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

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

This is our standard Data Processing Agreement, which can be amended to suit.

# Data Processing Agreement

**THIS AGREEMENT** is made the [ ] day of [insert month] [insert year]

**BETWEEN:**

1) [Insert name and address of controller client ], and the entities listed in Schedule 1 ("Data Controller") and

2) Alliants Limited, a company registered in England under number 6868886, whose registered office is at Fryern House, 125 Winchester Road, Chandlers Ford SO53 2DR ("Data Processor")

**This Data Processing Agreement includes:**

1) Details of the Data Controllers that are party to this agreement, attached hereto at Schedule 1.
2) Details of our services, attached hereto at Schedule 2.
3) 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 Service Agreement, attached hereto at Schedule 3.
4) List of approved Sub-Processors, attached hereto at Schedule 4.
5) List of Technical and organisational measures to ensure the security of Personal Data, attached hereto at Schedule 5.

**WHEREAS:**

1) Under an agreement between the Data Controller and the Data Processor dated [insert the date of the service agreement here] ("the Service Agreement") the Data Processor provides to the Data Controller the Services described in Schedule 2.
2) The provision of the Services by the Data Processor involves processing the Personal Data described in Schedule 3 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 between the Data Controller and any organisation which processes Personal Data on its behalf governing the processing of that 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:

| | |
|---|---|
| **"Data Privacy Laws"** | means (i) the EU GDPR (ii) the UK Data Protection Laws; |
| **"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; |
| **"IDT Addendum"** | means International Data Transfer Addendum to the EU Commission Standard Contractual Clauses VERSION B1.0, in force 21 March 2-22, issued by the Information Commissioner's Office; |
| **"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 3; |
| **"Services"** | means those services described in Schedule 2 which are provided by the Data Processor to the Data Controller and which the Data Controller uses for the purposes described in Schedule 2; |
| **"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; |
| **"Sub-Processor"** | means a sub-processor appointed by the Data Processor to process the Personal Data; |
| **"Sub-Processing Agreement"** | means an agreement between the Data Processor and a Sub-Processor governing the Personal Data processing carried out by the Sub-Processor, as described in Clause 9; |
| **"SOW"** | Statement of Work; |
| **"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. |

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 3, 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.

2.2. The provisions of this Agreement supersede any other arrangement, understanding, or agreement including, but not limited to, the Service Agreement 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 8.

## 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 that, in connection with the performance of the services under the Service Agreement, Personal Data will be transferred from the Data Processor to the Data Controller.

4.3. The Data Controller acknowledges and agrees that the Standard Contractual Clauses, together with supplementary measures, where necessary, will apply with respect to Personal Data that is transferred outside the EEA, either directly or via onward transfer, to the Data Controller and to any country not recognised by the EU as providing an adequate level of protection for Personal Data (as described in the EU GDPR).

4.4. The Data Controller acknowledges and agrees that either the IDTA or the Standard Contractual Clauses and the ADT Addendum (whichever is appropriate), together with supplementary measures, where necessary, will apply with respect to Personal Data that is transferred outside the UK, either directly or via onward transfer, to the Data Controller and to any country not recognised by the UK as providing an adequate level of protection for Personal Data (as described in the UK GDPR).

4.5. 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.

4.6. 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.

4.7. 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.

4.8. 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.

4.9. 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 conduct of data protection impact assessments, and in dealings with the ICO or other relevant Supervisory Authority.

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

4.10.1. 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 9;

4.10.2. 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);

4.10.3. 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 5 and shall inform the Data Controller in advance of any changes to such measures:

4.10.4. 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;

4.10.5. 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;

4.10.6. 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;

4.10.7. 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

4.10.8. inform the Data Controller immediately if it is asked to do anything that infringes the UK and EU GDPR or any other applicable data protection legislation.

## 5. Data Subject Access, Complaints and Breaches

5.1. 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 access requests, complaints, and data breaches.

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

5.2.1. a subject access request from a data subject; or

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

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

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

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

5.3.3. 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

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

5.4. The Data Processor shall notify the Data Controller immediately 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.

## 6. 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.

## 7. 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.

## 8. Confidentiality

8.1. 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.

8.2. 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.

8.3. The obligations set out in this Clause 8 shall continue for a period of six years after the cessation of the provision of Services by the Data Processor to the Data Controller.

8.4. 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.

## 9. Appointment of Sub-Processors

9.1. The Data Processor shall be entitled to engage Sub-Processors to fulfil its obligations defined in this Agreement only with the Data Controller's written consent. For these

purposes, the Data Controller consents to the engagement as Sub-Processors the third parties listed in Schedule 4.

9.2. If the Data Processor intends to instruct Sub-Processors other than the companies listed in Schedule 4, 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 at the 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.

9.3. Where the Data Processor engages Sub-Processors, the Data Processor will enter into a contract with the Sub-Processors 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.

9.4. Where a Sub-Processor is engaged, 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-Processing contract, where necessary by inspecting the relevant contract documents.

9.5. The provisions of this section 9 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.

## 10. Deletion and/or Disposal of Personal Data

10.1. 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:

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

10.1.2. 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 Service Agreement.

10.2. Following the deletion, disposal, or return of the Personal Data under sub-Clause 10.1, 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. Law and Jurisdiction

11.1. 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.

11.2. 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.

SIGNED for and on behalf of the Data Controller:

AUTHORISED SIGNATURE

Name: _____

Title: _____

Date signed: _____

SIGNED for and on behalf of the Data Processor:

AUTHORISED SIGNATURE

Name: _____

Title: _____

Date signed: _____

# SCHEDULE 1

| Company Name | Registered Office Address | Registration Number | Point of Contact |
|---|---|---|---|
| | | | [name], [position], [email address], [telephone number]. |
| | | | [name], [position], [email address], [telephone number]. |
| | | | [name], [position], [email address], [telephone number]. |
| | | | [name], [position], [email address], [telephone number]. |

# SCHEDULE 2

**Services, as per the Service Agreement**

## Alliants AXP Product

Provision of the AXP product to include:

- Core Platform
    - Concierge Module
    - Workflow and Automation
    - Staff App
    - Insights
    - Integrations
- Messaging
- Guest App
- Mobile Key
- Digital Wallet
- Transactional Email

## Alliants Support

Provision of support including:

- Ticket investigation, escalation, and resolution
- Monitoring and alerting of infrastructure and applications
- Management of bug fixes, releases, vulnerabilities
- Automation and Documentation of support processes
- Information Security and Data Protection

# SCHEDULE 3

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 Service Agreement.

## AXP Product

| Description | Details |
|---|---|
| Subject matter of the processing | This is set out in Schedule 2 above. |
| Duration of the processing | For the duration of the Service Agreement |
| 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:<br>• Name, work address, work email address, work phone number, job title, work profile picture and, in some cases, another type of unique identifier<br>The following Personal Data relating to the Data Controller's customers:<br>• 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<br>• Reservation information, such as confirmation number, room number, arrival date and departure date, rate information and in some cases other types of information<br>• Request Information such as booking reference, confirmation number, request date, billing information and in some cases other types of information<br>• Payment data, payment token, billing address, card holder name, email address, phone number and in some cases other types of information<br>• Electronic messages including message user identifier, date sent, to, from, time, subject, which may include Personal Data. |

| | |
|---|---|
| | • Conversation Data ie: Personal Data contained within electronic conversations within the AXP Platform. |
| Categories of Data Subject | Employees, freelancers and contractors of the Controller.<br><br>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.<br><br>Clients of the Controller and individuals with whom those End Users communicate with by email and/or other messaging media.<br><br>Employees of clients of the Controller.<br><br>Suppliers and service providers of the Controller.<br><br>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 Service Agreement. Upon termination of the Service Agreement the Personal Data will be destroyed by the Data Processor within thirty (30) calendar days of the effective date of termination. |

## Support

| Description | Details |
|---|---|
| Subject matter of the processing | This is set out in Schedule 2 above. |
| Duration of the processing | For the duration of the Service Agreement. |
| Nature and purposes of the processing | To provide support to the Data Controller in relation to the function and operation of the AXP Product or other Alliants Services designed and built by the Data Processor for the Data Controller and to assist with resolving any issues or queries. |
| Type of Personal Data | The following Personal Data relating to the Data Controller's employees:<br><br>• Name, email signature (which may contain, for example, work address, work phone number, job title, work profile picture), escalation details, and, in some cases, another type of unique identifier<br><br>The following Personal Data relating to the Data Controller's customers: |

| | |
|---|---|
| | As detailed in types of personal data in Schedule 2 for AXP Product, Alliants Services and Support. |
| Categories of Data Subject | • Employees of the Data Controller<br>• Customers of the Data Controller |
| 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 processed for as long as is necessary to provide the service described above. Upon termination of the Service Agreement the Personal Data will be destroyed by the Data Processor within thirty (30) calendar days of the effective date of termination. |

# SCHEDULE 4

## List of Approved Sub-Processors - AXP Product

| Entity name | Entity type | Entity country | Data centre (Region) |
|---|---|---|---|
| Amazon Web Services EMEA SARL (AWS Europe) | Hosting and Storage Provider | Luxembourg | Ireland (EU) |
| Automattic | Alliants online user training platform (Hosting) | USA - California | Ireland (EU) |
| Zendesk Sunshine Conversations (Formerly Smooch.io) | Unified Messaging API | USA - California | USA |
| Microsoft Corporation | PowerBI - Business Intelligence Reporting and Analytics | USA - Washington | UK |
| Mailgun Technologies, Inc. | User facing transactional (login, forgot password, escalation, etc.) emails | USA - Texas | EU |
| Google LLC | Website Analytics | USA - California | USA |
| qrd°by | QR code generation | Austria (EU) | EU |
| Pusher Limited | Desktop application notifications | UK | EU |
| One Signal | Mobile application notifications | USA - California | USA |
| WalkMe | Digital adoption platform (in application training, insights, engagement, etc.) | USA - California | EU |
| Sendgrid | Email Delivery | USA - California | USA |

## List of Approved Sub-Processors - Support

| Entity name | Entity type | Entity country | Data centre (Region) |
|---|---|---|---|
| Datadog Inc. | Application and Service monitoring | USA - California | USA |
| Freshworks Inc. | Service desk & support ticketing software | USA - California | EEA |
| Salesforce | Sales and project information | USA - California | UK |

# SCHEDULE 5

## 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. 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 27001:2013 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
    - 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:

The following are examples. Please add/amend/delete 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**

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.