controller with any Personal Data it holds in relation to a data subject (within the timescales required by the Data Controller); and

6.3.4.   providing the Data Controller with any other information requested by the Data Controller.

alliants

6.4.   The Data Processor shall notify the Data Controller without undue delay if it becomes aware of any form of Personal Data breach, including any unauthorised or unlawful processing, loss of, damage to, or destruction of any of the Personal Data.

7.   Liability and Indemnity

The Data Processor shall indemnify, keep indemnified and defend the Data Controller, at the Data Processor's own expense, against all claims, liabilities, costs, expenses, damages and losses (including all interest, penalties and legal costs (calculated on a full indemnity basis) and all other professional costs and expenses) suffered or incurred by the Data Controller arising out of the failure by the Data Processor or its employees or agents to comply with of its obligations under this Agreement ("Claims"). Each party acknowledges that Claims include any claim or action brought by a Data Subject arising from the Data Processor's breach of its obligations under this Agreement. The Data Controller shall indemnify, keep indemnified and defend the Data Processor, at the Data Controller's own expense, against all claims, liabilities, costs, expenses, damages and losses (including all interest, penalties and legal costs (calculated on a full indemnity basis) and all other professional costs and expenses) suffered or incurred by the Data Processor arising out of the failure by the Data Controller or its employees or agents to comply with of its obligations under this Agreement ("Claims"). Each party acknowledges that Claims include any claim or action brought by a data subject arising from the Data Controller's breach of its obligations under this Agreement.

8.   Intellectual Property Rights

All pre-existing copyright, database rights, and other intellectual property rights subsisting in the Personal Data provided to the Data Processor for processing shall belong to the Data Controller or to any other applicable third party from whom the Data Controller has obtained the Personal Data under licence (including, but not limited to, Data Subjects, where applicable). The Data Processor is licensed to use such Personal Data under such rights only for the purposes of the Services, and in accordance with this Agreement.

9.   Confidentiality

9.1.   The Data Processor shall maintain the Personal Data in confidence, and in particular, unless the Data Controller has given written consent for the Data Processor to do so, the Data Processor shall not disclose any Personal Data supplied to the Data Processor by, for, or on behalf of, the Data Controller to any third party. The Data Processor shall not process or make any use of any Personal Data supplied to it by the Data Controller otherwise than in connection with the provision of the Services to the Data Controller.

9.2.   The Data Processor shall ensure that all personnel who are to access and/or process any of the Personal Data are contractually obliged to keep the Personal Data confidential.

alliants

9.3.   The obligations set out in this Clause 9 shall continue for a period of six years after the cessation of the provision of Services by the Data Processor to the Data Controller.

9.4.   Nothing in this Agreement shall prevent either Party from complying with any requirement to disclose Personal Data where such disclosure is required by law. In such cases, the Party required to disclose shall notify the other Party of the disclosure requirements prior to disclosure, unless such notification is prohibited by law.

10.   Appointment of Sub-Processors

10.1.   The Data Controller authorises the Data Processor to appoint Sub-Processors in connection with the provision of the Services under this Agreement. The Data Processor has currently engaged the Sub-Processors listed within Schedule 3 of this Agreement.

10.2.   If the Data Processor intends to instruct Sub-Processors other than the companies listed in Schedule 3, the Data Processor will notify the Data Controller in writing and will give the Data Controller the opportunity to object to the engagement of the new Sub-Processors within 30 days after being notified. The objection must be based on reasonable grounds (e.g. if the Data Controller proves that significant risks for the protection of its Personal Data exist with the appointment of that Sub-Processor). If the Data Processor and the Data Controller are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party. The Data Controller shall receive a refund of any prepaid but unused fees for the period following the effective date of termination.

10.3.   Where the Data Processor engages Sub-Processors, the Data Processor will enter into a contract that imposes on the Sub-Processors the same obligations that apply to the Data Processor under this Agreement. Where a Sub-Processor fails to fulfil its data protection obligations, the Data Processor will remain liable to the Data Controller for the performance of such Sub-Processors obligations.

10.4.   Where a Sub-Processor is engaged, the Data Controller must be granted the right to monitor and inspect the Sub-Processor's activities in accordance with this Agreement and the UK and EU GDPR, including to obtain information from the Data Processor, upon written request, on the substance of the contract and the implementation of the data protection obligations under the Sub-Processor's contract, where necessary by inspecting the relevant contract documents.

10.5.   The provisions of this Clause 10 shall mutually apply if the Data Processor engages a Sub-Processor in a country outside the UK or the EEA that is not recognised as providing an adequate level of protection for Personal Data under the Data Privacy Laws. If, in the performance of this Agreement, the Data Processor transfers any Personal Data to a Sub-Processor located outside of the UK or the EEA, the Data Processor shall, in advance of any such transfer, ensure that a legal mechanism to achieve adequacy under the Data Privacy Laws is in place in respect of that processing.

alliants

11. Deletion and/or Disposal of Personal Data

11.1. The Data Processor shall, at the written request of the Data Controller, delete (or otherwise dispose of) the Personal Data or return it to the Data Controller in the format(s) reasonably requested by the Data Controller within a reasonable time after the earlier of the following:

11.1.1. the end of the provision of the Services; or

11.1.2. the processing of that Personal Data by the Data Processor is no longer required for the performance of the Data Processor's obligations under this Agreement or the SOW.

11.2. Following the deletion, disposal, or return of the Personal Data under sub-Clause 11.1, the Data Processor shall delete (or otherwise dispose of) all further copies of the Personal Data that it holds, unless retention of such copies is required by law, in which case the Data Processor shall inform the Data Controller of such requirement(s) in writing.

11.3. The processing of anonymised data shall be conducted in accordance with the Alliants Terms and Conditions (Clause 6).

12. Law and Jurisdiction

12.1. This Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall be governed by, and construed in accordance with, the laws of England and Wales.

12.2. Any dispute, controversy, proceedings or claim between the Parties relating to this Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of England and Wales.

alliants

SCHEDULE 1

Data Controller:

- **Name: The Customer, as defined in the Alliants Statement of Work**
- **Address: The Customer's address, as set out in the Alliants Statement of Work**
- **Contact person's name, position and contact details: the duly authorised representative as set out in the Alliants Order Form**
- **(and where relevant, the Data Importer)**

Data Processor:

- **Name: Alliants Limited**
- **Registered Address: Fleming Court, Leigh Road, Eastleigh, Southampton, Hampshire, SO50 9PD, United Kingdom.**
- **Office Address: Premier Universal Marina, Southampton, Hampshire, SO31 7ZN, United Kingdom**
- **Contact person's name, position and contact details: Data Protection Officer**
- **(and where relevant, the Data Exporter)**

alliants

SCHEDULE 2

Subject matter of the Processing, duration of the Processing, the nature and purpose of the Processing, the type of Personal Data, the categories of Data Subjects and the arrangements for the destruction of the Personal Data upon termination of the SOW.

Alliants Experience Platform (AXP)

Description	Details
Subject matter of the processing	This is set out in the relevant SOW.
Duration of the processing	For the Period of Service related to the SOW
Nature and purposes of the processing	To enable users of the AXP platform to interact with each other. For example, the employees of the Data Controller can communicate with the Data Controller's customers by exchanging messages with them on the AXP platform.
Type of Personal Data	The following Personal Data relating to the Data Controller's employees: ● Name, work address, work email address, work phone number, job title, work profile picture and, in some cases, another type of unique identifier The following Personal Data relating to the Data Controller's customers: ● Profile information, such as name, email address, phone numbers, mailing address, date of birth, job title, company and in some cases other types of information ● Reservation information, such as confirmation number, room number, arrival date and departure date, rate information and in some cases other types of information ● Request Information such as booking reference, confirmation number, request date, billing information and in some cases other types of information ● Payment data, payment token, billing address, card holder name, email address, phone number and in some cases other types of information ● Electronic messages including message user identifier, date sent, to, from, time, subject, which may include Personal Data.

alliants

	• Conversation Data ie: Personal Data contained within electronic conversations within the AXP Platform.
Categories of Data Subject	Employees, freelancers and contractors of the Controller. Customer users, affiliates and other participants from time to time to whom the Controller has granted the right to access the Services in accordance with the terms of the Agreement. Clients of the Controller and individuals with whom those End Users communicate with by email and/or other messaging media. Employees of clients of the Controller. Suppliers and service providers of the Controller. Other individuals to the extent identifiable in the content of emails or their attachments or in archiving content.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under applicable law to preserve that type of data	The Personal Data will only be held for the duration of the SOW. Upon termination of the SOW the Personal Data will be destroyed by the Data Processor within thirty (30) calendar days of the effective date of termination.

alliants

SCHEDULE 3

Further information regarding sub-processors and 3rd Party Integrations is available from our "Alliants Experience Platform - Sub-Processors and Third Party Integrations" documentation.

Whenever we transfer Personal Data outside the UK, we ensure a similar level of protection is afforded to it by conducting thorough due diligence on our sub-processors to ensure at least one of the following safeguards is in place:

1) the Sub-Processor is based in a country that has been granted an adequacy regulation by the UK Secretary of State confirming that the country in question provides an adequate level of protection for personal data (which include transfers from the UK to the US under the protection of the Data Privacy Framework, where the US companies have certified to this standard);

   or

2. we enter into either International Data Transfer Agreements or Standard Contractual Clauses (with the UK Addendum) with the Sub-Processor and ensure that supplementary measures are also applied, where necessary.

List of Approved Sub-Processors - Infrastructure

Entity name	Entity type	Entity country	Data centre (Region)	Transfer mechanism
Amazon Web Services EMEA SARL (AWS Europe)	Hosting Provider	Luxembourg	Ireland (EU)	Adequacy Regulation

List of Approved Sub-Processors – AXP Product

Entity name	Purpose	Mandatory / Optional	Entity country	Data Processing country	Personal Data	Transfer mechanism
Google LLC	Website Analytics	Mandatory	USA - California	USA	IP address	Data Privacy Framework
Google LLC	Google Cloud Platform APIs for Translations and Maps	Mandatory	USA - California	USA / EU	Conversational data, postal addresses	Data Privacy Framework

alliants

Intercom	Digital Adoption Platform	Mandatory	USA-California	USA	Property staff name	Data Privacy Framework
Looker (Part of Google LLC)	Business Intelligence Reporting and Analytics	Mandatory	USA - California	Ireland (EU)	Conversational data, property information (including staff name)	Adequacy Regulation
Mailgun Technologies , Inc.	User facing transactional (login, forgot password, escalation, etc.) emails	Mandatory	USA - Texas	EU	Customer email address	Adequacy Regulation
QR Planet (formerly qrd°by)	QR code generation	Mandatory	Austria (EU)	EU	None (UID generated)	Adequacy Regulation
Pusher Limited	Desktop application notifications	Mandatory	UK	EU	None (UID generated)	Adequacy Regulation
One Signal	Mobile application notifications	Mandatory	USA - California	USA	None (UID generated)	UK International Data Transfer Agreement
Sendgrid	Email Delivery	Optional	USA - California	USA	Customer email address	Data Privacy Framework
IXOPay (formerly TokenEx)	Payment details handler	Optional	Ireland (EU)	USA - Oklahoma	None (UID generated)	UK Addendum + EU Standard Contractual Clauses
OpenAI	AI-Powered Functionality	Optional	USA - California	USA	Conversational data	UK Addendum + EU Standard Contractual Clauses
Salesforce	Sales and project information	Mandatory	USA - California	UK	Corporate Staff information	N/A

alliants

					(name, email address)	
Zendesk Sunshine Conversations (formerly Smooch.io)	Unified Messaging API	Mandatory	USA - California	USA - Oregon	Conversational data	Data Privacy Framework
Airbyte	Data integration & replication platform	Mandatory	USA - California	USA	None (transit layer only)	UK Addendum + EU Standard Contractual Clauses
Databricks	Data analysis platform	Mandatory	USA - California	EU	Anonymised data only	Adequacy Regulation
Datadog Inc.	Application and service monitoring	Mandatory	USA - New York	USA	None	Data Privacy Framework
Mixpanel	Product usage analysis	Mandatory	USA - California	USA	IP Address	Data Privacy Framework
Rudderstack	Customer data platform	Mandatory	USA - California	EU	Anonymised data only	Adequacy Regulation

alliants

SCHEDULE 4

Technical and organisational measures to ensure the security of Personal Data

1. 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 risks to Data Subjects, the Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The Data Processor shall implement the following, as appropriate:

    a. the pseudonymisation and encryption of the Shared Personal Data;

    b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

    c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

    d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Further information about our Information Security and Data Protection resources can be found at the Alliants Trust Centre.

4. As a minimum, the Data Processor shall implement the items set out below.

Organisational Measures

-   The Data Processor will maintain their Information Security Management System (ISMS) to the standard required by ISO/IEC 27001:2022 and as certified by number IS 726570.

-   The Data Processor shall implement the following policies:

    ○   Data Subjects Rights Procedure - Controller & Processor

    ○   Personal Data Breach Policy and Procedure - Controller & Processor

    ○   ISMS Data Protection Policy

    ○   ISMS Information Security Policy

    ○   ISMS Asset Management Policy

    ○   ISMS Clear Desk and Screen Policy

    ○   ISMS Patch Management Policy

alliants

    ○   ISMS Media Handling and Disposal Policy

    ○   ISMS Vulnerability Management Policy

    ○   ISMS Password Management Policy

    ○   ISMS Business Continuity Policy

    ○   ISMS Access Control Policy

    ○   ISMS Backup and Restore Policy

    ○   ISMS Cryptography Policy

    ○   ISMS Mobile Devices Policy

    ○   ISMS Acceptable Use Policy

    ○   ISMS Physical Security Policy

The Data Processor shall ensure that all personnel that process and/or have access to Personal Data have data protection awareness training upon induction and regular refresher training thereafter. This includes:

- **Physical Security**
  Implement physical security controls to prevent unauthorised access to personal data and information systems used to process personal data.

- **Human Resources Security**
  Requiring all staff with access to personal data to be subject to obligations of confidentiality and having a disciplinary process in place to manage breaches of confidentiality or non-compliance with information security or data protection policies.

- **Incident Management**
  Implement information security incident management procedures.

Technical Measures

The Data Processor shall implement the following measures, as appropriate:

- **Access Control**
  The principle of least privilege shall be applied as well as access control based on role-based access. Defined user access management process with ongoing auditing of user access permissions. Restricted privileged and administrative access based on need-to-know, with ongoing auditing of user access permissions.

- **Identification & Authentication**
  Identity and access management controls shall be implemented to ensure only uniquely identified, authorised and authenticated users are granted access to systems processing personal data.

- **Data Security**

alliants

Data classification and labelling shall be implemented, as well as encryption of data at rest and in transit and centralised key management including rotation.

- **Technical Security**
  Secure configuration standards and builds shall be used, as well as network perimeter security controls and anti-malware software deployed on all computers. Firewalls shall be used and vulnerability scanning shall be conducted on a regular basis.

- **Independent Assurance**
  Third party assurance reviews shall be obtained, including penetration testing of appropriate information systems at least annually.

SCHEDULE 5

International Data Transfer Agreement, Alternative Part 4 Mandatory Clauses:

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.

alliants

SCHEDULE 6

List of approved jurisdictions

Jurisdiction name	How is the transfer to the jurisdiction approved?
Andorra	Adequacy regulation
Argentina	Adequacy regulation
Faroe Islands	Adequacy regulation
Gibraltar	Adequacy regulation
Guernsey	Adequacy regulation
Isle of Man	Adequacy regulation
Israel	Adequacy regulation
Jersey	Adequacy regulation
New Zealand	Adequacy regulation
Switzerland	Adequacy regulation
The Republic of Korea	Adequacy regulation
Uruguay	Adequacy regulation
Canada	Adequacy regulation (partial, only covers data subject to Canada's Personal Information and Electronic Documents Act)
Japan	Adequacy regulation (partial, only covers data transferred to private sector organisations subject to Japan's Act of the Protection of Personal Information)
The United States of America	Adequacy regulation (framework, only covers data which is transferred under the UK Extension to the EU-US Data Privacy Framework)

For the avoidance of doubt, the EU member states are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

The EFTA states are Iceland, Norway and Liechtenstein.

alliants