DATA USAGE & PRIVACY POLICY

SYSTEM OVERVIEW

1.1 This Data Usage & Privacy Policy ("Policy") governs the processing of personal data in connection with the Haccpy system (the "System"), operated by the Provider. The System is designed to support food safety compliance through AI-assisted monitoring of kitchen environments, including the detection of potential hygiene and procedural violations, and may involve the processing of personal data, including visual data relating to individuals present within monitored areas.

This Policy applies to:

- customers using the System ("Customer"); and
- individuals whose data may be processed through the System, including employees and contractors ("Data Subjects").

The Customer acknowledges that the privacy characteristics of the System differ materially depending on the selected deployment model, and that the Customer is solely responsible for selecting a model consistent with its legal obligations and internal policies.

For the purposes of this Policy, "System" and "Services" shall be used interchangeably unless the context requires otherwise.

1. NATURE OF THE SYSTEM AND DATA PROCESSING ARCHITECTURE

The System may operate under one or both of the following models:

(a) Edge Processing Model (Haccpy Bridge)

- Video feeds are processed locally within the Customer's premises
- No continuous video streaming to the cloud
- Only event-based outputs (e.g., metadata or snapshots, where enabled) are transmitted

(b) Cloud Processing Model (Haccpy Air)

- Video feeds may be transmitted to and processed within cloud infrastructure
- Processing occurs on Provider-controlled or third-party servers

The Customer:

- selects the deployment model, and
- is responsible for informing individuals accordingly.

(c) Output Data

Depending on configuration and subscription:

- Alerts and metadata (e.g., "PPE violation detected")
- Snapshots (still images capturing the event)
- Logs, reports, and analytics

For the avoidance of doubt:

- The System does **not guarantee that all violations will be detected**
- Outputs are probabilistic and AI-generated

2. ROLES AND RESPONSIBILITIES

2.1 Customer as Data Controller: The Customer acts as the data controller in respect of all personal data processed through the Services. The Customer determines, independently and exclusively:

- the purposes of processing, including workplace monitoring and compliance objectives,
- the deployment and positioning of cameras and devices,
- the categories of individuals subject to monitoring,
- the scope of data collected (including whether snapshots are enabled),
- retention periods and data access policies, and
- any disclosures to third parties.

The Customer shall be solely responsible for:

- ensuring that all processing is lawful under applicable legislation, including UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data,
- providing all required notices to employees and other individuals,
- obtaining any necessary consents or authorizations (where required),
- complying with applicable employment, surveillance, and data protection laws, and
- determining who is authorized to access and use the data generated by the Services.

2.2 Provider as Data Processor: The Provider shall act as a **data processor**, processing personal data solely:

- on behalf of the Customer, and
- in accordance with the Customer's documented instructions, as set out in this Policy and the applicable service configuration.

The Provider shall not:

- process personal data for its own independent purposes,
- sell, disclose, or otherwise exploit personal data, or
- determine the purposes for which personal data is processed.

2.3 The Customer acknowledges that the Services utilize **automated detection systems (AI models)** to identify predefined safety-related events (e.g. PPE non-compliance).

Such processing:

- is performed based on system parameters, configurations, and operational deployment determined by the Customer,
- constitutes a **technical means of executing the Customer's monitoring objectives**, and
- does not involve the Provider making independent decisions regarding the purposes of processing.

The Customer remains solely responsible for:

- interpreting system outputs,
- making any operational, disciplinary, or compliance decisions, and
- ensuring that any use of automated outputs complies with applicable law.

2.4 The Customer's instructions are defined by:

- this Policy,
- the system configuration selected by the Customer, and
- any written directions provided by the Customer.

The Provider shall process personal data only within the scope of such instructions, unless required to do otherwise by applicable law.

2.5 Subprocessors and Infrastructure: The Customer authorizes the Provider to engage third-party service providers (including cloud infrastructure providers) as subprocessors for the provision of the Services. The Provider shall:

- ensure that such subprocessors are bound by contractual obligations consistent with this Policy, and
- remain responsible for their compliance with applicable data protection requirements

2.6 No Reclassification of Roles: Nothing in this Agreement or the operation of the Services shall be interpreted as:

- creating a joint controller relationship, or
- granting the Provider any control over the purposes of processing.

The Parties expressly agree that the Provider's role is limited to that of a processor.

3. DATA PROCESSING TERMS

3.1 The Provider shall process personal data solely:

- on behalf of the Customer; and
- in accordance with the Customer's documented instructions as set out in this Agreement and any applicable system configuration.

The Provider shall not:

- determine independent purposes of processing; or
- process personal data for its own commercial benefit.

3.2 Scope and Limitation of Processing: Processing shall be strictly limited to:

- operation of the System
- detection and notification of compliance-related events
- system maintenance and support

Under no circumstances shall the Provider:

- use personal data for profiling unrelated to system functionality
- use personal data for marketing or advertising
- use personal data for AI training unless separately agreed

3.3 The Provider does not:

- make decisions regarding individuals
- take employment or compliance actions

All outputs generated by the System:

- are automated signals
- require human interpretation

The Customer retains sole responsibility for any decisions taken based on such outputs. If the Provider determines that any instruction from the Customer may violate applicable law, the Provider reserves the right to:

• suspend the relevant processing activity; and/or

• notify the Customer and request modification of such instruction.

3.4 Confidentiality: The Provider shall ensure that:

- all personnel authorized to process personal data are bound by confidentiality obligations
- access is restricted on a need-to-know basis

3.5 Security Measures: The Provider shall implement appropriate technical and organizational measures, including:

- encryption in transit
- access control mechanisms
- system monitoring

3.6 Sub-Processors: The Customer authorizes the Provider to engage sub-processors for infrastructure and service delivery purposes.
The Provider shall:

- ensure sub-processors are bound by equivalent data protection obligations
- remain fully liable for their performance

3.7 Data Breach Notification: In the event of a personal data breach, the Provider shall:

- notify the Customer without undue delay
- provide relevant information reasonably available

The Customer remains responsible for:

- regulatory notifications
- communication with affected individuals

3.8 The Provider shall provide reasonable assistance to the Customer in:

- responding to data subject requests
- demonstrating compliance with applicable data protection obligations

3.9 Data Return and Deletion: Upon termination of services:

- personal data shall be deleted or returned
- unless retention is required by law

4. WORKPLACE MONITORING COMPLIANCE

The Customer acknowledges that use of the System involves workplace monitoring and agrees as follows
4.1 The System shall be used solely for legitimate business purposes, including food safety compliance and operational management. The Customer shall ensure that monitoring is proportionate, limited to what is necessary for the stated purposes, and implemented in a manner that minimizes intrusion into the privacy of individuals.
4.2 The Customer is solely responsible for compliance with all applicable laws, including:

- **UAE Federal Decree-Law No. 45 of 2021 (PDPL)**
- applicable labour and privacy laws
- any other applicable law from time to time

4.3 The Customer must:

- provide clear prior notice to all monitored individuals
- implement visible signage
- maintain internal monitoring policies

4.4 The Customer must ensure a valid legal basis for processing, including:

- legitimate interest; or
- consent, where required

4.5 The Customer shall not:

- conduct covert surveillance
- monitor private areas (e.g., restrooms, changing rooms)
- use outputs for excessive or disproportionate disciplinary actions without human oversight

4.6 The Customer must:

- restrict access to authorized personnel
- define appropriate retention periods
- ensure lawful handling of snapshots and reports
- ensure monitoring is lawful, proportionate and justified

The Provider does not interact directly with monitored individuals and bears no responsibility for Customer compliance obligations.

5. DATA CATEGORIES AND PURPOSES OF PROCESSING

5.1 Categories of Data Processed: Depending on the deployment model, system configuration, and features enabled by the Customer, the Services may process the following categories of data:

(a) Visual Data

- live video feeds (processed locally and/or transmitted for cloud-based processing, where applicable),
- still image snapshots captured upon detection of predefined events (if enabled by the Customer).

(b) Event and Derived Data

- detected violations or compliance events,
- timestamps and duration markers,
- location or device identifiers,
- system-generated classifications and labels produced by automated detection models.

(c) Operational and Technical Data

- device identifiers and system configuration data,
- system logs and diagnostic information,
- usage metrics and performance data,
- connectivity and processing metadata.

(d) Personal Data (Conditional)

To the extent that individuals are identifiable from the data processed, personal data may include:

- employee presence within monitored areas,
- observable workplace behavior (e.g. PPE usage or non-compliance), and
- associations between individuals and recorded events.

For the avoidance of doubt:

- not all data processed by the Services constitutes personal data, and
- personal data is processed only where identification of an individual is reasonably possible in context.

5.2 Purposes of Processing: Personal data (where applicable) and related system data are processed strictly for the following purposes:

- monitoring compliance with food safety and HACCP-related protocols,
- detection of predefined operational or safety violations,
- generation of alerts, notifications, and compliance reports,
- maintenance of audit-ready compliance records,
- ensuring system functionality, performance, and reliability, and
- supporting troubleshooting, diagnostics, and service improvement.

Processing shall be limited to what is **necessary and proportionate** for the above purposes.

5.3 The Customer, as data controller, is solely responsible for determining the lawful basis for processing under applicable law, including but not limited to:

- legitimate business interests in ensuring food safety and operational compliance,

- compliance with applicable regulatory or health and safety obligations, and
- workplace monitoring requirements, where permitted by law.

The Provider does not independently determine or validate the lawful basis for processing.

The Customer acknowledges that where processing is based on legitimate interests, it shall conduct and document an assessment confirming that:

• the processing is necessary for a legitimate business purpose;
• such purpose cannot reasonably be achieved by less intrusive means; and
• the interests or fundamental rights of Data Subjects do not override such interests.

5.4 Purpose Limitation: The Provider shall process personal data exclusively for the purposes set out in Section 5.2 and in accordance with the Customer's documented instructions. The Provider shall not process data for:

- marketing or advertising purposes,
- behavioural profiling unrelated to system functionality,
- employee performance evaluation beyond system-defined compliance outputs, or
- AI model training, development, or improvement, except where expressly agreed under a separate and explicit policy.

5.5 Configuration-Dependent Processing: The Customer acknowledges that the scope and nature of data processed depend on system configuration choices, including:

- whether snapshot capture is enabled,
- whether processing occurs locally (edge) or via cloud infrastructure, and
- the number, placement, and quality of cameras deployed.

The Customer is responsible for configuring the system in a manner consistent with its legal obligations. Snapshot capture is event-triggered and dependent on Customer configuration. The Customer determines whether such functionality is enabled and is responsible for ensuring its lawful use

5.6 The Provider shall not:

- combine data from different Customers,
- use data to identify individuals beyond the intended system functionality, or
- expand the scope of processing beyond what is necessary to deliver the Services.

5.7 The Provider shall process only the minimum amount of personal data necessary to achieve the purposes defined in this Policy, and the Customer shall configure the System accordingly, including limiting:

• camera coverage,
• snapshot capture, and
• retention duration.

6. DATA SUBJECT RIGHTS

6.1 Controller Responsibility: The Customer acts as the **data controller** in respect of all personal data processed through the Services and shall be solely responsible for responding to any requests from individuals (data subjects) exercising their rights under applicable data protection laws, including, but not limited to, those under UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data.

6.2 Submission of Requests: All data subject requests, including requests for access, rectification, erasure, restriction of processing, or objection, must be directed

to the Customer. The Provider shall not be responsible for responding directly to data subjects except as required by applicable law.

6.3 Provider Assistance: To the extent required by applicable law, and subject to Section 6.5 below, the Provider shall provide **reasonable assistance** to the Customer in fulfilling data subject requests, including by:

- enabling access to relevant stored data (where technically feasible),
- facilitating correction or deletion of data within the system, and
- providing information regarding processing activities.

Such assistance shall be provided **only upon documented instructions from the Customer**.

6.4 If the Provider receives a request directly from a data subject, the Provider shall:

- not respond substantively to the request, and
- promptly refer the request to the Customer, unless otherwise required by applicable law.

6.5 Limitations and Technical Constraints: The Customer acknowledges that the Provider's ability to support data subject rights may be limited where:

- data has been deleted in accordance with agreed retention periods,
- data is contained within system logs, backups, or aggregated datasets,
- processing is limited to metadata or event-based outputs (e.g. violation records), or
- fulfilling the request would require disproportionate effort or is not technically feasible.

In such cases, the Provider shall inform the Customer and cooperate in good faith to determine an appropriate response.

6.6 **Legal Retention Requirements**:

The Provider shall not be required to delete or restrict processing of data where retention is required:

- to comply with applicable law,
- for the establishment, exercise, or defense of legal claims, or
- for legitimate internal security, audit, or compliance purposes.

6.7 Cost and Resource Allocation: Where assistance provided by the Provider requires **material effort, system changes, or manual intervention**, such assistance may be:

- subject to reasonable fees, and
- provided within commercially reasonable timelines.

6.8 The Customer acknowledges that:

- the Services are designed to process **event-based data (e.g. violations, metadata, and snapshots)** rather than continuous video streams (unless otherwise configured), and
- data subject rights shall apply only to the extent such data is actually processed and retained within the system.

7. DATA SECURITY

7.1 Security Measures: The Provider shall implement and maintain **appropriate technical and organizational measures** designed to protect personal data against unauthorized or unlawful processing, accidental loss, destruction, or damage, in accordance with applicable law, including UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data.

Such measures shall include, at a minimum:

- encryption of data in transit using industry-standard protocols (e.g. TLS/HTTPS),
- access controls based on least-privilege principles,
- authentication mechanisms for system access,
- segregation of environments where applicable,
- system monitoring, logging, and anomaly detection,
- secure configuration and maintenance of cloud infrastructure, and
- regular review of security practices.

7.2 The Provider's system is designed, where applicable, to:

- process video feeds locally at the edge (e.g. via on-site bridge devices), and
- transmit and store only **event-based outputs** (such as violation metadata and snapshots), rather than continuous video streams.

The Customer acknowledges that system configuration (including use of cloud-based processing modes) may affect the scope and location of data processing and associated security controls.

7.3 Access Control and Personnel: The Provider shall ensure that access to personal data is:

- restricted to authorized personnel on a need-to-know basis,
- subject to confidentiality obligations, and
- protected through appropriate authentication and authorization controls.

7.4 The Customer acknowledges that data security is a **shared responsibility**, and the Customer remains solely responsible for:

- securing its own infrastructure, networks, and camera systems,
- configuring devices and environments in accordance with Provider recommendations,
- managing user access credentials and permissions, and
- implementing appropriate internal security policies and staff training.

The Provider shall not be responsible for security incidents arising from Customer-controlled environments or third-party systems.

7.5 Data Retention and Secure Deletion: The Provider shall retain data only for the period agreed with the Customer and shall implement reasonable measures to ensure secure deletion or anonymization of data upon expiry of such retention period, unless retention is required by applicable law or for legitimate legal purposes.

7.6 Security Incidents and Breach Notification: In the event of a **confirmed personal data breach** affecting Customer data, the Provider shall:

- notify the Customer without undue delay after becoming aware of the breach,
- provide reasonably available information regarding the nature and scope of the incident, and
- cooperate with the Customer in assessing and mitigating the impact of the breach.

The Customer remains responsible for determining whether notification to regulators or data subjects is required under applicable law.

7.7 Subprocessors and Third Parties: Where the Provider engages third-party service providers (including cloud infrastructure providers), the Provider shall:

- ensure such parties are subject to contractual obligations consistent with this Policy, and
- implement appropriate safeguards to protect personal data.

7.8 While the Provider implements security measures consistent with industry standards, the Customer acknowledges that:

- no system can be guaranteed to be completely secure, and
- the Provider does not warrant that the Services will be free from vulnerabilities, unauthorized access, or security breaches.

8. DATA TRANSFERS

8.1 The Customer acknowledges that, in order to provide the Services, personal data may be processed, stored, or accessed in jurisdictions outside the United Arab Emirates.
Such processing may occur where necessary for:

- operation of cloud infrastructure;
- system functionality and performance;
- technical support, maintenance, and security operations.

8.2 The Provider does not commit to processing personal data exclusively within any specific jurisdiction and reserves the right to determine and modify the location of its processing infrastructure, provided that such processing complies with this Policy and applicable data protection laws.
8.3 To the extent the Provider processes personal data on behalf of the Customer, any cross-border transfer shall be carried out:
(a) on the documented instructions of the Customer; and
(b) as necessary for the performance of the Services; and
(c) subject to the implementation of appropriate safeguards in accordance with applicable data protection laws, including the UAE Personal Data Protection Law.
8.4 The Provider shall implement and maintain appropriate safeguards for cross-border processing, including:

- contractual obligations binding the Provider and any sub-processors to data protection standards consistent with this Policy;
- implementation of industry-standard technical and organizational security measures;
- access controls and role-based restrictions; and
- processing strictly limited to defined and legitimate purposes.

8.5 Where cross-border transfers involve third-party service providers or sub-processors, the Provider shall ensure that:

- such entities are subject to written agreements imposing data protection obligations equivalent to those set out in this Policy; and
- the Provider remains responsible for the acts and omissions of such sub-processors in connection with the processing of personal data.

8.6 By using the Services, the Customer:

- acknowledges that cross-border data transfers are necessary for the provision of the Services; and
- authorizes the Provider to perform such transfers in accordance with this Section and applicable law.

8.7 If applicable laws impose additional restrictions or requirements in relation to cross-border data transfers, the Provider may:

- implement additional safeguards; or
- modify processing arrangements

as reasonably necessary to ensure compliance.
8.8 To the maximum extent permitted by law, the Provider shall not be liable for:

- legal restrictions arising from the Customer’s jurisdiction of operation; or

- any requirement imposed on the Customer relating to international data transfers beyond the Provider's direct control,

provided that the Provider has implemented the safeguards set out in this Section.

9. DATA RETENTION & DATA LIFECYCLE

9.1 Data access and processing by the Provider: The Provider may access personal data only to the extent strictly necessary for:

- provision of the Services,
- system maintenance, troubleshooting, and support, and
- performance of its obligations under documented instructions from the Customer.

The Provider shall ensure that:

- access is restricted to authorized personnel on a need-to-know basis,
- appropriate role-based access controls are implemented, and
- personal data is processed solely for the purposes defined in this Policy.

9.2 Data Lifecycle Overview: The Services process data in a structured lifecycle consisting of:

- **capture**,
- **transmission**,
- **processing**,
- **storage**, and
- **deletion.**

Each stage is governed by system configuration and Customer-defined parameters.

9.3 Event Capture: Where the System detects a potential compliance or safety event:

- an event record is generated, and
- a snapshot or data point may be created (if enabled by the Customer configuration).

For the avoidance of doubt, the System is designed to generate **event-based records rather than continuous video storage**, unless explicitly configured otherwise.

9.4 Transmission of Data: Depending on system configuration:

- event data and associated snapshots are transmitted from on-site devices to cloud infrastructure via encrypted communication channels, and/or
- processed locally and transmitted as metadata-only records.

9.5 Storage of Data: The Provider stores only the following data in cloud infrastructure:

- event records, and
- snapshots (where enabled by the Customer).

No continuous video footage is stored unless the Customer explicitly enables a cloud-processing mode. All stored data remains logically segregated per Customer environment. The Customer acknowledges that snapshots may constitute high-risk personal data due to their potential to identify individuals and depict specific conduct, and shall implement appropriate safeguards governing access, use, and disclosure of such data.

9.6 Retention Period: Retention of data is determined by the Customer, based on system configuration and operational requirements. Accordingly:

- event data and snapshots are retained only for the period defined by the Customer,
- upon expiry of the retention period, data is automatically deleted or anonymized by the system, and
- the Customer is responsible for configuring and maintaining appropriate retention settings.

9.7 Where the Customer does not actively configure retention settings, the Provider may apply a default retention period, as defined in system documentation or technical configuration, solely to ensure system operability.
Such default retention shall:

- not override Customer instructions once provided, and
- remain subject to applicable legal requirements.

9.8 Deletion and Irretrievability: Upon expiry of the applicable retention period:

- data shall be securely deleted or anonymized using commercially reasonable technical methods, and
- such data shall not be recoverable through normal system operation.

The Provider shall not be responsible for recovery of data once deletion has been executed in accordance with this Section.
9.9 Backups and Residual Data: The Customer acknowledges that:

- limited copies of data may persist in encrypted backup systems for disaster recovery purposes, and
- such backups are subject to rolling overwrite cycles and are not actively accessible for operational use.

Backup data shall be retained only for the minimum period necessary for system recovery and integrity.
9.10 Legal and Operational Retention Overrides: Notwithstanding the above, the Provider may retain data where required:

- by applicable law,
- for the establishment, exercise, or defense of legal claims, or
- for security, audit, or system integrity purposes.

9.11 Except as expressly set out in this Section, the Provider shall not:

- retain personal data beyond the Customer-defined retention period,
- use retained data for any independent purpose, or
- extend retention for analytical, commercial, or training purposes.

10. LIMITATIONS OF THE SYSTEM

10.1 The System is an AI-assisted monitoring and alerting tool designed to support food safety and operational compliance. It operates through automated analysis of visual inputs and generates event-based outputs. The System is not designed as an employee performance evaluation or disciplinary tool, and any such use shall be solely at the Customer's discretion and risk, subject to applicable labour laws. For the avoidance of doubt, the System:

- does not identify or verify the identity of individuals
- does not perform biometric identification or facial recognition
- does not make legal, regulatory, or employment decisions
- does not replace human supervision, judgment, or compliance obligations

10.2 The Provider does not warrant or guarantee that:

- all violations or non-compliant behaviour will be detected;

- detections will be accurate, complete, or error-free; or
- the System will operate without interruption or misclassification.

The Customer acknowledges that the System may generate:

- false positives (incorrect alerts), and/or
- false negatives (missed events).

10.3 System performance is inherently dependent on factors outside the Provider's control, including:

- camera quality, resolution, and field of view
- positioning and installation of cameras
- lighting, obstructions, and environmental conditions
- network connectivity and infrastructure

The Provider shall have no liability for any failure, inaccuracy, or degradation of performance arising from such factors.

10.4 All outputs generated by the System, including alerts, classifications, and snapshots:

- are probabilistic and algorithmically generated
- are intended solely as assistive indicators
- do not constitute verified facts, conclusions, or determinations

Such outputs must be independently reviewed and validated by the Customer prior to any action

10.5 The System performs automated analysis and classification of visual inputs; however, it does not produce decisions that have legal or similarly significant effects on individuals without human intervention. The Customer shall ensure that:

- no decision affecting an individual is based solely on automated outputs; and
- meaningful human review is applied before any action is taken.

10.6 The Customer retains sole and exclusive responsibility for:

- interpreting System outputs
- determining whether a violation has occurred
- taking any operational, disciplinary, or compliance-related action

The Provider shall have no liability for:

- any decisions made by the Customer based on System outputs; or
- any consequences arising from such decisions.

10.7 Use of the System does not:

- ensure compliance with HACCP or other regulatory requirements
- replace legally required processes, audits, or supervision
- The Customer remains fully responsible for compliance with all applicable laws and regulations.

10.8 System outputs, including snapshots and alerts:

- are generated for operational support purposes only
- are not certified records
- shall not be treated as conclusive evidence of misconduct or non-compliance

11. INDEMNITY & LIABILITY ALLOCATION

11.1 Customer Indemnity: The Customer shall indemnify, defend, and hold harmless the Provider and its affiliates, officers, employees, and contractors from and against any and all:

- claims, demands, actions, or proceedings,
- regulatory investigations or enforcement actions,

- damages, losses, liabilities, fines, penalties, and costs (including reasonable legal fees),

arising out of or in connection with:
(a) the Customer's use of the Services in violation of applicable law, including but not limited to UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data;
(b) unlawful or non-compliant workplace monitoring practices, including improper camera placement or excessive surveillance;
(c) failure to provide adequate notice to employees or other individuals, or failure to obtain required consents or authorizations;
(d) the Customer's determination of purposes of processing or reliance on an invalid or insufficient legal basis;
(e) misuse, misinterpretation, or improper reliance on system outputs, alerts, or AI-generated classifications;
(f) failure to configure the system in accordance with legal or operational requirements, including retention settings and access controls;
(g) any disclosure, sharing, or use of data by the Customer outside the scope of this Policy; and
(h) any breach by the Customer of this Policy or applicable laws and regulations.

11.2 Provider Indemnity: The Provider shall indemnify the Customer solely against third-party claims arising directly from:

- the Provider's willful misconduct or fraud, or
- a material breach of its obligations under this Policy in relation to data security.

This indemnity shall not apply to the extent that any claim arises from matters listed in Section 11.1.

11.3 A Party seeking indemnification shall:

- promptly notify the other Party in writing of the claim,
- provide reasonable cooperation in the defense and resolution of the claim, and
- allow the indemnifying Party to control the defense and settlement of the claim, provided that no settlement admitting liability or imposing obligations on the indemnified Party shall be entered into without its prior written consent (not to be unreasonably withheld).

11.4 This Section shall be read in conjunction with any limitation of liability provisions set out in the applicable Terms and Conditions and any individual Agreement between the Provider and the Customer.
To the maximum extent permitted by law:

- indemnity obligations shall be subject to the agreed liability caps, except in cases of fraud or wilful misconduct, and
- no Party shall be liable for indirect or consequential damages except as expressly provided.

11.5 The Parties acknowledge and agree that:

- the Customer acts as data controller and bears primary responsibility for compliance with applicable data protection, employment, and workplace monitoring laws, and
- the Provider acts solely as a data processor and shall not be responsible for determining the legality of the Customer's data processing activities.

The User further confirms that it has had the opportunity to seek independent advice prior to acceptance.

For [USER]
Name: _____
Title: _____
Signature: _____
Date: _____