PRIVACY POLICY

Last Updated On: October 28, 2026

1. INTRODUCTION

This privacy policy explains how AssureOne Technologies LLC (collectively, "Company", "we," "us," and "our") collects, uses, shares, and processes information about you. This privacy policy describes our practices concerning your personal data that we process when we provide you with AssureOne's services, including the services available through our website at http://assureone.ai, our mobile, browser, and desktop applications, and other services where we link this Policy (collectively the "Services").

It also tells you about your privacy rights. Our Terms of Service provide further terms governing your use of the Services. Together, along with this Privacy Policy, our Terms of Service, and any other electronic or written agreement as applicable between or applicable to AssureOne and Customer, which govern the provision of the Service to you, as may be updated from time to time, form our "Agreement." By accessing, downloading, registering with, purchasing from, or otherwise using our Services, you agree to the Agreement.

Please read this Privacy Policy and all other applicable terms of our Agreement carefully before you start to use the Services. By using the Services or signing up for an account, you accept and agree to be bound and abide by the Agreement and consent to and agree that we may collect, process, use, retain, disclose, and transfer your Personal Data as described in this Privacy Policy. If you do not agree to the full Agreement, you must not access or use the Services.

We reserve the right to change this Privacy Policy at any time. We will alert you that changes have been made by indicating the "Last updated on" date of the current version. We encourage you to review this Privacy Policy from time to time to make sure that you understand how any Personal Data we collect will be used.

2. SCOPE AND DEFINITIONS

2.1 Scope. This Privacy Policy applies to Personal Data processed through the Services, including data processed on account registration, during use and configuration of the platform, in support

interactions, during migration or integration, and in communications with us. It applies to our processing wherever carried out, subject to any additional requirement imposed by applicable law in a particular jurisdiction, and in particular to the provisions under the headings European Economic Area and United Kingdom and California and Other United States State Privacy Laws. It does not apply to third-party websites, applications or platforms accessible through or connected to the Services, or to any processing you carry out outside the Services.

2.2 Definitions. In this Privacy Policy:

(a) "Customer" means any individual, legal entity, organisation or professional firm that subscribes to, purchases, or enters into an agreement with the Company for access to or use of the Services. "You" and "your" mean the Customer, as the context requires. Where this Privacy Policy assigns obligations specifically to a Data Controller or contracting party, those obligations apply to the Customer.

(b) "Customer Data" means all data, content, documents and records uploaded, submitted, imported, migrated, transmitted or generated by or on behalf of a Customer through the Services;

(c) "Personal Data" means any information relating to an identified or identifiable natural person, and includes "personal information" and any equivalent term used under applicable law; and

(d) "Data Controller" and "Data Processor" have the meanings given to them under applicable data protection law, and include the equivalent terms used under applicable law, including "business", "service provider" and "processor".

(e) "Authorised User" means an individual authorised by a Customer to access or use the Services on the Customer's behalf, including its administrators, employees, officers, contractors, consultants and invited collaborators. Each Authorised User acts under the authority and responsibility of the Customer that granted them access.

(f) "Sub-processor" means a third party engaged by the Company to process Personal Data contained in Customer Data on behalf of a Customer for the purpose of providing, operating, supporting or securing the Services. A Sub-processor does not include a

Customer-Enabled Integration or an independent third-party website or service that is not engaged by the Company to process Customer Data on its behalf.

(g) "Aggregated Data" means information combined from multiple records or Customers and maintained in a form that does not identify an individual or a specific Customer.

(h) "Account Data" means registration, authentication, subscription, billing, administrator, user profile, and account-configuration information processed by the Company for its own operational purposes.

(i) "Usage Data" means technical, device, log, diagnostic, and interaction information generated through use of the Services.

(j) "De-identified Data" means data modified so that it does not identify and cannot reasonably be linked to an individual or a specific Customer.

(k) "Customer-Enabled Integration" means a third-party application, platform or service that a Customer or its Authorised User voluntarily connects to, enables or directs the Company to use with the Services in order to import, export, transmit, synchronise or otherwise exchange Customer Data.

(l) "Applicable Data Protection Law or Applicable Law" means all data protection, privacy and data security laws applicable to a party's processing of Personal Data, including Regulation (EU) 2016/679 (the "GDPR"), the UK General Data Protection Regulation and the Data Protection Act 2018 (the "UK GDPR"), the Swiss Federal Act on Data Protection, the California Consumer Privacy Act as amended by the California Privacy Rights Act and its implementing regulations (the "CCPA"), and the comprehensive consumer privacy statutes of other States of the United States, in each case as amended, supplemented or replaced from time to time and to the extent applicable.

(m) "Sensitive Personal Data" means Personal Data classified as sensitive, special category or of a special nature under Applicable Data Protection Law.

(n) "Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data processed within our environment.

(o) “Consent” means a freely given, specific, informed and unambiguous indication of a data subject’s wishes, given by a clear affirmative action, signifying agreement to the processing of Personal Data relating to them for a specified purpose.

(p) "Data Processing Addendum” or “DPA” means a standalone data processing addendum entered into by, or otherwise applicable to, the Company and the Customer in connection with the Services, or the data processing terms contained in a Signed Addendum such as Engagement Letter, that are expressly intended to govern the Processing of Personal Data.

3. ROLES OF THE PARTIES

3.1 You are the Data Controller. In respect of Personal Data contained in Customer Data, the Customer is the Data Controller. The Customer determines the categories of Personal Data submitted to the Services, the purposes for which it is processed, the lawful basis relied upon, the notices provided and consents obtained, the persons authorised to access it, the Customer-Enabled Integration connected to its account, and the period for which it is retained within the Services. Authorised Users access and process Customer Data on behalf of, and under the authority of, the relevant Customer and do not become Data Controllers merely by accessing or using the Services.

3.2 We are the Data Processor. In respect of Customer Data, the Company acts solely as data processor. We process Customer Data only on your documented instructions and only as necessary to host, provide, operate, support and secure the Services and to generate the outputs you request. We do not determine the purposes of that processing, do not process Customer Data for our own purposes, and do not review, verify or assess the accuracy, legality or provenance of Customer Data or the adequacy of your lawful basis for processing it.

3.3 Where we act as Controller. We act as data controller only in respect of data we process for our own business purposes, namely website and marketing data, account registration and authentication data, subscription and billing records, support correspondence, and security and system log data generated in operating the Services. We are not a controller of Customer Data.

3.4 Service Provider Status. Where the law treats us as a “service provider” or “processor” for Personal Data in Customer Data, we will use that data only to provide the Services. We will not sell or share it, use it outside our relationship with you, or combine it with data from anyone else, unless the law expressly allows it.

3.5 No Joint Controllership. Nothing in this Privacy Policy is intended to establish the Company and any Customer as joint controllers in respect of Customer Data. The Company and the Customer perform their respective roles in accordance with Applicable Data Protection Law and the applicable Data Processing Addendum.

4. YOUR RESPONSIBILITIES AS DATA CONTROLLER

4.1 Controller obligations.

Where a Customer uploads, submits or otherwise makes Personal Data available through the Services, the Customer acts as the Data Controller in respect of that Personal Data, and the Company acts as the Data Processor on the Customer's behalf. The Customer is responsible for complying with the data protection and privacy laws applicable to its collection, use, disclosure, transfer and retention of Personal Data. The Customer is also responsible for the acts and omissions of its Authorised Users in connection with their access to and use of the Services.

4.2 Onward protection and written agreement. A Data Controller is also responsible for protecting the Personal Data it entrusts to its Data Processors and shall have a written agreement in place with the processor recording the details of the processing, including its subject matter, duration, nature and purpose, the categories of Personal Data and of data subjects concerned, and the respective obligations and rights of the parties. Your use of the Services is accordingly subject to the Terms of Service, Applicable Law and Data Processing Addendum entered into between you and the Company, which forms part of your agreement with us.

4.3 Specific responsibilities. You are responsible for issuing privacy notices and obtaining any consents required from the individuals whose Personal Data you upload; for ensuring you hold a valid lawful basis for that processing; for granting, reviewing and withdrawing access permissions within your account; for the security of your own credentials, devices, systems and personnel; for configuring any third-party integration you elect to connect; for responding to requests from the individuals whose data you control; and for observing the professional, confidentiality and record-retention obligations applicable to you.

4.4 Reliance. You warrant that you hold all rights, notices, consents and authorisations necessary to upload Personal Data to the Services and to instruct us to process it as described in this Privacy Policy. We are entitled to rely on that warranty without independent verification.

4.5 Lawfulness of instructions. You warrant that your instructions to us in respect of Customer Data are lawful. Where we reasonably consider that an instruction infringes Applicable Data Protection Law, we may notify you and suspend performance of that instruction until it is confirmed, amended or withdrawn, without liability to you for the suspension.

5. OUR ROLE AND ITS LIMITS

5.1 What we do. In relation to Customer Data, our role is limited to owning, hosting and technically operating the platform and the website; providing and maintaining the technical and cloud infrastructure on which the Services run; maintaining the hosting environment, including configuration, patching, monitoring and technical administration; ensuring the availability, uptime, continuity and infrastructure-level security of the Services; processing Customer Data to generate the outputs you request or configure; and providing technical support, onboarding, migration and integration assistance.

5.2 What we do not do. We do not independently determine or influence what Personal Data you collect, the lawful basis or purposes you rely upon, or the notices and consents you issue. We do not supervise, monitor, validate or control your business operations, professional engagements, client interactions, communications or transactions conducted through the Services. We do not exercise professional judgment and do not provide accounting, audit, assurance, attest, tax, bookkeeping, legal or other professional advice in respect of Customer Data or any output generated through the Services.

5.3 Effect. Nothing in this Clause reduces the obligations we owe as a processor under applicable data protection law or under any Data Processing Addendum executed with you, and nothing in this Clause excludes or limits any liability that cannot lawfully be excluded or limited.

6. PERSONAL DATA WE COLLECT

6.1 Account and organisation data. Name, username, business e-mail address, telephone number, job title, organisation name and business address, account credentials and authentication data, profile details, contact preferences, subscription and licensing details, billing information, administrator and Authorised User records, and account configuration settings, together with records of consent, preference and opt-out settings.

6.2 Customer Data. Documents, spreadsheets, accounting and bookkeeping records, financial statements, ledgers, transaction and bank data, tax and sales tax records and returns, audit and assurance workpapers, review notes, risk assessments, audit evidence, engagement files, invoices, receipts, reports, correspondence and other materials submitted to or generated through the Services. Customer Data may contain Personal Data relating to the Customer's Authorised Users, personnel, clients and other individuals whose affairs the Customer administers. We process Personal Data contained in Customer Data solely as a Data Processor, as described in this Privacy Policy.

6.3 Technical and usage data. IP address, browser type and settings, operating system, device identifiers, language and time zone settings, pages and features accessed, dates and times of access, referring URLs, session data, diagnostic data and system and audit logs. This data is collected automatically and is used for authentication, security, availability monitoring, troubleshooting and service improvement.

6.4 Communications data. Information contained in enquiries, support requests, incident tickets, feedback and survey responses, and other correspondence exchanged with us by e-mail, telephone, chat or ticketing system.

6.5 Sensitive and regulated data. The Services are not designed to collect special categories of Personal Data directly from individuals. Customer Data uploaded by you may nonetheless contain sensitive, confidential or regulated information, including financial account details and tax identification numbers. Any such data is processed solely as processor, on your instructions, and you are responsible for ensuring you are entitled to upload it, for obtaining any explicit or opt-in consent required for it, and for observing any additional requirements that apply to it.

6.6 Data from other sources. For data in respect of which we act as controller, we may obtain business contact details from public sources, business directories, referral partners, event and webinar registrations and professional social media platforms, limited to name, job title, organisation, business contact details and records of interaction with us.

6.7 Sources of collection. We collect Personal Data directly from Customers, Authorised Users and website visitors; automatically through access to or use of the Services; from Customers that upload Customer Data containing Personal Data relating to other individuals; from Customer-

Enabled Integration connected by a Customer, to the extent of the permissions granted; and from the other sources described in this Privacy Policy.

6.8 Provision of data. Where processing is necessary for the performance of a contract with you or is required by law, a failure to provide the Personal Data requested may prevent us from providing all or part of the Services. Provision of Personal Data for marketing purposes is optional and refusal has no effect on the Services.

7. HOW WE USE PERSONAL DATA

We use Personal Data only for the following purposes:

(a) to create, administer, authenticate and secure accounts and to enable the features and functionality of the Services;

(b) to deliver the modules you use, including customer relationship management, practice management, bookkeeping and accounting, tax and sales and use tax, audit and assurance, and document management;

(c) to administer subscriptions, issue invoices and process payments;

(d) to operate, maintain, monitor, troubleshoot, secure and improve the Services, using aggregated or de-identified data wherever identifiable data is not required;

(e) to provide support, respond to enquiries, resolve service issues and assist with onboarding, migration and integration;

(f) to send administrative, transactional, security, billing and service communications, and, where we have a lawful basis, marketing communications from which you may opt out at any time;

(g) to authenticate Authorised Users, secure Customer accounts, detect and prevent unauthorised access, fraud and misuse, maintain audit logs and enforce our agreements;

(h) to comply with applicable law and regulatory or professional obligations and to establish, exercise or defend legal claims;

(i) to obtain, record, evidence and give effect to consents, preferences, opt-outs and withdrawal requests; and

(j) to develop, test and improve the Services, in which case we use Aggregated Data or De-identified Data only.

We do not use Personal Data for any purpose that is incompatible with those set out above, and we do not use Customer Data for any purpose other than providing the Services to the Customer that submitted it. We do not carry out any decision-making producing legal effects concerning an individual, or similarly significantly affecting them, based solely on automated processing, and we do not profile individuals for advertising purposes.

8. HOW WE PROCESS CUSTOMER DATA

In processing Customer Data as processor, we undertake that we may:

(a) process Customer Data only on your documented instructions, including as to any transfer of that data, unless required to act otherwise by law, in which case we will inform you unless prohibited from doing so;

(b) process Customer Data only for the purpose of providing, supporting and securing the Services and producing the outputs you request, and for no purpose of our own;

(c) ensure that our personnel authorised to access Customer Data are bound by confidentiality obligations and are granted access only on a least-privilege basis;

(d) implement and maintain the technical and organisational security measures stated under the heading Data Security;

(e) engage Sub-processors only under written contracts imposing data-protection obligations materially no less protective than those to which we are subject, and remain responsible to you for their performance;

(f) provide you with reasonable assistance in responding to requests from individuals exercising their rights, in carrying out data protection impact assessments, and in meeting your own security and notification obligations, taking into account the nature of the processing and the information available to us;

(g) notify you without undue delay on becoming aware of a security incident affecting Customer Data;

(h) delete or return Customer Data as stated under the heading Data Retention and Deletion on termination; and

(i) make available to you the information reasonably necessary to demonstrate compliance with these obligations, as further provided in the applicable Data Processing Addendum;

(j) not sell or share Customer Data, and not combine it with Personal Data received from or on behalf of any other person, except as expressly permitted by law; and

(k) make available our then-current audit reports, certifications and security documentation and, where Applicable Data Protection Law so requires, permit an audit not more than once in any twelve (12) month period, on not less than thirty (30) days' written notice, during business hours, subject to confidentiality undertakings, at your cost, and conducted so as not to disrupt the Services or compromise the confidentiality of other Customers' data.

9. CONSENT

9.1 The Customer obtain consent for Customer Data. The Services work only on the data you provide to us. We do not collect that data from the people it concerns and have no relationship with them. So, before you upload Personal Data, you must give the required notices and obtain and keep evidence of every consent the law requires. That includes valid consent to our processing, storage, transfer and disclosure of the data as described in this Privacy Policy, consent to the use of AI Features on it, and any parental or guardian consent needed. You must produce that evidence to us on request. We rely on your confirmation that consent is held other than where specifically required by law. We are not responsible if a consent is missing, invalid, expired or withdrawn.

9.2 Consent obtained by us. Where we act as controller and applicable law requires consent, we obtain it before the relevant processing begins. This applies principally to non-essential cookies and similar technologies and to marketing communications. Consent is requested separately from any other term, by a clear affirmative action, and is accompanied by a plain-language notice stating the data concerned, the purpose, and the means of withdrawal. We do not rely on pre-ticked boxes, silence, inactivity, bundled consent or continued use of the Services as consent.

9.3 Withdrawal. Consent may be withdrawn at any time, by a method as easy to use as that by which it was given, through the in-product privacy settings, the unsubscribe mechanism in a communication, our cookie consent tool, or by writing to us at [insert privacy e-mail address].

Withdrawal takes effect prospectively and does not affect the lawfulness of processing carried out before it. Following withdrawal, we will cease the relevant processing and, where no other lawful basis applies, erase the Personal Data concerned. Withdrawal may prevent us from providing the feature or communication to which the consent related, and any consequence of withdrawal is borne by the Authorised User or the Customer.

9.4 Records. We maintain records of the consents we obtain for so long as necessary to demonstrate compliance and to establish, exercise or defend legal claims. You are responsible for maintaining equivalent records in respect of the consents you obtain.

9.5 Consent under the GDPR and the UK GDPR. Where the GDPR or the UK GDPR applies, we rely on consent as per the applicable law. That means it is freely given, specific, informed and unambiguous, given by a clear affirmative act, recorded, kept separate from other terms, written in plain language, and as easy to withdraw as it was to give. We do not rely on consent where there is a clear imbalance between the parties, and we do not make a service conditional on consent we do not need. We obtain explicit consent under applicable law before relying on consent to process special category data.

9.6 U.S. State Privacy Laws. Requirements relating to consent and individual privacy choices vary under applicable U.S. state privacy laws. We obtain consent and give effect to applicable choices, restrictions and withdrawal requests to the extent required by those laws. For Personal Data contained in Customer Data, the Customer is responsible for providing required notices, obtaining and maintaining any necessary consents, and communicating relevant requests or instructions to us. We process such data in accordance with the Customer's lawful documented instructions and the applicable DPA, subject to our own obligations under applicable law.

10. ARTIFICIAL INTELLIGENCE FEATURES AND NO MODEL TRAINING

10.1 AI functionality. Certain features of the Services use artificial intelligence to assist with drafting, summarisation, document analysis, data extraction and classification, reconciliation support, search, recommendations and workflow automation ("AI Features"). AI Features may be enabled by default or made available as configurable functionality that an administrator may enable or disable, as described in the applicable product documentation and administrative settings.

10.2 Data minimisation. Where an AI Feature is used, we transmit only the data necessary to process the request, being the prompt, the selected text or the document intentionally submitted through that feature. Transmissions to AI providers are encrypted in transit, and we apply commercially reasonable measures to limit the data disclosed to what is necessary to deliver the requested functionality.

10.3 No training on Customer data. We do not use Customer Data or Personal Data processed through the Services to train, re-train, fine-tune, develop, benchmark or otherwise improve any artificial intelligence model, machine learning model, large language model or algorithm, whether our own or that of any third party. Our written contracts with third-party AI providers require that data transmitted through the Services is not used to train or improve their models, and we will not knowingly engage an AI provider on terms that do not contain that restriction. Where available, we use enterprise-tier AI services configured so that submitted content is not retained beyond the period necessary to process the request, save for any short-term retention applied by a provider solely for security or abuse-monitoring purposes and subject to that provider's confidentiality and security obligations.

10.4 No use for our own benefit. We do not use Customer Data, or any output generated from it by an AI Feature, for our own commercial benefit, for the benefit of any other Customer, or for any purpose other than delivering the requested functionality to the Customer that submitted it.

10.5 Nature of AI output. Output generated by AI Features is produced automatically and may be incomplete, inaccurate or unsuitable for a particular purpose. It does not constitute accounting, audit, assurance, attest, tax, bookkeeping, financial, legal or other professional advice and must not be relied upon as such. AI Features assist, and do not replace, professional judgment. You remain solely responsible for reviewing, verifying and approving all AI output and for every professional judgment, deliverable, filing, return and conclusion you issue. To the fullest extent permitted by law, we accept no liability for any loss, damage, penalty or regulatory consequence arising from the use of, or reliance on, AI output.

10.6 Human oversight and control. AI Features are decision-support tools only, and no AI Feature makes a decision producing legal or similarly significant effects concerning an individual without human review and approval by you. Where an AI Feature is configurable, your administrator may disable it at account level at any time.

11. SUB-PROCESSORS, CUSTOMER-ENABLED INTEGRATIONS AND INDEPENDENT THIRD-PARTY SERVICES

11.1 Sub-processors engaged by us. We engage Sub-processors to provide hosting, storage, artificial intelligence functionality, authentication, monitoring, security, technical support, payment processing and other infrastructure or operational services necessary to provide the Services. Sub-processors process Customer Data on our behalf and under our instructions. Each Sub-processor is engaged as per the terms that restricts its processing to the relevant services, imposes appropriate confidentiality, security, breach-notification, deletion and data-protection obligations, and prohibits the sale or sharing of Customer Data except as expressly permitted by Applicable Data Protection Law. We remain responsible to the Customer for the performance of our Sub-processors to the extent required by Applicable Data Protection Law.

Our current Sub-processors include **Amazon Web Services ("AWS")** for cloud hosting, storage and processing in the United States, and OpenAI where AI Features are used. We also use authentication, analytics, monitoring, security and support providers identified in our current Sub-processor list. Stripe processes subscription and payment information; complete payment-card details are collected and stored by **Stripe** and are not received or stored by us. To the extent Stripe processes Personal Data solely on our behalf, it acts as our Sub-processor. To the extent Stripe determines its own purposes for processing, including for legal, regulatory, fraud-prevention or security purposes, its processing is governed by its own privacy notice.

11.2 Customer-Enabled Integrations. A Customer or an Authorised User with appropriate account permissions may choose to connect the Services to Customer-Enabled Integrations, including Gmail, Microsoft Outlook, Calendly, MYCPE ONE, Karbon, TaxDome and Canopy. These integrations may be used to synchronise e-mail, contact and calendar information, schedule appointments, or import, export or migrate records, documents, engagements, workflow data and Authorised User profiles.

A Customer-Enabled Integration is activated only when the Customer or its appropriately authorised user enables the integration, grants the requested permissions, completes the applicable authorisation process or otherwise instructs us to connect it. That action constitutes the Customer's documented instruction to us to transmit or receive the relevant Customer Data. We exchange

Customer Data only to the extent permitted by the authorisation granted and reasonably necessary to provide the requested integration functionality.

11.3 Governed by their own terms. Each Sub-processor is engaged contractually and operates its services under its applicable terms, privacy policies and security standards, which we accept. Those terms do not reduce its obligations under our agreement, any applicable Data Processing Addendum or Applicable Data Protection Law. We remain responsible for our Sub-processors to the extent required by law and the applicable Data Processing Addendum.

The Services may also contain links or references to independent third-party websites, applications or services that are neither Sub-processors nor Customer-Enabled Integrations. We do not control those third parties, and their own terms and privacy notices govern any Personal Data provided directly to them.

11.4 Customer instructions, lawful basis and consent. Acceptance of our Terms of Service alone does not activate an optional Customer-Enabled Integration or constitute consent to the independent processing carried out by its provider. The Customer is responsible for connecting only accounts it is authorised to use and for ensuring that it has provided all required notices and holds a valid lawful basis and, where specifically required by Applicable Data Protection Law, valid consent for the disclosure of Personal Data through a Customer-Enabled Integration.

11.5 Changes. We may add or replace sub-processors from time to time. Where an applicable Data Processing Addendum so requires, we will give notice of material changes and afford the objection rights set out in that agreement. A current list of sub-processors is available on request at info@assureone.ai. Where you object to a new sub-processor on reasonable data protection grounds, we will use reasonable endeavours to make available an alternative or a change in configuration; if we are unable to do so within a reasonable period, you may terminate the affected subscription in accordance with the Terms of Service.

12. DISCLOSURE OF PERSONAL DATA

We disclose Personal Data only:

(a) to the service providers and sub-processors stated in this Privacy Policy, for the purposes described there;

(b) to Authorised Users, in accordance with the access permissions you configure;

(c) to Customer-Enabled Integration connected at your election, to the extent of the permissions granted;

(d) to our affiliates and to professional advisers, auditors and insurers, under confidentiality obligations, where necessary for the administration of our business;

(e) where required by law, regulation, court order, subpoena or lawful request of a competent authority, or where necessary to establish, exercise or defend legal claims, enforce our agreements, or protect the rights, property or safety of the Company, our Customers or others;

(f) in connection with a merger, acquisition, financing or reorganisation, or a sale or transfer of all or part of our business or assets, subject to the recipient being bound by obligations materially no less protective than those in this Privacy Policy; and

(g) with the consent of the individual concerned or at your documented direction.

Where we receive a binding legal demand for Customer Data, we will, unless legally prohibited from doing so, notify you before disclosure so that you may seek protective relief, challenge or seek to narrow any demand that appears unlawful or overbroad, seek to redirect the demand to you as data controller, and disclose only the minimum data necessary to comply.

13. NO SALE AND NO COMMERCIAL EXPLOITATION

13.1 No sale. We do not sell Personal Data for monetary or other valuable consideration, and we do not share Personal Data for cross-context behavioural advertising or targeted advertising, in each case within the meaning of the CCPA and other Applicable Data Protection Law. We have not sold or shared Personal Data in the twelve (12) months preceding the date of this Privacy Policy, and we do not sell or share the Personal Data of any individual we know to be under sixteen (16) years of age.

13.2 No exploitation. We do not sell, rent, licence, lease, publish, mine, monetise or otherwise exploit Customer Data or Personal Data processed through the Services for our own commercial benefit or that of any third party. We do not use Customer Data to build, populate or enrich any marketing database, data product, lead-generation service, benchmarking product or advertising service, and we do not disclose Customer Data to any other Customer.

13.3 Aggregated data. We may generate and use aggregated, statistical and de-identified data derived from use of the Services to operate, secure, support and improve them. Such data is maintained so that it does not identify, and cannot reasonably be used to identify, any individual or Customer, and we do not attempt to re-identify it. We contractually prohibit any recipient of it from attempting re-identification.

13.4 No financial incentives. We do not offer any financial incentive, price difference or service difference in exchange for the retention, sale or sharing of Personal Data.

14. COOKIES, SIMILAR TECHNOLOGIES AND OPT-OUT SIGNALS

14.1 What we use. We use cookies, pixels, local storage, log files and similar technologies to authenticate users, maintain sessions, remember preferences, operate and secure the platform, analyse usage and improve performance. These technologies may collect device identifiers, browser type, operating system, IP address, pages visited, referring URLs, session data and usage statistics. We do not use advertising or cross-context behavioural advertising cookies on the Services.

14.2 Consent and control. Where required by law, non-essential cookies are set only with consent obtained through our cookie consent mechanism, and you may withdraw consent or change your preferences at any time through that mechanism or through your browser or device settings. Restricting cookies may limit the functionality of parts of the Services.

14.3 Opt-out preference signals. Where applicable law requires us to do so, including under the CCPA and the comparable statutes of other States of the United States, we recognise and honour opt-out preference signals, including the Global Privacy Control, transmitted by your browser, device or extension, and treat such a signal as a valid request to opt out of the sale or sharing of Personal Data and of processing for targeted advertising in respect of that browser or device. Because no common standard exists for the interpretation of legacy “Do Not Track” browser signals, the Services do not respond to them.

14.4 Third-party technologies. Third-party providers whose content or features are made available through the Services may use their own technologies, which we do not control and which are governed by their own privacy policies.

15. HOSTING, STORAGE AND INTERNATIONAL TRANSFERS

15.1 Cloud hosting. The Services are hosted, stored and processed on secure cloud infrastructure operated by AWS and located in the United States. Backup, disaster recovery and business continuity copies are held in encrypted, access-controlled storage within that environment. Customer Data is logically segregated by account so that it is accessible only to the Users you authorise and to authorised personnel and sub-processors who require access to operate, support or secure the Services, on a need-to-know and least-privilege basis.

15.2 Transfers. Personal Data may be transferred to, stored in and accessed from countries other than the country in which it was collected, including the United States where data protection laws may differ. Where applicable law requires a transfer mechanism or safeguard, we put in place the mechanism recognised under that law before the transfer is made, which, for Personal Data originating in the European Economic Area, the United Kingdom or Switzerland, means the Standard Contractual Clauses approved by the European Commission, the UK International Data Transfer Agreement or Addendum, or such other mechanism as is then recognised under the GDPR or the UK GDPR, supported by a transfer impact assessment, and support it with technical and organisational measures including encryption in transit and at rest and least-privilege access control. Details of the mechanism applicable to a particular transfer, subject to necessary redactions, are available to Customers and their Authorised Users on request at info@assureone.ai. We do not transfer Personal Data to any country or recipient where applicable law prohibits or restricts that transfer.

15.3 Your instruction. By subscribing to the Services and uploading Customer Data, you instruct us to host, store, access and process that data in the locations described above. Where an individual's consent to an international transfer is required, it must be obtained by you before the data is uploaded. Where we make a material change to the countries in which Customer Data is hosted, we will give reasonable prior notice to the account administrator.

16. LAWFUL BASIS FOR PROCESSING

Where required by applicable data protection law, including the EU General Data Protection Regulation and the UK General Data Protection Regulation and, as to notice and choice, the CCPA, we process Personal Data only where a lawful basis exists. We rely on:

(a) performance of a contract, where processing is necessary to provide, administer and support the Services, or to take steps at your request before entering into a contract;

(b) legitimate interests, where processing is necessary to operate, maintain, secure and improve the Services, prevent fraud and misuse, administer our business and communicate with business contacts, provided those interests are not overridden by the rights and freedoms of the individuals concerned;

(c) compliance with a legal obligation, where processing is required by law, regulation, court order or lawful request of a competent authority;

(d) consent, where given for a specific activity as stated under the heading Consent, which may be withdrawn at any time without affecting the lawfulness of processing carried out before withdrawal; and

(e) protection of vital interests, in exceptional circumstances.

Where we act as processor in respect of Customer Data, the lawful basis for that processing is determined and maintained by the Customer as data controller as stated in this Privacy Policy.

17. PRIVACY RIGHTS AND HOW TO EXERCISE THEM

17.1 Rights. Subject to applicable data protection law, individuals have the following rights in respect of their Personal Data: the right to be informed how their data is processed; the right of access to a copy of their data; the right to rectification of inaccurate or incomplete data; the right to erasure; the right to restrict processing; the right to object to processing carried out on the basis of legitimate interests or for direct marketing; the right to data portability; the right to withdraw consent where processing is based on consent; the right not to be subject to a decision producing legal or similarly significant effects based solely on automated processing; the right, where applicable law so provides, to limit the use and disclosure of sensitive personal information, to appeal a refusal to act on a request, and not to be discriminated against for exercising a right; and the right to lodge a complaint with a competent supervisory authority. These rights apply only in the circumstances defined by law and are subject to statutory exemptions and the rights of others.

17.2 Requests concerning Customer Data. Where Personal Data is contained in Customer Data, the Customer is the data controller of that data. Requests to access, correct, delete, port, restrict or object to the processing of such data must therefore be made to that Customer. We have no

authority to act on such a request unless and until formally instructed to do so by the Customer, and we will not respond directly to it except where required by law or expressly authorised in writing by the Customer. Where we receive such a request directly, we will, where practicable and permitted, refer it to the relevant Customer and give that Customer reasonable assistance in responding.

17.3 Requests concerning data we control. For Personal Data in respect of which we act as controller, requests may be made to us at info@assureone.ai. We may request further information to verify identity or the authority of any agent acting on an individual's behalf before responding, and we will respond within the period required by applicable law. We do not charge for responding to a request unless it is manifestly unfounded, excessive or repetitive, in which case we will explain the reason and provide an estimate before proceeding. Where we are unable to verify identity to the standard required by law, we may decline to act, and will explain why. Where applicable law provides a right of appeal against a refusal, we will notify the individual of that right and of the means of exercising it.

17.4 Marketing. You may opt out of marketing communications at any time using the unsubscribe mechanism in the communication or by contacting us. Opting out does not affect administrative, transactional, billing or security communications relating to an active account.

17.5 Complaints. An individual who is dissatisfied with our handling of Personal Data may complain to us at info@assureone.ai and has the right to complain to the supervisory or regulatory authority competent in their jurisdiction.

18. APPLICABLE PRIVACY LAWS AND INDIVIDUAL RIGHTS

We process Personal Data in accordance with Applicable Data Protection Law to the extent it applies to our processing activities. Depending on their location and the applicable law, individuals may have rights concerning their Personal Data, subject to applicable conditions, exemptions and limitations. Requests may be submitted to info@assureone.ai. We may verify the requester's identity and authority where permitted and will respond within the period required by applicable law. Requests may be declined or restricted where legally permitted, with reasons and information about available appeal or complaint mechanisms where required.

Where we process Customer Data on behalf of a Customer, the Customer is responsible for addressing individual requests and providing required notices, consents and choices. We will refer such requests to the relevant Customer and provide assistance as required by applicable law and the applicable DPA. We implement transfer safeguards and provide regulatory or individual notifications where legally required. Nothing in this Clause creates rights or obligations beyond those imposed by applicable law or expressly agreed in the applicable DPA or limits any mandatory right or obligation.

21. DATA RETENTION AND DELETION

21.1 General. We retain Personal Data only for as long as reasonably necessary to provide the Services, fulfil the purposes described in this Privacy Policy, comply with legal, accounting, tax and regulatory obligations, resolve disputes and enforce our agreements. During the term of your subscription, Customer Data is retained in accordance with your configuration and instructions, and you may delete, export or amend it at any time using the functionality available within the Services.

21.2 Retrieval and deletion on termination. On termination or expiry of your subscription, you may retrieve and export your Customer Data for a period of thirty (30) days from the effective date of termination. Following the expiry of that thirty (30) day retrieval period, we will permanently delete Customer Data from our production systems within thirty (30) days, unless retention is required by law as stated below. Residual copies held in encrypted, access-controlled backup systems are deleted in the ordinary course of backup rotation and, in any event, no later than ninety (90) days, and are not restored to active use except in the course of disaster recovery, following which deletion is re-applied. Where deletion within these periods is technically impracticable, we will isolate the data, cease active processing of it and delete it as soon as reasonably practicable.

21.3 Retention required by law. We may retain data where required by law, regulation, professional obligation or legal hold, or where necessary to establish, exercise or defend legal claims. Data so retained remains subject to the confidentiality, security and processing restrictions set out in this Privacy Policy and in the applicable agreement, and is deleted once the requirement lapses.

21.4 Deleted data and aggregated data. Data deleted from the Services may remain in secure backups, archives or audit logs for the limited period described above before being deleted, anonymised or securely destroyed. Aggregated and de-identified data that does not identify any Authorised User or Customer may be retained and used as stated in this Privacy Policy.

21.5 How we set retention periods. Where no fixed period is stated, we decide how long to keep data by looking at how sensitive it is, the harm that misuse could cause, why we hold it, how long the subscription and any later limitation period run, and what the law requires.

22. DATA SECURITY

22.1 Measures. We maintain administrative, technical, physical and organisational safeguards designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, misuse and unauthorised access, having regard to the nature and sensitivity of the data and the risks to the individuals concerned. Our measures include encryption of data in transit (currently TLS 1.2 or higher) and at rest (currently AES-256), which we may replace with equivalent or stronger standards; multi-factor authentication; role-based, least-privilege access controls; identity and access management; network and infrastructure security; logging, alerting and continuous monitoring; vulnerability assessment and remediation; patch and change management; secure development practices; personnel screening, confidentiality undertakings and security training; backup, disaster recovery and business continuity procedures; and vendor security assessment. Our security programme is aligned with recognised industry frameworks, including ESOF, SOC 2 Type 1 and ISO/IEC 27001. Any certification or framework referred to is stated as at the date of this Privacy Policy and is not a warranty of continued certification or of any particular security outcome.

22.2 Access control. Access to Personal Data is restricted to authorised personnel and sub-processors who require it to perform their roles and is subject to confidentiality and security obligations.

22.3 Your responsibilities. Accounts are protected by credentials that you are responsible for keeping confidential. You are responsible for all activity conducted under your credentials and for managing and revoking access within your account, for enabling and enforcing multi-factor authentication where made available, and for the security of the devices, networks and systems

from which the Services are accessed. Suspected compromise of any credential should be reported to us immediately at info@assureone.ai.

22.4 No absolute security. No method of transmission over the Internet or of electronic storage is completely secure. While we apply commercially reasonable measures, we cannot guarantee absolute security, and data is transmitted to and from the Services at your own risk.

22.5 Security documentation. Our then-current security documentation, penetration test summaries and audit reports are available to Customer or its Authorised User on request, on a need-to-know basis, subject to execution of a confidentiality undertaking and to reasonable redaction.

23. SECURITY INCIDENTS

If we become aware of a Security Incident, being a security incident affecting Personal Data within our environment, we will promptly investigate, take appropriate steps to contain, mitigate and remediate it, and, where the incident affects Customer Data, notify the affected Customer without undue delay so that the Customer, as data controller, may assess its own notification obligations. We will provide the information reasonably available to us and reasonable assistance in meeting those obligations. Where we act as controller, we will notify affected individuals and competent supervisory authorities to the extent, in the manner and within the time required by law, and, where the GDPR or the UK GDPR applies, within seventy-two (72) hours of becoming aware of a notifiable personal data breach. Where we act as processor, responsibility for notifying individuals and supervisory authorities rests with the Customer as data controller, and we will not make such notifications on your behalf unless instructed in writing or required by law. We are not responsible for incidents originating from your own systems, personnel, credentials, access configuration or connected third-party service provider, save to the extent that responsibility cannot lawfully be excluded. Notification of a Security Incident, and any assistance or remediation provided by us, is not an acknowledgement of fault, liability or breach of contract on our part.

24. CHILDREN AND DATA COLLECTION

The Services are intended for business and professional use and are not directed to children. Individuals under the age of 18 may not register for or use the Services, and we do not knowingly collect Personal Data directly from them. If we become aware that we have done so without the

required parental or guardian consent, we will delete that data as soon as practicable, and a parent or guardian may request deletion by writing to info@assureone.ai. Where Customer Data uploaded by a Customer or its Authorised User contains information relating to a minor, we process that information solely as processor on that Customer's instructions and do not collect it directly from the individual concerned, and the Customer is responsible for obtaining and verifying any parental or guardian consent required in respect of it.

25. THIRD-PARTY WEBSITES

The Services may link to or integrate with third-party websites, applications or services that we do not own or control. This Privacy Policy does not apply to them, and we do not endorse, supervise or assume responsibility for their content, security or data practices. You should review their privacy policies before providing them with Personal Data.

26. DISCLAIMERS AND LIMITATION OF LIABILITY

26.1 Customer data practices. To the fullest extent permitted by law, we disclaim all liability arising out of or in connection with: (a) your data collection, processing, disclosure, retention or deletion practices; (b) the existence, adequacy or lawfulness of your privacy notices, consents, lawful bases or data protection compliance; (c) the accuracy, completeness, legality or provenance of Customer Data; (d) any unauthorised access to, breach, loss, misuse or exposure of Personal Data arising from your own systems, personnel, contractors, vendors, credentials, access permissions, misconfiguration or failure to implement appropriate controls; (e) the acts, omissions or data practices of any Customer-Enabled Integration connected to the Services at your election; (f) any professional accounting, audit, assurance, attest, tax, sales tax, bookkeeping or advisory judgment, deliverable, filing, return or conclusion made or issued by you or relied upon by those you serve; and (g) any loss or consequence arising from the absence, invalidity, expiry or withdrawal of a consent that you were responsible for obtaining.

26.2 Allocation of responsibility. We do not supervise, monitor, validate or control any Customer-managed business operation, professional engagement, communication or transaction conducted through the Services. All responsibilities, obligations and liabilities relating to the handling of Personal Data contained in Customer Data, including compliance with applicable data protection law, remain the Customer's responsibility, except for the obligations expressly imposed on the

Company as Data Processor under Applicable Data Protection Law. We are not liable for any claim, loss, damage, penalty, fine or regulatory action arising from your acts, omissions, non-compliance or misuse of the Services or of any Customer-Enabled Integration. The Company shall assist where its assistance is required by law.

26.3 No individual liability. The Services are provided by AssureOne Technologies LLC, a limited liability company. No director, officer, member, manager, shareholder, employee, contractor, consultant, agent or affiliate of the Company bears any personal or individual liability to any Customer, individual or other person in respect of the processing of Personal Data under this Privacy Policy or the operation of the Services. Any claim relating to Personal Data processed through the Services lies solely against AssureOne Technologies LLC as an entity.

26.4 No agency. Nothing in this Privacy Policy creates any partnership, agency, joint venture, fiduciary, employment or representative relationship between the Company and any Customer or other person. We do not endorse or assume responsibility for any representation, content, communication or business activity undertaken by a Customer through the Services.

26.5 Other agreements. Nothing in this Privacy Policy limits, extends or modifies the warranties, disclaimers, exclusions, indemnities, limitations of liability or remedies set out in the Terms of Service, any Data Processing Addendum or any other written agreement between you and the Company, which govern the allocation of liability between the parties. Nothing in this Privacy Policy excludes or limits any liability that cannot lawfully be excluded or limited.

26.6 Cap on liability. To the fullest extent permitted by law, our aggregate liability arising out of or in connection with the subject matter of this Privacy Policy is subject to, and does not exceed, the limitations, exclusions and aggregate cap on liability set out in the Terms of Service and any applicable Data Processing Addendum. We are not liable for any indirect, incidental, special, consequential, exemplary or punitive loss, or for loss of profit, revenue, goodwill, business, anticipated savings or data, however arising.

26.7 No warranty of compliance. This Privacy Policy is not legal advice and is not a representation, warranty or guarantee that your use of the Services will render you compliant with any law, professional standard or regulatory requirement applicable to you. You are responsible for obtaining your own legal and compliance advice.

27. INDEMNITY

27.1 Indemnity. You will indemnify AssureOne Technologies LLC and its affiliates, officers, employees and agents against all claims, proceedings, investigations, losses, fines, penalties and reasonable legal costs arising from: (a) your breach of your responsibilities as data controller or of your consent obligations under this Privacy Policy; (b) a notice or consent you were responsible for that is missing, invalid, expired or withdrawn; (c) an instruction from you that breaks data protection law; (d) the content, accuracy or legality of Customer Data; (e) a Security Incident starting in your systems, staff, credentials or access settings; and (f) the acts or omissions of a Customer-Enabled Integration you connect.

27.2 Conduct of claims. We will notify you of any claim to which this indemnity applies, will not settle it without your prior written consent (not to be unreasonably withheld or delayed), and will give you reasonable assistance at your cost. We reserve the right to control the defence of any claim that concerns our own compliance posture, regulatory standing or the security of the Services.

28. COMPLIANCE WITH APPLICABLE LAW

We process Personal Data in accordance with applicable data protection law, including the EU General Data Protection Regulation and the UK General Data Protection Regulation to the extent they apply to our processing activities, the CCPA and the comparable statutes of other States of the United States to the extent they apply to our processing activities, together with such other data protection and privacy laws as apply to us in the jurisdictions in which we operate and in which the Services are made available. Where we act as processor, we process Customer Data in accordance with your documented instructions and the applicable Data Processing Addendum. We review and update our privacy practices as the Services develop and as legal requirements change.

Where the law of a particular jurisdiction requires a disclosure, notice, right or mechanism additional to those described in this Privacy Policy, we provide it to the extent, and in the manner, that law requires. Details of the additional disclosures applicable to a particular jurisdiction are available to the persons entitled to them on request at info@assureone.ai. A statement that a particular law applies to our processing is not an admission that it applies to yours, or that it applies to any processing beyond that described in this Privacy Policy.

29. GOVERNING LAW, DISPUTES AND NO PRIVATE RIGHT OF ACTION

29.1 Governing law. This Privacy Policy, and any dispute or claim arising out of or in connection with it or its subject matter, is governed by the laws of the State of Delaware, United States, without regard to its conflict of laws principles, and is subject to the dispute resolution provisions of the Terms of Service.

29.2 Mandatory rights preserved. The preceding sub-clause does not deprive any individual of the protection of, or of any remedy under, the mandatory provisions of the law applicable to them, including the right to lodge a complaint with a competent supervisory authority.

29.3 Contractual Enforcement and No Third-Party Rights. As between the Company and a Customer, this Privacy Policy forms part of, and is enforceable in accordance with, the Terms of Service and any applicable Data Processing Addendum. Any dispute or claim between the Company and a Customer arising out of or relating to this Privacy Policy shall be subject to the dispute-resolution provisions, limitations of liability and remedies set out in those agreements. This Privacy Policy does not create any independent cause of action separate from a right arising under Applicable Data Protection Law, the Terms of Service or an applicable Data Processing Addendum and does not confer any third-party beneficiary rights on any person. Nothing in this Clause limits or waives any right, remedy or cause of action that cannot lawfully be limited or waived under Applicable Data Protection Law.

30. GENERAL

30.1 Severability. If any provision of this Privacy Policy is held to be invalid, illegal or unenforceable in any jurisdiction, that provision is severed to the minimum extent necessary and the remainder continues in full force and effect, and the validity of that provision in any other jurisdiction is unaffected.

30.2 No waiver. No failure or delay in exercising any right under this Privacy Policy operates as a waiver of it, and no single or partial exercise precludes any further exercise.

30.3 Survival. The provisions of this Privacy Policy under the headings Your Responsibilities as Data Controller, Consent, Data Retention and Deletion, Disclaimers and Limitation of Liability, Indemnity, Governing Law, Disputes and No Private Right of Action, and General survive the termination or expiry of your subscription.

30.4 Order of precedence. In the event of any conflict, the following order of precedence applies: the Data Processing Addendum or any signed addendum, in respect of the processing of Customer Data; then the Terms of Service; then this Privacy Policy.

30.5 Headings and language. Headings are for convenience only and do not affect construction. This Privacy Policy is made in the English language, and in the event of any inconsistency with a translation, the English version prevails, save where applicable law requires otherwise.

30.6 Assignment. We may assign or transfer our rights and obligations under this Privacy Policy in connection with a merger, acquisition, financing, reorganisation or sale or transfer of all or part of our business or assets. You may not assign your rights under this Privacy Policy without our prior written consent.

31. UPDATES TO THIS PRIVACY POLICY

The Company may update this Privacy Policy from time to time, and you should take the time to review it each time you visit or use the Services. Where we make material changes, we will update the "Effective Date" and "Last Updated" dates at the beginning of this Privacy Policy and, where required by law or contract, give notice through the Services or by other appropriate means. The current version is available at https://assureone.ai/ and governs our processing of Personal Data from its effective date. Continued use of the Services after an updated Privacy Policy takes effect constitutes acknowledgement of it. If a change significantly reduces anyone's rights or widens why we use Personal Data, we will give at least 30 days' notice first and, where the law requires it, ask for fresh consent instead of relying on continued use. Earlier versions are available on request.

32. CONTACT US

For any question, request or concern regarding this Privacy Policy or our privacy practices, please contact us at:

AssureOne Technologies LLC

AssureOne

Address: 16192 Coastal Highway, Lewes, Delaware 19958

E-mail: info@assureone.ai

Telephone: 19843712869

Privacy Contact / Data Protection Officer: Saul Sony, saul@assureone.ai