Asset Investment Manager

RM1557.15 G-Cloud 15 Supplier Terms

Date: January 29, 2026

Document Version: AIM-GCLOUD-TERMS-2026-01-29

Probit Ltd. is registered at 4 Chestnut Court, Parc Menai, Bangor, Gwynedd LL57 4FH, United Kingdom and incorporated in England & Wales under company number 07228092 ("**Probit**", "**Company**").

IT IS AGREED BETWEEN THE PARTIES THAT:

1. RM1557.15 Call-Off Contract Alignment

1.1 In these Supplier Terms:

"**Call-Off Contract**"	means the contract formed under RM1557.15 between the Supplier and the Buyer for the supply of the Services, comprising the Order and any schedules, attachments and other documents incorporated into it under RM1557.15.
"**Order**"	means the Call-Off order form (or equivalent) agreed under RM1557.15 that incorporates these Supplier Terms.
"**Services**"	has the meaning given in the Call-Off Contract (and is the services described in the Supplier Service Descriptions and ordered under the Order).

1.2 These Supplier Terms are incorporated into the Call-Off Contract in accordance with Framework Schedule 6 (Order Form). In the event of any conflict between these Supplier Terms and the Core Terms, Order Form, or Framework Special Terms, the order of precedence set out in the Call-Off Contract shall apply.

1.3 These Supplier Terms are limited to operational terms for the use of the Services (including User Subscriptions, Acceptable Use, and technical preconditions). Nothing in these Supplier Terms is intended to contradict or vary the Core Terms relating to liability, indemnities, or the Buyer's termination rights. In the event of any unintended conflict, the Core Terms and Order Form shall prevail.

1.4 Charges (including Tier fees and add-ons) and service limits are as set out in the Order and Call-Off Schedule 5 (Pricing Details). Nothing in these Supplier Terms varies or supplements the pricing and charging provisions of the Call-Off Contract.

1.5 Any service levels, targets and Service Credits described in the SLA are without prejudice to the Buyer's rights and remedies under the Call-Off Contract.

2. Definitions

2.1 All capitalised terms used in these Supplier Terms have the meaning given to them in these Supplier Terms, unless defined otherwise in the Call-Off Contract.

"**Probit**"	means the owner and licensor of the Software, Probit Ltd., a company incorporated in England & Wales under company number 07228092.
"**AUP**"	means the acceptable use policy in Schedule 3.

"**Authorised User**"	means an employee, agent or independent contractor of the Buyer who is authorised by the Buyer to use the Services and the Documentation.
"**Buyer Data**"	means all data inputted into the Services by the Buyer or Authorised Users, or on the Buyer's behalf, for the purpose of using the Services or facilitating the Buyer's use of the Services, including Government Data (as defined in the Call-Off Contract), where applicable.
"**Documentation**"	means the user document(s) and other materials made available by the Supplier to the Buyer which describe the Services and provide instructions for use.
"**DPA**"	means the Data Processing Agreement in Schedule 2.
"**Feedback**"	means any feedback, innovations or suggestions, requests for changes to functionality or improvements in each case created by the Buyer or Authorised Users regarding the attributes, performance or features of the Services or Software.
"**SLA**"	means the service level agreement in Schedule 1.
"**Software**"	means the software components of the Services.
"**Supplier**"	means Probit.
"**User Subscriptions**"	means the user licences purchased under the Call-Off Contract which entitle Authorised Users to access and use the Services and Documentation in accordance with the Call-Off Contract and these Supplier Terms.

3. Liability

3.1 Liability is governed exclusively by the RM1557.15 Call-Off Contract.

4. Licence and Use of the Services

4.1 The Supplier grants the Buyer a non-exclusive, non-transferable right for Authorised Users to access and use the Services and the Documentation during the term of the Call-Off Contract solely for the Buyer's internal business operations.

4.2 Access to and use of the Services is limited to the User Subscriptions purchased under the Order and is subject to the service limits set out in the Order and Call-Off Schedule 5 (Pricing Details).

4.3 The Buyer shall ensure that Authorised Users use the Services and the Documentation in accordance with the Call-Off Contract and these Supplier Terms, including the AUP.

4.4 The Buyer shall not, and shall ensure that Authorised Users do not:

a) copy, modify, duplicate, create derivative works from, frame, mirror, republish, down-

load, display, transmit, or distribute all or any portion of the Software or Documentation except as expressly permitted by the Call-Off Contract;

b) attempt to de-compile, reverse compile, disassemble, or reverse engineer all or any part of the Software; or

c) access the Services and Documentation in order to build a product or service which competes with the Services.

4.5 The Supplier retains all intellectual property rights in and to the Services, the Software, the Documentation and any Supplier materials (including any improvements or updates made generally available as part of the Services).

4.6 The Buyer retains all right, title and interest in and to Buyer Data (including Government Data, as defined in the Call-Off Contract), and nothing in these Supplier Terms transfers ownership of Buyer Data to the Supplier.

4.7 The Buyer grants the Supplier a non-exclusive, worldwide, perpetual, royalty-free licence to use Feedback for the purpose of maintaining, supporting and improving the Services, provided that the Supplier does not incorporate any Buyer Data into the Services as a result of such Feedback.

5. Documentation

5.1 The Supplier may provide and update Documentation from time to time to reflect changes in functionality, security practices and operational procedures. Updated Documentation may be made available within the Services or otherwise provided to the Buyer.

5.2 Documentation forms part of the operational instructions for use of the Services. The Buyer shall use, and shall ensure Authorised Users use, the Services in accordance with the Documentation (subject to the Call-Off Contract).

6. Service updates and maintenance

6.1 The Supplier may implement updates and releases to the Services from time to time.

6.2 Planned and emergency maintenance are managed in accordance with the SLA.

6.3 **AIM API Sandbox (where enabled):** The Supplier may reset the AIM API Sandbox environment (including deletion of sandbox data) to support stability, security and maintenance. Where practicable, the Supplier will provide at least two (2) Working Days' notice of planned resets.

6.4 For the avoidance of doubt, any notice of Service Modifications or modifications to Supplier Service Specific Terms will be provided in accordance with the Call-Off Contract and the notice provisions completed in the Order.

7. Account administration and access

7.1 The Buyer is responsible for:

a) managing its Authorised Users, including ensuring that only permitted users are granted access and that access is removed promptly when no longer required; and

b) ensuring that Authorised Users keep credentials confidential and do not share accounts.

7.2 The Buyer shall promptly notify the Supplier if it becomes aware of any unauthorised access to the Buyer's user accounts or credentials.

7.3 **API fair use:** Use of any AIM API integration is subject to fair usage limits to ensure service stability. The Supplier may apply reasonable rate limiting (including throttling requests that exceed 300 requests per minute) where necessary to protect the Services or the integrity and availability of the Services for the Buyer and other users. Where practicable, the Supplier will notify the Buyer of material rate limiting and work with the Buyer to address the underlying cause (for example batching, scheduling, caching or optimisation of integration behaviour).

8. Acceptable Use enforcement

8.1 The Supplier may monitor use of the Services to confirm compliance with the AUP and to protect the Services and the Supplier's systems and networks.

8.2 Where the Supplier reasonably believes that the AUP has been breached, the Supplier will notify the Buyer and request remediation.

8.3 Any restriction or suspension of access to the Services will occur only to the extent expressly permitted under the Call-Off Contract and/or required to address an immediate and material security risk.

9. Use of Supplier marks

9.1 The Buyer may use the Supplier's name and marks only as necessary to access and use the Services in accordance with the Call-Off Contract. Any other use (including publication, marketing or press activity) requires the Supplier's prior written consent.

10. Third party components

10.1 The Services may incorporate or depend on third party software and services (including open source components) as part of normal operation.

10.2 Where the Supplier is required to provide third party notices or attributions, these will be made available in the Services or on request. Any such notices are provided for information and do not amend the Call-Off Contract.

11. Decision support outputs

11.1 AIM is a decision-support service. Outputs are generated based on the Buyer's configuration, assumptions and inputs (including Buyer Data) and are intended to support governance and planning.

11.2 The Buyer remains responsible for its asset management decisions, including review and approval of assumptions, outputs and investment programmes, and for ensuring that use of outputs is appropriate to its circumstances and governance.

12. Beta and pre-release features

12.1 The Supplier may make beta, preview or pre-release features available from time to time ("**Beta Features**"). Beta Features are optional, may be withdrawn or changed at any time, and are provided on an "as-is" basis for evaluation purposes.

12.2 Beta Features may not be fully tested and are not intended for critical production workloads. Beta Features will not form part of the Supplier SLA unless expressly included in the Order, and no service levels, targets or Service Credits apply to Beta Features unless expressly set out in the Call-Off Contract.

12.3 Nothing in this section is intended to, or shall, limit or exclude any rights or remedies the Buyer has under the Call-Off Contract.

13. Data Protection

13.1 To the extent the Supplier processes personal data on behalf of the Buyer in connection with the Services under the Call-Off Contract, the parties shall comply with the DPA and the Call-Off Contract.

Schedule 1

Service Level Agreement

This Service Level Agreement ("**SLA**") sets out service level commitments for the Services.

1. Definitions

1.1 All capitalised terms used in this SLA shall have the meaning given to them in the Call-Off Contract unless defined otherwise below.

"**Available**"	means the Services are operable and accessible by Authorised Users.
"**Availability**"	means, for a given measurement period (e.g. a calendar month), the percentage of total time during which the Services are Available, excluding Excused Downtime.
"**Downtime**"	The total number of minutes during a calendar month when the Services is not Available to the Buyer, excluding Excused Downtime.
"**Emergency Maintenance**"	Unplanned maintenance required to address critical security vulnerabilities or system failures, notified as soon as reasonably practicable.
"**Excused Downtime**"	Time the Services is not Available due to: a) Scheduled Maintenance; b) Emergency Maintenance; c) Force Majeure Events; d) failures or delays caused by the Buyer, its Authorised Users, or its systems/connectivity; e) failures of the internet, public telecommunications networks, or other third-party utility providers not under Supplier's direct contract or control; f) a restriction or suspension expressly permitted by the Call-Off Contract and implemented in accordance with the Call-Off Contract (including any required notice or process), or required to mitigate an immediate and material security risk.
"**Incident**"	means an event which is not part of the standard operation of the Services and which causes, or may cause, an interruption to, or a reduction in, the quality of the Services.
"**Incident Priority Levels**"	Defined classifications for Incidents based on impact:

a) **Priority 1 (P1 - Critical)**: Complete Services unavailability or failure of a critical function affecting all or a significant majority of users, with no workaround available.

b) **Priority 2 (P2 - High)**: Significant degradation of Services performance or failure of a key function impacting core business operations for multiple users, where a reasonable workaround may not be feasible, or unavailable.

c) **Priority 3 (P3 - Medium)**: Partial disruption of non-critical functions, or issues affecting a limited number of users, with a workaround potentially available. Includes general usage queries.

d) **Priority 4 (P4 - Low)**: Minor functional issues with minimal business impact, informational requests, or cosmetic errors.

"**Monthly Uptime Percentage**"	Calculated as: ((Total Minutes in Calendar Month - Downtime Minutes) / Total Minutes in Calendar Month) * 100%.
"**Normal Business Hours**"	means 9.00 am to 5.00 pm local UK time, on each Working Day.
"**Scheduled Maintenance**"	Planned maintenance windows announced by Supplier at least two (2) Working Days in advance, typically conducted outside of Normal Business Hours.
"**Service Credit**"	means a credit, calculated as set out in clause 3 of this SLA, applicable if the Monthly Uptime Percentage falls below the Uptime Commitment in clause 2. The mechanism for claiming and receiving Service Credits is described in clause 3.
"**Workaround**"	means a method, configuration change, or alternative solution provided by Supplierto restore the availability or functionality of the Services, or to mitigate the impact of an Incident. For the avoidance of doubt, a Workaround may serve as a permanent Resolution to an Incident.

2. Services Availability Commitment

2.1 Supplier commits to achieving a Monthly Uptime Percentage of at least 99.5% for the Services provided to the Buyer.

2.2 The Monthly Uptime Percentage is calculated per calendar month using monitoring data collected by Supplier for the Services provided to the Buyer.

2.3 Downtime minutes resulting from Excused Downtime are excluded from the Monthly Uptime Percentage calculation.

3. Service Credits

3.1 Supplier commits to monitoring Availability of the Services. Following the end of each calendar month, Supplier shall calculate the Monthly Uptime Percentage for that month. Reports detailing monthly performance will typically be made available via email notification.

3.2 If the calculated Monthly Uptime Percentage for a given calendar month falls below the 99.5% commitment, eligibility for a Service Credit arises, subject to the terms herein and the Order.

3.3 Where eligibility arises, Service Credits will be calculated based on the following percentages applied to the Charges paid or payable by the Buyer under the Order for the Services for the affected month.

i) Less than 99.5% but greater than or equal to 99.0%: 5% Service Credit Value

ii) Less than 99.0% but greater than or equal to 97.5%: 10% Service Credit Value

iii) Less than 97.5% but greater than or equal to 90.0%: 25% Service Credit Value

iv) Less than 90.0%: 50% Service Credit Value

3.4 The maximum total Service Credit value that can be accrued in any single calendar month is 50% of the Charges paid or payable by the Buyer under the Order for the Services for the affected month.

3.5 If eligibility for a Service Credit arises under clause 3.2, the Buyer's entitlement to receive such credits, and the process for claiming them, is governed by the terms of the Order.

3.6 Service Credits apply in accordance with this SLA and are without prejudice to the Buyer's rights and remedies under the Call-Off Contract.

4. SLA Exclusions

4.1 This SLA (including the Uptime Commitment and Response Time Targets) does not apply to any performance or availability issues:

i) Caused by factors defined under Excused Downtime (including Scheduled Maintenance, Emergency Maintenance, Force Majeure).

ii) Resulting from any actions or inactions of the Buyer or its Authorised Users (e.g., misuse, configuration errors, failure to follow documentation).

iii) Resulting from Buyer's equipment, software, network connections, or other infrastructure not provided by Supplier.

iv) Related to third-party software, services, or integrations not supplied by Supplier as part of the core Services (including but not limited to Buyer-side integrations, identity providers, or external API connections).

v) Occurring during Free Trial periods or for beta/pre-release features.

vi) Resulting from a restriction or suspension expressly permitted by the Call-Off Contract and implemented in accordance with the Call-Off Contract (including any required notice or process), or required to mitigate an immediate and material security risk.

5. Support Services

5.1 **Requesting support:** The Buyer's Authorised Representative(s) may request support (including reporting Incidents) by email at `support@probit.io`. The Buyer may nominate up to three (3) Authorised Representatives for this purpose (as set out in the Order or otherwise notified to Supplier in writing).

5.2 **Support Hours:** Standard support is available during Normal Business Hours. Support requests logged outside these hours will typically be actioned on the next Working Day.

5.3 **Information to include:** To help triage and resolve a request, the Buyer should (where applicable) provide a clear description of the issue, time of occurrence, affected users, environment/context, steps to reproduce, screenshots/log extracts (where available) and the impact on the Buyer.

5.4 **Incident prioritisation:** Supplier will classify Incidents based on the Incident Priority Levels. Supplier may reasonably re-classify the priority level based on its assessment and any additional information obtained during investigation.

5.5 **Response Time Targets:** Supplier will use commercially reasonable efforts to meet the following Response Time targets during Normal Business Hours for Incidents reported by a Buyer Authorised Representative:

i) Priority 1 (Critical): Within 1 Normal Business Hour

ii) Priority 2 (High): Within 4 Normal Business hours

iii) Priority 3 (Medium): Within 2 Working Days

iv) Priority 4 (Low): Within 5 Working Days

5.6 **Progress updates:** Supplier will use commercially reasonable efforts to provide status updates for:

i) Priority 1 (Critical): typically at least every 2 Normal Business Hours while actively being worked;

ii) Priority 2 (High): typically at least daily while actively being worked; and

iii) other priorities: as reasonably required.

5.7 **Resolution approach:** Supplier will use commercially reasonable efforts to resolve verified Incidents or provide a functional Workaround. Resolution may involve a permanent fix, a functional

Workaround, or confirmation that the reported behaviour is expected functionality or requires a feature request.

5.8 The following are indicative resolution time targets and are not guaranteed resolution commitments:

i) Priority 1 (Critical): Target 4-8 Normal Business Hours

ii) Priority 2 (High): Target 1-3 Working Days

iii) Priority 3 (Medium): Target 5-10 Working Days

iv) Priority 4 (Low): Resolved as resources permit / in future release cycle.

5.9 **Security incidents:** Where an Incident relates to a suspected security issue or personal data breach, Supplier will respond and communicate in accordance with the Call-Off Contract and (where applicable) the DPA, including providing relevant information and updates as it becomes available.

5.10 **Escalation:** The Buyer may request escalation of a Priority 1 or Priority 2 Incident via the support channel above. Supplier will use commercially reasonable efforts to ensure appropriate technical and managerial attention.

6. Maintenance

6.1 **Scheduled Maintenance:** Planned maintenance windows are typically carried out outside Normal Business Hours with at least two (2) Working Days' notice, unless the Call-Off Contract specifies otherwise.

6.2 **Relationship to Service Modifications notice:** For the avoidance of doubt, Scheduled Maintenance notices under this SLA are operational notices and do not replace any notice of Service Modifications or modifications to Supplier Service Specific Terms required under the Call-Off Contract and completed in the Order.

6.3 **Emergency Maintenance:** Unplanned maintenance may be required to address security vulnerabilities or system failures. Where practicable, Supplier will provide notice to the Buyer as soon as reasonably practicable.

7. Backups and resilience

7.1 **Resilience methodology:** Buyer environments are designed for resilience. Backup data resilience is protected using a standard 3-2-1 model where three copies of the data exist on two types of media, with one off-site from the primary datacentre location.

7.2 **Backup frequency:** Buyer data is backed up daily and retained for 14 days.

7.3 **Testing:** Backup and restore processes are tested at least annually.

7.4 **Data location:** Data location and resilience arrangements are as described in the DPA and as set out in the Order.

8. Changes to this SLA

8.1 This SLA applies for the duration of the Call-Off Contract and may be amended only by written agreement in accordance with the Call-Off Contract.

9. Service Updates

9.1 Supplier may implement updates to the Services from time to time (including new features, bug fixes, security fixes, user interface improvements and enhancements), provided that such updates do not materially reduce the Uptime Commitment or other service level commitments in this SLA for the duration of the Call-Off Contract. If the Buyer reasonably considers that an update has materially reduced such commitments, the Buyer shall notify Supplier and the parties shall use their respective commercially reasonable efforts to discuss the issue and any potential remedial steps in accordance with the Call-Off Contract. Where an update constitutes a Service Modification or a modification to Supplier Service Specific Terms, Supplier will provide notice in accordance with the Call-Off Contract and the notice provisions completed in the Order.

Schedule 2

Data Processing Agreement

1. Scope

1.1 This section sets out the details of personal data processing by Supplier when providing the Services to the Buyer pursuant to the Call-Off Contract.

This DPA is intended to satisfy and supplement the data protection obligations in the Call-Off Contract (including Joint Schedule 10 (Processing Data)) and does not limit any Government Data obligations (as defined in the Call-Off Contract). This DPA does not vary the Call-Off Contract; if there is any inconsistency, the Call-Off Contract prevails.

Supplier acts as a Data Processor and processes personal data solely on behalf of and in accordance with the documented instructions of the Buyer (the "**Data Controller**"), as defined in this data processing agreement ("**DPA**"), and in compliance with the UK GDPR and the Data Protection Act 2018, and, to the extent applicable, the EU GDPR (together, the "**Data Protection Legislation**").

Supplier is committed to protecting Buyer's privacy and handling Buyer's personal data transparently and securely in its role as a Data Processor.

2. Definitions

2.1 Capitalised terms used in this DPA have the meanings set out in the Call-Off Contract, unless defined otherwise in this DPA. References in this DPA to "personal data", "processing", "controller", "processor", "data subject", and "personal data breach" have the meanings given to them in the Data Protection Legislation. For data protection enquiries relating to this DPA, the Buyer may contact Supplier at `privacy@probit.io`.

3. Processor obligations

3.1 Supplier shall:

a) process personal data only on the documented instructions of the Buyer (including with regard to transfers of personal data to a third country or international organisation), unless required to do so by applicable law; where Supplier is required by applicable law to process personal data other than on the Buyer's instructions, Supplier shall

inform the Buyer of that legal requirement before processing, unless applicable law prohibits such information;

b) ensure that persons authorised by Supplier to process personal data are subject to appropriate obligations of confidentiality;

c) implement and maintain appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage;

d) not appoint any sub-processor to process personal data except as set out in this DPA or as otherwise authorised in writing by the Buyer; where Supplier appoints a sub-processor, Supplier shall ensure that the sub-processor is subject to written obligations that are no less protective than the obligations applicable to Supplier under this DPA, and Supplier shall remain responsible for the performance of the sub-processor's obligations;

e) provide reasonable assistance to the Buyer (taking into account the nature of the processing) to enable the Buyer to comply with its obligations under the Data Protection Legislation and Joint Schedule 10 (Processing Data), including in relation to Data Subject requests, security, Data Loss Events, data protection impact assessments and consultations with supervisory authorities;

f) notify the Buyer **immediately** upon becoming aware of any personal data breach and/or any Data Loss Event (as defined in the Call-Off Contract), and provide the Buyer with available information reasonably required to meet the Buyer's notification obligations, and provide further information as details become available;

g) notify the Buyer **immediately** if Supplier receives any complaint, communication or request relating to: (i) a Data Subject Access Request (or purported request), (ii) a request to rectify, block or erase personal data, (iii) any other request, complaint or communication relating to either party's obligations under the Data Protection Legislation, (iv) any communication from the Information Commissioner's Office or other regulatory authority, or (v) any request from a third party for disclosure of personal data where compliance is required or purported to be required by law, and provide reasonable assistance as required by the Call-Off Contract;

h) maintain complete and accurate records and information to demonstrate compliance with this DPA and Joint Schedule 10 (Processing Data), and make such records available to the Buyer in accordance with the Call-Off Contract;

i) at the Buyer's option, return or delete personal data (including copies) at the end of the provision of Services relating to processing under this DPA and, unless otherwise agreed in writing, within 30 days of such end date (or, where the Buyer requests return, within 30 days of such request), unless applicable law or the Call-Off Contract requires retention of some or all of the personal data; and

j) make available to the Buyer information reasonably necessary to demonstrate compliance with this DPA and allow for audits (including inspections) by the Buyer or an

auditor mandated by the Buyer, subject to reasonable notice and reasonable confidentiality and security requirements, provided that nothing in this DPA limits or restricts any audit or inspection rights under the Call-Off Contract.

4. Technical and Organisational Measures (TOMs)

4.1 Without limiting Supplier's obligation to maintain appropriate technical and organisational measures, Supplier maintains a security programme which includes measures such as:

a) **Access control:** role-based access control, least privilege, separation of duties where practicable, and periodic access reviews for sensitive systems;

b) **Authentication:** multi-factor authentication for administrative access and remote access scenarios;

c) **Encryption:** encryption of personal data in transit and at rest using industry-standard encryption mechanisms;

d) **Endpoint security:** controls over authorised devices, and encryption of endpoint storage drives used to access systems processing personal data;

e) **Logging and monitoring:** security logging and monitoring of systems processing personal data to support auditability and incident detection;

f) **Backup and recovery:** encrypted backups with resilience measures, and periodic backup integrity testing and disaster recovery testing; and

g) **Third-party management:** controls over third-party access and contractual requirements for third parties who process personal data on Supplier's behalf.

5. Nature of processing

5.1 The processing involves the collection, access, storage, transmission, and deletion of personal data necessary to provide, maintain, secure, and support the Services. This includes activities such as:

a) Creating and managing Authorised User accounts, including importing data received from the Buyer via email or file transfer;

b) Authenticating users and securing access (e.g., via Multi-Factor Authentication);

c) Logging and monitoring user activity for audit, operational integrity, and security purposes;

d) Providing service support and technical assistance;

e) Performing maintenance, updates, service performance enhancements, and issue diagnostics.

6. Purpose of processing

6.1 The personal data is processed solely for the following purposes:

a) Enabling Authorised Users to access and use the Services;

b) Ensuring the availability, security, performance, and integrity of the Services;

c) Supporting the Buyer's use of the Services in accordance with the Call-Off Contract;

d) Providing technical support and responding to incidents, tickets, or change requests;

e) Complying with the Buyer's lawful and documented instructions, as outlined in this DPA.

7. Duration of the processing

7.1 Supplier will process personal data for the duration of the Buyer's subscription to the Services and thereafter in accordance with the data retention and deletion obligations set out in this DPA or as otherwise instructed by the Buyer, unless applicable law requires a longer retention period.

8. Types of personal data

8.1 The categories of personal data processed may include:

a) Full name, job title or role;

b) Work email address, work telephone number (e.g., for MFA);

c) User login credentials (e.g., username, hashed password);

d) IP addresses, system-generated user ID, login and activity logs;

e) Any personal data incidentally included in Buyer Data uploaded or processed by Authorised Users in the Services.

9. Categories of data subjects

9.1 The personal data processed relates primarily to:

a) Authorised Users of the Services (e.g., employees, contractors, or representatives of the Buyer);

b) Other individuals whose personal data may be incidentally included in Buyer Data (e.g., in documents, free-text notes, or asset-related records uploaded by Authorised Users).

10. International Data Transfers

10.1 Personal data will be stored and processed in the location(s) specified in the Order. If no location is specified, Supplier will store and process personal data primarily within the United Kingdom (UK), with limited copies within the European Economic Area (EEA) solely for backup and resilience purposes. All such personal data shall be encrypted both in transit and at rest using industry-standard encryption mechanisms. Supplier will not transfer personal data outside the UK and/or EEA except where: (i) the Order specifies a location outside the UK and/or EEA, or (ii) the Buyer has provided prior written consent. Where a transfer outside the UK and/or EEA is permitted, Supplier will ensure that the transfer is made in accordance with the Data Protection Legislation and subject to appropriate safeguards (for example, the UK's International Data Transfer Agreement (IDTA) and/or the EU Standard Contractual Clauses (SCCs), as applicable).

11. Permitted Use for Service Improvement

11.1 To the extent permitted by the Call-Off Contract and the Buyer's documented instructions, Supplier may generate and use anonymised and aggregated statistical data derived from the Buyer's use of the Services for the limited purpose of maintaining, supporting, securing and improving the Services (such anonymised and aggregated statistical data, "**Aggregated Service Usage Data**").

Aggregated Service Usage Data:

a) does not include Buyer Data content; and

b) does not identify the Buyer, any Authorised User, or any other individual.

Supplier will not attempt to re-identify any individual from Aggregated Service Usage Data, and will not disclose Aggregated Service Usage Data in a manner that identifies the Buyer or any individual (including in any public benchmarking or marketing materials).

To the extent that any personal data is processed in connection with the activities described in this paragraph, Supplier will process such personal data solely on behalf of and in accordance with the documented instructions of the Buyer and the terms of this DPA.

12. Details of Sub-Processors

Name of Sub-Processor	Purpose of Sub-processing	Location
Google Cloud EMEA Limited[1]	Provision of infrastructure hosting and cloud platform services, email communications, and secure receipt of personal data	As specified in the Order

The Buyer provides its written consent to the appointment of the sub-processor(s) listed in this section

for the purposes described. Supplier will not add or replace sub-processors for the Services without the Buyer's prior written consent, in accordance with Joint Schedule 10 (Processing Data).

[1] Google Cloud EMEA Limited is a sub-processor used by Supplier for infrastructure hosting services. Supplier remains responsible for its sub-processors' compliance with the obligations applicable to them under this DPA. Further information about Google Cloud's data processing terms is available at: https://cloud.google.com/terms/data-processing-addendum.

Schedule 3

Acceptable Use Policy

1. Authorised User Acceptable Use Policy

1.1 This Acceptable Use Policy (the "**AUP**") forms part of, and is incorporated into, the Supplier Terms (the "**Supplier Terms**") for the Services.

1.2 This AUP applies to all individuals who are authorised by the Buyer to access or use the Services on the Buyer's behalf ("**Authorised Users**"). The Buyer shall ensure that its Authorised Users comply with this AUP.

1.3 This AUP is a policy that governs permitted and prohibited use of the Services and does not create a separate agreement between Supplier and any individual Authorised User.

1.4 Capitalised terms used in this AUP have the meaning given to them in the Call-Off Contract and/or the Supplier Terms unless defined otherwise below.

"**Authorised User**"	means an individual authorised by the Buyer to access and use the Services.
"**Malicious Software**"	means any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on programme files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfuly, negligently or without knowledge of its existence, including computer programs commonly referred to as viruses, worms, trojan horses, time or logic bombs, backdoors and rootkits.
"**Services**"	means the Services as defined in the Supplier Terms.

1.5 Reports of suspected misuse should be directed to Supplier by email at: `abuse@probit.io`.

2. Acceptable Use

2.1 Authorised Users shall only use the Services in compliance with the Call-Off Contract, the Supplier Terms, applicable laws, and regulations. In particular, Authorised Users must not, directly or indirectly:

a) Use the Services for illegal or fraudulent activities or infringe the rights of others, in-

cluding intellectual property and privacy rights.

b) Copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Software or Documentation except as expressly permitted by the Call-Off Contract;

c) Attempt to de-compile, reverse compile, disassemble, reverse engineer, or otherwise derive source code or underlying structures from the Services.

d) Use the Services, Software, or Documentation to provide services to third parties or to build any competing product or service.

e) Licence, sell, rent, lease, transfer, assign, or otherwise make available the Services or Documentation to third parties not authorised by the Buyer under the Call-Off Contract and/or the Supplier Terms.

f) Introduce, distribute, transmit, or enable the introduction, distribution, or transmission of, any Malicious Software, vulnerabilities, or harmful code into or via the Services.

g) Probe, scan, or test the Services or Supplier's systems and networks for vulnerabilities, or breach or exploit any identified vulnerability, without Supplier's express prior written authorisation.

h) Disrupt, impair, or interfere with the integrity, performance, or security of the Services or Supplier's systems and networks, including denial-of-service attacks and unauthorised penetration tests.

i) Attempt unauthorised access, modification, or damage to the Services, user accounts, or data belonging to others.

j) Upload, store, or transmit content that is unlawful, harmful, defamatory, abusive, obscene, discriminatory, harassing, hateful, sexually explicit, or racially or ethnically offensive.

k) Upload, store, or transmit any data or material that infringes or misappropriates the intellectual property rights or proprietary rights of any third party, or that the Buyer or the relevant Authorised User does not have the right or necessary permissions to use.

l) Falsify identity or affiliation with intent to mislead.

m) Remove, obscure, or alter any copyright, trademark, proprietary rights, or confidentiality notices within or generated by the Services or Documentation.

n) Violate applicable export controls, sanctions, or economic restrictions, including those of the UK, EU, or US.

2.2 Supplier may monitor use of the Services to confirm compliance with this AUP and to protect the Services and Supplier's systems and networks.

2.3 If Supplier reasonably believes that this AUP has been breached, Supplier will notify the Buyer and request remediation. Any suspension or restriction of access to the Services will occur only

to the extent expressly permitted under the Call-Off Contract and/or required to address an immediate and material security threat.

3. Access and Security

3.1 Authorised Users' access to the Services is restricted to the login credentials provided by the Buyer (or by Supplier where applicable).

3.2 Authorised Users must maintain the confidentiality of their login credentials and not share them with any other individual.

3.3 Authorised Users must promptly notify the Buyer if they suspect or become aware of any unauthorised use or breach of their account security.

4. Technical Requirements

4.1 The Buyer and its Authorised Users must ensure their networks, devices, and software meet any published technical requirements necessary to effectively use the Services.

5. Personal Information and Data Protection

5.1 Any personal information or personal data uploaded, stored, or transmitted via the Services is processed by Supplier solely as a data processor on behalf of the Buyer, in accordance with the Data Processing Agreement agreed between Supplier and the Buyer.

5.2 The Buyer is the data controller of personal data input into the Services by Authorised Users, and the Buyer shall ensure that Authorised Users follow any relevant data protection policies and instructions provided by the Buyer in relation to use of the Services.