oneSaaS

Software-as-a-Service, Cloud Services Agreement

Cover Page

The **Agreement** comprises of the contents in this **Cover Page**, including **Key Terms** and **Supplemental Documentation** (if any). By executing this Cover Page, the **Parties** enter into an Agreement which incorporates the oneSaaS **Standard Terms** (available at lawinsider.com/standards/onesaas) by reference. Capitalized terms that are not defined in this Cover Page will have the meanings given in the oneSaaS Standard Terms.

KEY TERMS

1. GENERAL TERMS

Contractual Term	Definition
Agreement Start Date	[Insert Agreement Start Date]
Governing Law	This agreement, and any dispute, controversy, proceedings or claim of whatever nature arising out of or in any way relating to this agreement or its formation (including any non-contractual disputes or claims), shall be governed by and construed in accordance with English law.
Dispute Resolution Method	In the event of any dispute arising out of or in connection with this Agreement, either Party shall invite the other Party to commence negotiations to resolve the dispute in good faith. Any invitation to negotiate shall be issued in writing, in the usual way the Parties communicate in writing. If the Parties do not reach a settlement within **28 calendar days** of one Party having invited the other in writing to negotiate, the dispute shall be exclusively and finally resolved by litigation in the courts of **England**.

	Notwithstanding anything to the contrary in this Agreement, either Party may seek equitable relief, including injunctions, in any court of competent jurisdiction to protect its intellectual property rights or confidential information.
Documentation	"**Documentation**" refers to the Provider's proposal, user guides, manuals, technical specifications, and other materials made available by the Provider, in any form or medium, that set out the Provider's offer to the Customer and/or describe the functionality, use, or operation of the Services.
Publicity	The Customer permits the Provider to use its name and logo (**Customer Marks**) during the Agreement Term to identify the Customer as a user of the Services in promotional materials, following any provided usage guidelines. The Provider will not alter the Customer Marks.

2. SERVICES & USAGE

Services Description of the cloud-based and other services provided by the Provider under the Agreement.	The cloud-based software-as-a-service solution(s) provided by the Provider to the Customer under this Agreement. This includes access to and use of the Provider's software, hosting, updates, support, and related services as specified in the Provider's Documentation. Services exclude any third-party applications, integrations, or services that may interact with or be accessible through the Provider's software unless expressly included in the Agreement.
Support Services Description of the support services provided by the Provider under the Agreement. These are distinct from any professional services outlined in the Add-On Terms (if applicable) or other supplemental documents.	Technical assistance, maintenance, and updates provided by the Provider to ensure the effective use and operation of the Services, including issue resolution, delivery of patches and upgrades, access to user documentation, and support through designated communication channels, subject to the scope and limitations outlined in this Agreement or any applicable Supplemental Document.
Authorized Purpose: The specific use of the Services permitted under this Agreement.	To enable the Customer to manage business performance, track goals, and feedback, and generate reports for internal business purposes. This includes storing and analyzing data solely for improving business productivity and excludes any use for commercial resale, or distribution to third parties.
Authorized Users: Individuals or entities permitted to access and use the Services under this Agreement.	"**Authorized User**" means only those of Customer's or its Affiliates' employees, consultants, contractors, and agents authorized by Customer to access and use the Services under the rights granted to Customer pursuant to this Agreement.
Affiliates Entities that control, are controlled by, or are under common control with a Party to this Agreement.	"**Affiliates**" means, with respect to a Party, any entity that directly or indirectly, through one or more intermediaries, controls, or is controlled by, or is under common control with, such Party, where "**control**" means at least a 50% ownership interest in such entity or the power to direct the management of such entity, whether through the ownership of voting securities, by contract, or otherwise.

Affiliate Usage Rights: The rights granted under this Agreement allowing Affiliates to access and use the Services, subject to the same terms and conditions.	The Customer may extend the use of the Services to its Affiliates, provided that such Affiliates comply with the terms of this Agreement. The Customer is responsible for all actions or omissions of its Affiliates as if they were its own.
Additional Use Rights and Limitations: Any additional rights granted to the Customer beyond the standard use of the Services along with any corresponding restrictions, if any.	[Complete if required]

3. PAYMENT TERMS

Fees: Fees payable for the Services.	The Provider makes the Services available subject to the payment of a combination of two fees: 1) A price per case for each case that is opened in a month in mycomplaints.ai. The price per case for this usage type is [£xx.xx plus VAT] 2) A price per Authorized User per month for the use of the mycomplaints.ai Insights MS-Teams app. The monthly fee for the use of the Insights MS-Teams app is [£xx.xx plus VAT] per Authorized User.
Billing Frequency: Frequency of billing.	Monthly in arrears.
Payment Terms: The terms and process for payments due under the Agreement.	30 days from receipt of valid invoice.

4. DATA AND SUSPENSION

Data Export Period: The period within which the Customer can export their data after notice of termination.	60 days post notice of termination throughout the Agreement Term. Data Export will not be possible post-termination of the Agreement.
Data Deletion Period: The period after termination within which the Provider must delete Customer Content.	30 days.

5. USAGE AND LIMITATIONS

Usage Limits: Restrictions on the scope or volume of use of the Services.	The Customer's use of the Services is subject to reasonable usage limits, as determined by the Provider in good faith based on industry standards and typical usage patterns. If the Provider reasonably determines that the Customer's usage exceeds reasonable limits, the Provider may notify the Customer, and the Parties will work together in good faith to

	address the excess usage, which may include agreeing on additional fees or adjusting the Customer's subscription tier.
High-Risk and Sensitive Use Restrictions: Limitations on using the Services for high-risk activities or processing sensitive data.	The Provider takes all reasonable commercial steps in accordance with industry best practice to ensure the availability of the service and the security of the Customer's data. The Provider's Security Measures are documented in its Security Whitepaper. It is the Customer's responsibility to satisfy themself that the Services meet their needs, specifically if the Services are to be used in high-risk environments or for processing sensitive personal data.
Third-Party Integration Connections: Integrations established between the Services and third-party applications or systems.	The Provider may transmit Customer Content to third-party applications and services configured by the Customer to integrate with the Services, provided such integrations are set forth in the Key Terms. Integrations required in this agreement are listed below: [List integrations required, or state "None" if there are none]

6. SPECIAL PROVISIONS

Special Provisions:	[Use if required]

7. SUPPLEMENTAL DOCUMENTS

The following Supplemental Documents are incorporated into the Agreement:

Document Description	Where to find the Information
Service Level Agreement (SLA): The expected performance standards, availability, and support levels for the Services.	Please see Addendum 1: oneSLA: Service Level Agreement.
Data Protection Addendum: The agreement between the Provider and the Customer that governs the processing of personal data in connection with the Services.	[To be agreed between the Parties and attached as Addendum 2].
Security Measures: The technical, organizational, and administrative safeguards implemented by the Provider to protect the confidentiality, integrity, and availability of the Customer's data and the Services.	Please see Addendum 3 – Security Whitepaper.

PARTIES AND EXECUTION

	CUSTOMER	PROVIDER
Company Name, Unique Identifier and Country of Organization	[Organisation Name] [Company Registered Number] [Registered Office Address:]	Mycomplaints Ltd Registered in England No. 16004977 Registered Office Address: Invision House, Wilbury Way, Hitchin, England, SG4 0TY
Signature		
Print Name and Title		
Signature Date		
Notices Address Post and email		

Collectively referred to as the "**Parties"** and individually as the "**Party".**

oneSaaS

Software-as-a-Service, Cloud Services Agreement

Standard Terms

1. ORDER OF PRECENDENCE

This Agreement is comprised of the following documents, listed in order of precedence:

a) the Cover Page or any alternative document, such as an order form, specifying the services and other key terms (of which there may be multiple) (**Key Terms**);
b) any document referred to in the Key Terms, including any addendum, agreement, schedule, or statement of work (**Supplemental Document**); and
c) the oneSaaS standard terms (**Standard Terms**).

2. RULES OF INTERPETATION

In this Agreement:

a) section, schedule, and paragraph headings will not affect its interpretation;
b) reference to a person includes a natural person and an incorporated or unincorporated body (whether having a separate legal personality or not);
c) reference to legislation or any legislative provision is a reference to the same as amended, extended, or re-enacted in the future and includes all legislation made under such legislation now or in the future; and
d) a reference to writing or written includes email and any notifications given through the Services (where applicable).
e) in case of a conflict or inconsistency between various terms contained in the different documents listed in the Order of Precedence section above, the terms contained in a higher-listed document shall take precedence over the terms in a lower-listed document.

3. USE OF SERVICES

3.1 Provision and Use of Services. During the Agreement Term, the Provider shall provide the Services to the Customer in accordance with the terms of this Agreement.

3.2 Customer Obligations. The Customer agrees to:

(a) use the Services solely for the Authorized Purpose;

(b) ensure that only Authorized Users use the Services and that Authorized Users comply with the terms of this Agreement;

(c) refrain from copying, modifying, reverse engineering, decompiling, disassembling, creating derivative works, or otherwise attempting to identify, discover, or obtain any source code, underlying algorithms, or technical information of the Services, except to the extent expressly permitted by law or this Agreement;

(d) not observe the functionality of the Services to develop a product or service that is substantially similar to the Services;

(e) not use Services in breach of applicable law, regulations, and the Documentation;

(f) refrain from accessing, uploading, storing, or transmitting any viruses, malicious code, spam, or material that is unlawful, abusive, obscene, harmful, or otherwise inappropriate; and

(g) not to use the Services to build, train, or configure any artificial intelligence model.

4. DATA AND SECURITY

4.1 Customer Content. "Customer Content" means all data, materials, or content uploaded by the Customer or its Authorized Users in connection with the Services, including but not limited to structured or unstructured data such as personal data, financial metrics, or operational data. For the avoidance of doubt, this does not include usage data or audit logs, which the Provider may monitor independently for their internal purposes, including but not limited to improving the Services, ensuring accurate billing, and providing support.

4.2. Customer Content Responsibilities. Customer Content will remain the property of the Customer. The Customer is responsible for:

(a) the content, quality, legality, and accuracy of the Customer Content provided by the Customer and its Authorized Users;

(b) obtaining all necessary consents before sharing the Customer Content with the Provider; and

(c) notifying the Provider promptly if the Customer becomes aware of any unauthorized access to the Services that may impact the security, stability or integrity of Provider's systems, or other users.

4.3 Data Security. The Provider shall maintain appropriate administrative, physical, technical, and organizational safeguards to protect the security, confidentiality, and integrity of Customer Content, as further outlined in any applicable Data Processing Addendum or related Documentation. The Provider agrees to notify the Customer of any security breaches that adversely impact the Customer Content within 72 hours of becoming aware of such security breach.

5. INTELLECTUAL PROPERTY RIGHTS

5.1 Ownership of Services and Documentation. The Provider or its third-party licensors own all intellectual property rights in and to the Services and Documentation, including any modifications or derivatives.

5.2 Ownership of Feedback. The Customer acknowledges that any intellectual property rights related to the Services or Documentation that arise from the Customer's, its Affiliates' (where applicable), or Authorized Users' requests, suggestions, or ideas (**Feedback**) will vest in the Provider. The Customer grants the Provider a worldwide, perpetual, irrevocable, royalty-free license to use, modify, and incorporate such Feedback into its products or services in any manner the Provider deems appropriate. If the Feedback includes the Customer's Confidential Information, the Provider does not own that information and will handle it in accordance with the Confidentiality Section in this Agreement.

5.3 Independent Development and Use of Customer Content

5.3.1 The Customer grants the Provider the right to:

(a) use Customer Content as necessary to provide the Services and fulfil the Provider's obligations under this Agreement;

(b) anonymise and aggregate Customer Content (and related usage data) with similar information from other customers ensuring no individual can be identified directly or indirectly, to improve, develop, or offer new services, tools, or insights that align with the Authorized Purpose or benefit the Customer and its industry; and

(c) transmit Customer Content to third-party applications and services configured to integrate with the Services provided under this Agreement.

5.3.2 The Provider will ensure that any anonymization is performed using industry-standard techniques to render the data irreversibly non-identifiable. The Customer acknowledges that anonymized data will not be subject to any controller-processor relationship and that the Provider may use such data in compliance with applicable laws and this Agreement, including for the development and improvement of the Services.

6. FEES

6.1 Payment Terms. Fees for the Services will be invoiced according to the Billing Frequency and paid by the Customer as per any Payment Terms outlined in the Key Terms. Late payments may incur interest at the maximum rate allowed by law, calculated from the due date until payment is made in full, including the period where the Parties are engaged in dispute resolution through mediation or court.

6.2 Non-Cancellable and Non-Refundable Fees. All fees are non-cancellable and non-

refundable, except in the event of early termination by the Customer due to a material breach by the Provider. In such cases, the Provider will refund any prepaid fees for services not yet delivered as of the termination date.

6.3 Disputed Payments. In the absence of any disputes or amounts mandatorily withheld by law, all payments must be settled in full by the Customer in accordance with the Agreement. Undisputed invoice(s) received from the Provider must be paid by the date stipulated without any set-off, deduction, or withholding. To dispute an invoice, the Customer must notify the Provider in writing within 30 days, as specified in the Key Terms, providing a clear explanation of the dispute. The Provider agrees to review and consider the dispute in good faith and provide a written determination within a reasonable timeframe. Any undisputed portion of the invoice must still be paid by the due date.

7. TAXES

7.1 Applicability of Taxes. All fees and charges under this Agreement are exclusive of applicable taxes, levies, duties, or similar governmental charges, such as value-added tax (VAT), sales tax, goods and service tax, or use tax (collectively, **Taxes**), which shall be paid by the Customer at the rate and in the manner prescribed by law.

7.2 Taxes Collected by Provider. If the Provider is legally required to collect Taxes on behalf of a taxing authority, these Taxes will be itemized on the invoice provided to the Customer. Customer agrees to pay the invoiced Taxes unless it provides the Provider with a valid tax exemption certificate authorized by the appropriate taxing authority by the invoice payment due date.

8. WARRANTIES

8.1. Provider Warranties. The Provider warrants that:

(a) the Services will perform in substantial conformity with the applicable Documentation;

(b) any Support Services and Add-On Services (if applicable) will be provided with reasonable care and skill;

(c) the Provider will take reasonable steps to keep the Services free from viruses, malware, or other harmful code.

8.2 Sanctions and Export Controls. Customer shall not (and shall procure that Authorized Users shall not):

(a) export, re-export, or transfer the Services (i) in violation of any applicable export control laws or regulations, sanctions, embargoes, restrictive state lists or measures; or (ii) to any embargoed country; or

(b) permit access to or use of the Services by an organization or individual identified on any

government denied-party list or owned 50% or more by an organization or individual on a denied-party list.

8.3 Mutual Warranties and Representations

8.3.1 Each Party warrants that it will comply with all applicable laws in performing its obligations or exercising its rights in this Agreement and represents that it:

(a) has the legal power and authority to enter into this Agreement;

(b) is duly organized, validly existing, and in good standing under applicable laws; and

(c) has all rights necessary to meet its obligations under this Agreement.

8.3.2 For the avoidance of doubt, the Provider makes no warranty that the Customer's use of the Services will comply with the Customer's legal obligations, which the Customer is solely responsible for determining.

8.4 Limitation of Warranties. The Provider's warranties shall not apply if any loss or damage arises from:

(a) using or causing the Services to be used in a way that is outside the scope of this Agreement and accompanying Documentation;

(b) unauthorized modifications or alterations to the Services, whether directly or materially caused by the Customer;

(c) negligence, misuse, or omission by the Customer that results in or amounts to a breach of its obligations under this Agreement;

(d) delays, delivery failures, or any other loss or damage resulting from the transfer of data over third-party communications networks and facilities, including the internet; or

(e) the Customer's failure to determine its compliance with applicable laws in its use of the Services.

8.5 Remedies

8.5.1 If the Customer notifies the Provider in writing of a breach of the warranties, the Provider will, within 30 days of notification, at its discretion (acting reasonably) and expense:

(a) repair or replace the non-conforming Services or re-perform the Support Services or Add-On Services (if applicable); or

(b) if repair, replacement, or reperformance is not feasible, terminate the affected Services and provide a pro-rata refund for any unused fees paid by the Customer.

8.5.2 These remedies are the Customer's sole and exclusive remedies for breach of warranties.

8.6. Disclaimers

8.6.1 To the maximum extent permitted by law, the Provider disclaims all warranties not expressly stated in this Agreement, including but not limited to implied warranties of merchantability, fitness for a particular purpose, non-infringement, and uninterrupted or error-free operation.

8.6.2 Except as expressly provided, all Services, support, and materials are provided on an "as is" and "as available" basis. The Provider makes no warranty that the Services, Documentation, or that results of use will:

(a) meet the Customer's or any third party's requirements;
(b) operate without interruption;
(c) achieve any intended result;
(d) be error-free; or
(e) be compatible or work with Customer components.

Changes to or unavailability of Customer components, connections, or environments during the Agreement Term do not alter the Customer's obligations under this Agreement.

9. LIMITATION OF LIABILITY

9.1 Liability Cap. Unless otherwise agreed in the Key Terms, each Party's total aggregate liability arising under or in connection with this Agreement shall not exceed fees paid or payable in the 12-month period immediately preceding the first event giving rise to a claim (**Liability Cap**).

9.2 Liability Exemption. Neither Party will be liable for (a) any indirect, special, or consequential damages; or (b) whether incurred directly or indirectly, any loss of profits, revenue or goodwill, anticipated savings, or wasted expenditure (and even if advised of the possibility of such losses).

9.3 Exclusions from Liability Cap

9.3.1 The limitations and exclusions of liability set forth in this Agreement do not apply to:

(a) amounts due and payable by the Customer for the Services under this Agreement;
(b) the indemnification obligations in Section 10;
(c) violation of a Party's or its Affiliates' intellectual property rights;
(d) fraud or wilful misconduct; or
(e) any other liability that cannot be excluded or limited under applicable law.

9.4 Applicability of Limitations and Exclusions. The limitations and exclusions in this Section 9 shall apply regardless of the legal basis of the claim, including contract, tort (including negligence), statute, strict liability, or any other legal theory.

10. INDEMNITIES

10.1 Indemnity by the Provider

10.1.1 Subject to Section 9.3 (Exclusions from Liability Cap), the Provider agrees to defend any suit or action brought against Customer for any third-party claim that the Services directly infringe such third party's patent, copyright, or trademark, or misappropriates such third party's trade secret (**Infringement Claim**).

10.2 Exclusions and Limitations

The Provider shall have no liability or obligations under this Section 10 for any Infringement Claim to the extent that it results from:

(a) modifications to the Services made by a party other than the Provider or a party under its direct control;
(b) the combination, operation, or use of the Services with unauthorized third-party products, software, services, or materials;
(c) use of the Services in breach of the Agreement; or
(d) any Customer Content, designs, instructions, specifications, or similar materials provided by the Customer.

10.3 Remedies for Infringement. In the event of an Infringement Claim or Provider's reasonable belief that an Infringement Claim may arise, the Provider, at its option and expense, may:

(a) procure the right for the Customer to continue using the Services in accordance with the Agreement; or
(b) make modifications to or replace the Services so that they become non-infringing without incurring a material reduction in performance or functionality; or,
(c) if (a) or (b) are not commercially feasible, terminate the Customer's right to use the infringing Services and refund the unused remainder of any prepaid Fees for those Services.

10.4 Indemnity by the Customer. Subject to Section 9.3 (Exclusions from Liability Cap), the Customer agrees to defend any suit or action brought against the Provider for any third-party claim that the Customer Content directly infringes such third party's patent, copyright, or trademark, or misappropriates such third party's trade secret, or violates applicable law.

10.5 Indemnification Procedure. The indemnifying Party shall not settle any claim in a manner that materially prejudices the indemnified Party without the indemnified Party's

prior written consent. Each Party agrees to indemnify the other from any resulting costs related to such defence and damages finally awarded by a court of competent jurisdiction, provided that:

(a) the indemnified Party promptly notifies the indemnifying Party in writing of the claim;
(b) the indemnifying Party has sole control of the defence and all related settlement negotiations; and
(c) the indemnified Party provides the indemnifying Party with the information, assistance, and authority necessary to fulfil its obligations under this Section 10.

10.6 Limitation. This Section 10 sets out the Parties' sole and exclusive remedies and their entire liability with respect to claims that are subject to indemnification under the Agreement.

11. CONFIDENTIALITY

11.1 Definition of Confidential Information Each Party may share confidential, proprietary, or sensitive information (**Confidential Information**) with the other in connection with this Agreement. Confidential Information does not include publicly available information obtained without breach of this Agreement or any information that:

(a) was known by the receiving Party on a non-confidential basis before disclosure,

(b) was lawfully obtained from a third party without confidentiality obligations, or

(c) is independently developed without reference to or use of the disclosing Party's information.

11.2 Obligations Regarding Confidential Information. The receiving Party agrees to use Confidential Information solely for purposes of this Agreement, to protect it using at least the same level of care as it uses for its confidential information, and to limit the disclosure to its employees, contractors, or agents who need to know it to fulfil obligations under this Agreement and are bound by confidentiality obligations. The receiving Party may disclose Confidential Information if required by law, provided it promptly notifies the disclosing Party (if permitted) and cooperates to minimise the disclosure. Upon termination of this Agreement, the receiving Party will, upon written request, destroy or return Confidential Information, except as required for legal or regulatory purposes or archival practices.

12. TERM AND TERMINATION

12.1 Term. This Agreement commences on the Agreement Start Date and remains in effect until access to the Services is terminated in accordance with its terms (**Agreement Term**). Unless otherwise specified in the Key Terms, the initial term begins on the Agreement Start Date and lasts for 12 months. Thereafter, the subscription will automatically renew for successive 12-month terms unless either Party provides written notice of non-renewal at least 60 days prior to the expiration of the current term.

12.2 Termination Rights. Either Party may terminate this Agreement immediately by giving written notice to the other Party if:

(a) the other Party commits a material breach of this Agreement that is not remedied within 30 business days of receiving written notice specifying the breach and requiring it to be remedied;
(b) the other Party engages in persistent breaches which, when taken together, can reasonably be considered to constitute a material breach and shall be subject to the remedy period set out in 12.2(a) above;
(c) the other Party is unable to pay its debts when they fall due or admits inability to pay its debts, becomes insolvent, files for bankruptcy, or undergoes similar proceedings; or
(d) the other Party's operational or business processes have demonstrably and substantially changed to the extent that it is no longer capable of meeting its obligations under this Agreement.

12.3 Actions on Termination. Upon termination of this Agreement, if requested by Customer during the Data Export Period, the Provider must return to the Customer (or otherwise make available functionality for the Customer to download) a copy of the Customer Content in a commonly used, machine-readable format. Following the conclusion of any applicable Data Export Period, the Provider will delete all Customer Content from its systems within the Data Deletion Period specified in the Key Terms unless retention is required to comply with legal or regulatory obligations. The Provider will ensure that deletion is performed in a secure and industry-standard-compliant manner.

12.4 Suspension of Services

12.4.1 The Provider may suspend or limit the Customer's use of the Services under the following circumstances (**Suspension Triggers**):

(a) Overdue Payments: Payments are overdue by 15 days or more.
(b) Illegal or Inappropriate Use: The Provider becomes aware of, or has valid reason to believe, the Customer is engaging in unlawful use of the Services.
(c) Risk of Harm: The Provider determines that the Customer's use may harm the Services, compromise the security of the Provider's systems or other customers, or infringe on third-party rights.
(d) Breach of Agreement: The Customer's use of the Services breaches this Agreement, disrupts other customers or adversely impacts the performance of the Provider's systems.

12.4.2 In the event of a Suspension Trigger, the Provider may take actions including immediate suspension in emergencies or within 30 days for other triggers. The Provider will notify the Customer in writing (where permitted by law) and may modify, suspend, or deactivate the Services to address the issue or comply with this Agreement and applicable laws.

12.4.3 If the Customer is subject to an investigation for alleged illegal or inappropriate use of the Services, they must cooperate with the Provider. Failure to cooperate or resolve the issue within a reasonable timeframe may result in immediate suspension or termination of access to the Services.

12.4.4 The Provider will take reasonable steps to mitigate and minimise the duration of any suspension. Access to the Services will be restored promptly once the underlying issue is resolved to the Provider's reasonable satisfaction.

13. GENERAL TERMS

13.1 Notices. Formal notices under this Agreement must be in writing and sent to the email or postal addresses on the Agreement's Cover Page as may be updated by a Party to the other in writing.

13.2 Third parties. Only Parties to this Agreement have the right to enforce any of its terms.

13.3 No Partnership. Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership, joint venture, agency, fiduciary relationship, or other form of legal association between the Parties. Neither Party shall have any authority to bind or obligate the other Party in any manner unless expressly agreed in writing.

13.4 Amendments. Any amendments to this Agreement must be agreed in writing and in accordance with any change management procedures outlined in the Key Terms or Supplemental Documentation, if any.

13.5 Assignment. Neither Party may assign this Agreement without the prior written consent of the other Party, except (a) to an Affiliate, or (b) in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all its assets. Any assignment made in violation of this Section will be null and void.

13.6 Waiver. If a Party fails to enforce a right under this Agreement, that will not be deemed a waiver of that right at any time.

13.7 Counterparts. This Agreement may be executed in any number of counterparts, and this has the same effect as if the signatures on the counterparts were on a single copy of this Agreement.

13.8 Governing Law. This Agreement shall be governed by and construed in accordance with, the Governing Law as outlined in the Key Terms, disregarding its conflict of laws and jurisdiction provisions.

13.9 Dispute Resolution. Any dispute arising in connection with this Agreement must be resolved by the Dispute Resolution Method as outlined in the Key Terms.

13.10 Force Majeure. Neither Party will be considered in breach of this Agreement if a

delay in meeting their obligations is caused by something beyond their reasonable control. This includes, but is not limited to, strikes, industrial disputes, utility or transport failures, natural disasters, war, riots, vandalism, compliance with laws or government orders, terrorist acts, internet or communication network failures, cyberattacks, fires, floods, or storms. The affected Party must inform the other Party as soon as possible and resume their obligations as soon as the issue is resolved.

13.11 Entire Agreement. This Agreement, including its appendices and other documents that are referenced throughout the Agreement, constitutes the entire agreement between the Parties and replaces any pre-contractual agreements, warranties, conditions, duties and obligations that the Parties have agreed to during their negotiations.

13.12 Severability. If any provision in this Agreement is determined to be unenforceable, invalid, frustrated, or otherwise beyond the scope permitted by law, the remainder of the Agreement shall remain operative.

13.13 Survival. The rights and obligations of the Parties under this Agreement that by their nature or context are intended to survive termination or expiration of this Agreement will remain in effect, including but not limited to Sections related to Fees, Confidentiality, Intellectual Property, Indemnification, Limitation of Liability, Governing Law, and Dispute Resolution.

Addendum 1: oneSLA: Service Level Agreement

This Addendum is provided under and forms a Supplemental Document to the main Agreement. Capitalized terms not defined in this SLA have the meaning given to them in the main Agreement.

SERVICE AVAILABILITY

Facet of Service Availability	Service Level
Service Availability	99.9%
Scheduled Maintenance Notice Period	5 business days
Maximum Scheduled Maintenance Duration	8 hours, wherever possible outside of core hours (9:00 AM to 5:00 PM GMT/BST as appropriate)

SUPPORT AVAILABILITY

Hours/Days	Days & Times
Hours	9:00 AM to 5:00 PM GMT/BST as appropriate
Days	Monday to Friday, excluding Bank & Public Holidays in England

SUPPORT RESPONSE TIMES

Issue Severity	Response Time
Critical Issues	The Services are monitored on a 24x7x365 basis and outside of business hours (9:00 AM to 5:00 PM GMT/BST as appropriate) an engineer will respond to a Critical Issue as soon as that Critical Issue is notified to him or her by our automated monitoring systems. Within business hours, Customers will receive a response from a member of the support team within one hour of the logging of their call.
High Issues	Within business hours, Customers will receive a response from a member of the support team within four hours of the logging of their call.
Medium Issues	Within business hours, Customers will receive a response from a member of the support team within sixteen hours of the logging of their call.

SERVICE CREDIT THRESHOLDS FOR DOWNTIME

AVAILABILITY %	SERVICE LEVEL CREDIT
98.5% – 99.89%	5% of the Fees due for the month in which the service level commitment was not met
97% – 98.49%	7.5% of the Fees due for the month in which the service level commitment was not met
< 97%	10% of the Fees due for the month in which the service level commitment was not met

SLA TERMS

1. Service Level Commitment

The Provider commits to maintaining the specified **Service Availability** during each calendar month, excluding scheduled maintenance.

2. Scheduled Maintenance

2.1 Scheduled maintenance will be communicated to the Customer in advance based on the Scheduled Maintenance Notice Period.
2.2 Scheduled maintenance will typically be conducted during off-peak hours to minimise disruption.
2.3 The Provider shall use reasonable endeavors to ensure that scheduled maintenance does not exceed the Maximum Scheduled Maintenance Duration.

3. Excluded Downtime

3.1 Excluded Downtime means any period of unavailability of the Service caused by:

(a) scheduled maintenance, provided that the Scheduled Maintenance Notice Period is given;
(b) Force Majeure events;
(c) issues arising from the Customer's use, configuration, or network environment;
(d) third-party dependencies outside the Provider’s control;
(e) service suspension due to Customer's breach of the Agreement; or
(f) use of non-production features or environments.

3.2 Service unavailability caused by the following will not count towards downtime calculations:

(a) Actions or inactions by the Customer or third parties outside the Provider's control.
(b) Excluded Downtime

4. Support Commitments

4.1 Support will be provided through the designated channels (e.g., email, support portal).

4.2 The Provider will respond to issues within the Support Response Times based on the severity level of the issue.

5. Service Integrity

5.1 The Provider will implement reasonable administrative, physical, and technical measures to maintain the security, stability, and integrity of the Services.
5.2 The Provider will promptly notify the Customer of any known security breaches or service issues.

6. Service Credits

6.1 If Service Availability falls below the specified commitment, the Customer may claim service credits in accordance with the Service Credit Threshold for Downtime.

6.2 Service credits are calculated based on the monthly Fees and are the Customer's sole remedy for downtime.

6.3 Service credits cannot be converted to cash or applied to past-due invoices

6.4 The Customer must submit a request for service credits within 30 days of the end of the affected month.

Addendum 2: Data Protection

[To be agreed between the Parties]

Addendum 3: Security Whitepaper Version 3.3

1. Introduction
This document outlines the comprehensive architecture and robust security measures employed by mycomplaints.ai to safeguard the confidentiality, integrity, and availability of customer data. At mycomplaints.ai, we are deeply committed to maintaining the highest standards of information security, data protection, and operational resilience, catering to government departments, large enterprises, and smaller organisations handling sensitive information.

Security is fundamentally embedded into every layer of our system – from our core infrastructure and stringent access controls to continuous monitoring, comprehensive encryption, and regulatory compliance. We consistently review, enhance, and audit our security practices to uphold the complete trust our customers place in our service.

Our platform is engineered using Amazon Web Services (AWS), a leading cloud computing platform, ensuring real-time scalability, failure-resilient services, and high levels of physical and network security. All data communications are secured using industry-standard Transport Layer Security (TLS 1.2 or higher). Customer data is physically segregated, with each customer having dedicated storage resources and protected through granular access controls enforced at all times. Data is encrypted at rest using strong encryption mechanisms, such as AES-256, managed via AWS Key Management Service (KMS). Access to the platform can be further restricted using IP address whitelisting. Our services communicate externally via a fixed IP address, which client systems can whitelist.

2. Certifications and Assurance
mycomplaints.ai has achieved the following internationally recognised security certifications, providing independent assurance of our controls:

- **ISO/IEC 27001:** The globally accepted standard for information security management systems (ISMS), demonstrating our commitment to a systematic approach to managing sensitive company information.
- **SOC 2 Type II:** An independent audit verifying that our controls related to security, availability, and confidentiality are operating effectively over a period of time.

The following additional security certifications are currently in the final stages of completion:

- **HIPAA:** Our platform aligns with key requirements of the Health Insurance Portability and Accountability Act (HIPAA), which are essential for our customers in the healthcare sector who handle protected health information (PHI).
- **PCI DSS (Payment Card Industry Data Security Standard):** We adhere to the PCI DSS framework to ensure the secure processing, storage, and transmission of payment card information. This is critical for customers handling payments and

financial data, as it offers assurance that we meet stringent security standards for the protection of cardholder data.

Adhering to these rigorous frameworks ensures our security practices remain robust, transparent, and fully aligned with global expectations across diverse industries.

3. Secure Cloud Infrastructure on AWS

Our infrastructure is hosted within Amazon Web Services (AWS), leveraging a secure, well-architected design that prioritises data privacy, scalability, and resilience. Our application is a React application written in TypeScript.

3.1. Key Architectural Components and Security Features

- **User Access & Edge (Frontend Stack):**
    - **Content Delivery Network (Amazon CloudFront):** Acts as the primary entry point for users. It serves static content from secure storage (Amazon S3) and routes API requests to our backend. All traffic is enforced to HTTPS.
    - **Secure Storage for Frontend Assets (Amazon S3):** Stores our static website assets (HTML, CSS, JS, images). The content delivery network serves these assets using secure origin access controls, ensuring the storage bucket is not directly accessible to the public. Data in this storage is encrypted at rest.
    - **Web Application Firewall (AWS WAF):** The content delivery network is protected by a web application firewall to filter malicious traffic, such as SQL injection and cross-site scripting (XSS), providing a critical layer of defence at the edge.
- **Application Layer (Backend Stack):**
    - **Managed Application Hosting (AWS App Runner):** Hosts our containerised backend application.
        - Container images are pulled from a secure **Container Registry (Amazon ECR)**. Images in the registry can be encrypted.
        - The application hosting service is configured to connect to our **Virtual Private Cloud (Amazon VPC)**, ensuring it operates within a private network environment and can securely access internal resources.
        - It utilises identity-based **Instance Roles** for granular permissions to other AWS services, such as our secrets management service, DynamoDB tables, data warehouse, and object storage.
        - An **Access Role** grants the application hosting service permissions to pull images from the container registry.
- **Network Foundation (Custom Virtual Private Cloud - Amazon VPC):**

- Our services operate within a custom virtual private cloud, providing a logically isolated section of the AWS Cloud, configured for high availability across multiple Availability Zones.
- **Private Network Segments (Private Subnets):** Host the application hosting service (via its VPC connection) and our data warehouse. Resources in these private network segments are not directly accessible from the internet, enhancing security.
- **Public Network Segments (Public Subnets):** Contain the **Network Address Translation (NAT) Gateway**.
- **NAT Gateway:** Enables services in private network segments to initiate necessary outbound IPv4 traffic to the internet (e.g., for pulling OS updates or accessing approved external APIs) while preventing inbound traffic initiated from the internet.
- **Private Endpoints for AWS Services (VPC Gateway Endpoints):**
  - **Secure Storage Endpoint:** Allows resources within our virtual private cloud (such as the application hosting service) to access secure object storage buckets (for application data) without traversing the public internet. Access is further restricted by identity policies and endpoint configurations, ensuring only authorised resources from within our virtual private cloud can use the endpoint.
  - **DynamoDB Endpoint:** Similar to the storage endpoint, allows resources within our virtual private cloud to access DynamoDB tables privately. Access is governed by identity policies and endpoint configurations that verify the request originates from authorised resources within our virtual private cloud.
- **Network Firewalls (Security Groups):** Act as virtual firewalls to control traffic at the resource level. For instance, the data warehouse security group is configured to allow inbound traffic only from the application hosting service on the specific port required for database communication.
- **Network Traffic Logging (VPC Flow Logs):** Captures information about IP traffic going to and from network interfaces in our virtual private cloud. These logs are delivered to a centralised logging service (Amazon CloudWatch Logs) for monitoring, security analysis, and troubleshooting.

- **Fixed Egress IP:** For any required outbound communications from our backend services that need to be whitelisted by external client systems, traffic routes through the NAT Gateway, which uses a static Elastic IP address.

3.2. Data Layer

Our data layer is designed with security and segregation as primary considerations.

- **Transactional Data (Amazon DynamoDB tables):**
  - Our core transactional data is stored in Amazon DynamoDB tables.

- Each customer's transactional data resides in a separate, dedicated DynamoDB table, ensuring strict data isolation.
- These DynamoDB tables are accessed privately from the application hosting service via a private DynamoDB endpoint within our virtual private cloud.
- Data within DynamoDB tables is encrypted at rest by default using AWS-owned keys, with the option to use AWS-managed encryption keys.

- **Data Warehouse (Amazon Redshift Serverless):** Serves as our data warehouse for Business Intelligence (BI).

  - Operates within our virtual private cloud's private network segments.
  - Its network firewall rules strictly control inbound access, permitting traffic only from the application hosting service.
  - Data in the data warehouse is encrypted at rest by default using managed encryption keys.

- **Redshift Serverless Data Sharing:** We leverage Amazon Redshift Data Sharing to provide clients with secure, governed access to their data within our Redshift data warehouse. For each client, we provision a dedicated datashare that includes only the data owned by that client. Ownership of the datashare is retained by us, and access is granted to the client's AWS account. Clients query the shared data using their own AWS compute and preferred BI tools, ensuring robust separation of data as well as strong performance isolation between tenants.

After the datashare is attached in the client's environment, they can connect using standard analytics platforms—including Power BI, Tableau, Qlik, and other JDBC/ODBC-compatible tools—to directly consume, model, and visualize the shared datasets. This approach enables a flexible and tightly controlled integration path for incorporating our data into client reporting ecosystems, without exposing or duplicating underlying warehouse resources.

- **Business Intelligence & Reporting (Amazon QuickSight):** Amazon QuickSight is used as our business intelligence and reporting layer, delivering interactive dashboards and visualizations to support root cause analysis as well as natural language driven QnA analytics. QuickSight is offered as an add-on service that reads datasets from our data warehouse and presents insights securely to each customer. Curated data from Amazon Redshift Serverless is ingested into QuickSight SPICE to improve responsiveness and scalability. SPICE accelerates dashboard performance, reduces load on Redshift, and supports automatic incremental refreshes with built-in compression and elastic scaling.

QuickSight access to warehouse resources is restricted to private networking only. All QuickSight connections are made through dedicated VPC endpoints, allowing private reachability to our Redshift Serverless and RDS environments under tightly scoped security group rules. Data movement between QuickSight and Redshift/RDS occurs exclusively over the private VPC network and is protected with TLS encryption. Security groups permit

inbound traffic only from the QuickSight VPC connection and deny all public access, ensuring BI processing remains within our controlled network boundary.

Clients access QuickSight dashboards solely through our application's existing SSO flow. Upon authentication, the application generates a secure, short-lived federated QuickSight session containing the user's customer context and authorized dashboards. Clients do not log in to QuickSight directly; all entitlements and data access are enforced via the application and AWS IAM controls.

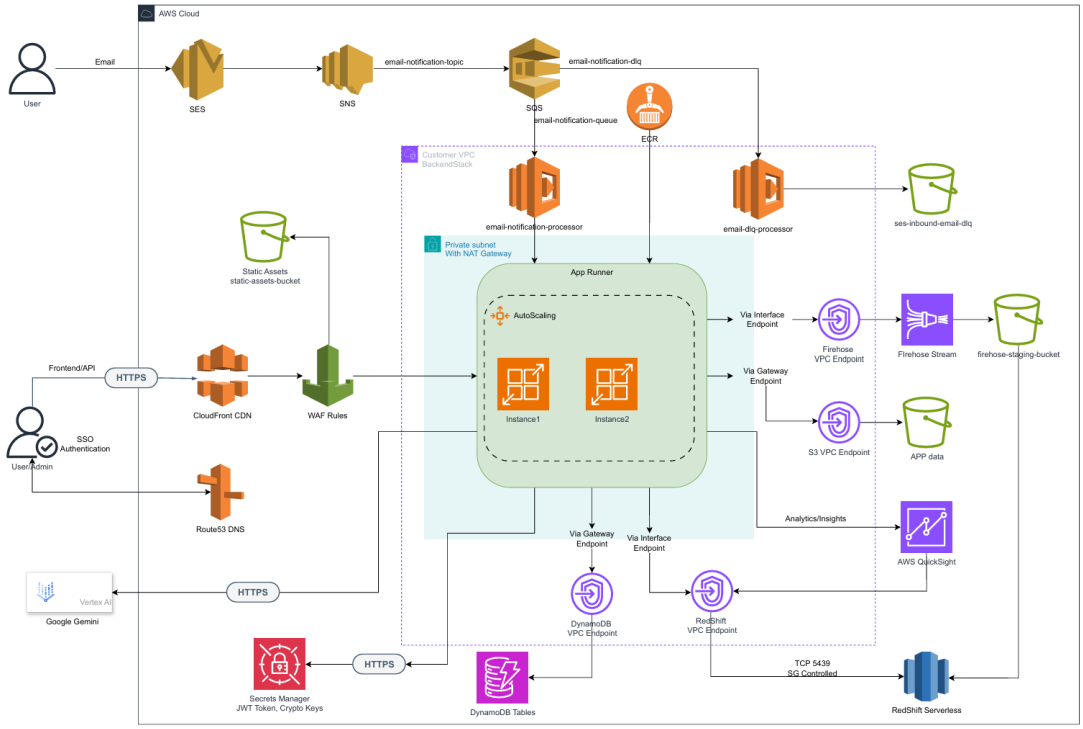
Tenant isolation is maintained end-to-end across the BI stack. Each customer can access only their dedicated SPICE datasets, which are mapped to their corresponding Redshift schema. Both Redshift and SPICE datasets are encrypted at rest using customer-managed encryption keys, providing strong cryptographic separation in addition to access-control boundaries.

- **Secure Object Storage for Application Data (Amazon S3):** Besides static assets and logs, our application uses object storage for other data storage needs (e.g., customer file uploads).
    - Accessed privately from the application hosting service via a private storage endpoint.
    - Data is encrypted at rest.
- **Data Store Security:** All database systems (DynamoDB tables, Redshift) and storage systems (S3) are configured as private resources. They are accessible only via internal private endpoints (for DynamoDB tables and S3) or from within our virtual private cloud (for Redshift) and are protected by strict identity policies, endpoint policies, and network firewalls, ensuring no direct public access.

3.3. AWS Physical Security

AWS infrastructure is housed in Amazon-controlled data centres. These data centres are secured with extensive physical barriers and access controls. Only authorised Amazon personnel with a legitimate business need are aware of the actual locations of these data centres. AWS maintains a high level of physical security, which is regularly audited.

3.4. AWS Network Architecture



4. Identity and Access Control

Access to the mycomplaints.ai platform and its underlying infrastructure is tightly controlled using the principle of least privilege:

- **Single Sign-On (SSO) Only Access:** Access to the mycomplaints.ai application for organisational users is exclusively managed through Single Sign-On (SSO). We integrate with Azure Active Directory (Azure AD) and Google Workspace as identity providers, utilising the OAuth 2.0 authorisation protocol. We do not support local username/password authentication for these users.
- **Identity and Access Management (IAM) for Cloud Resources:**
    - **Service Roles:** Defines roles and policies to grant least-privilege access for services. Our application hosting service has distinct roles:
        - An **Access Role** grants permission to pull container images from the secure container registry.
        - An **Instance Role** grants runtime permissions to access other AWS services, such as the Secrets Management Service, DynamoDB tables, data warehouses, and object storage. These roles are configured with specific permissions (e.g., read access for specific secrets, granular DynamoDB/storage/data warehouse actions).
    - **Private Endpoint Policies:** Policies attached to private endpoints for storage and DynamoDB further restrict access, ensuring that only specified resources within our virtual private cloud (like the application hosting service, identified by its role and originating from within the VPC) can use these endpoints.

- **Role-Based Access Control (RBAC) within Application:** Access to sensitive data and platform functionalities is strictly limited based on user roles and responsibilities defined within the mycomplaints.ai application itself.
- **Secure Secrets Management (AWS Secrets Manager):** Stores and manages sensitive information securely, including JWT signing keys and cryptographic keys. Our application hosting service instances are granted specific read access only to the secrets they require via their IAM Instance Role. Secrets are encrypted at rest.
- **Infrastructure Access:** Access to the AWS Management Console for authorised mycomplaints.ai administrative staff is protected by multi-factor authentication (MFA) and managed via SSO. Direct access to underlying server instances is generally not required due to the managed nature of our application hosting and serverless services; system operations are performed via secure APIs and management consoles.

5. Comprehensive Encryption and Data Security

We employ strong encryption mechanisms for all data, both in transit and at rest, to ensure its confidentiality and integrity.

5.1. Encryption in Transit

- **User to Content Delivery Network:** All communication is enforced over HTTPS (TLS 1.2 or higher).
- **Content Delivery Network to Secure Storage (Static Assets):** Communication uses HTTPS via secure origin access controls.
- **Content Delivery Network to Application Hosting Service Origin:** Communication is enforced over HTTPS.
- **Internal AWS Service Communication:**
    - **Application Hosting Service to Data Warehouse:** SSL/TLS is enabled by default for data warehouse connections.
    - **Application Hosting Service to Secrets Management, DynamoDB tables, Secure Object Storage (via Private Endpoints):** All AWS service API endpoints are accessed over HTTPS/TLS.
    -

5.2. Encryption at Rest

All customer data stored within our platform is encrypted at rest:

- **Secure Object Storage (Static Assets, Application Data, Audit Logs):** Data is encrypted. Our audit log storage is configured for default encryption.
- **DynamoDB tables:** Data is encrypted at rest by default.
- **Data Warehouse:** Data is encrypted by default using managed encryption keys.
- **Secrets Management Service:** Secrets are encrypted using managed encryption keys.
- **Secure Container Registry:** Container images can be configured for encryption at rest.

Encryption keys (where applicable) are managed through a dedicated key management service (AWS KMS), ensuring a high level of security and control.

5.3. IP Address Restrictions
Access to the mycomplaints.ai application can be restricted to a whitelist of IP addresses or address ranges, providing an additional layer of security for customers who require it.

6. Continuous Monitoring and Threat Detection
mycomplaints.ai operates with a focus on continuous visibility and proactive threat detection across its environment.

- **Audit Logging for Cloud Resources (AWS CloudTrail):** All AWS management API calls, including configuration changes to AWS services, and account activity across our environment are meticulously recorded. These logs are stored durably in a dedicated, encrypted secure object storage bucket. This is crucial for audit, compliance, and security analysis.
- **Network Traffic Logging (VPC Flow Logs):** Provides detailed insights into IP traffic patterns to and from network interfaces in our virtual private cloud. These logs are delivered to a centralised logging service for security analysis, incident response, and troubleshooting.
- **Threat Detection Service (AWS GuardDuty):** This service continuously monitors for malicious activity and unauthorised behaviour to protect our AWS accounts, workloads, and data. It analyses various AWS data sources, including audit logs, network traffic logs, and DNS logs. Alerts are generated for suspicious activities.
- **Centralised Logging and Alerting (Amazon CloudWatch):** System, application (from the application hosting service), and security logs (including network traffic logs) are consolidated in a centralised logging service. We leverage its metrics, alarms, and dashboards for real-time monitoring and to alert our operations team to potential security incidents or operational issues, enabling rapid investigation and response. All logging utilises a synchronised time service for accurate time referencing.

7. Handling of Sensitive and Regulated Data
mycomplaints.ai provides the necessary controls and safeguards for organisations handling sensitive complaints data, health records (PHI), or other types of regulated information:

- **Encryption for PHI and Personal Data:** All sensitive information, including PHI and other personal data, is encrypted at all times throughout its lifecycle – in transit and at rest, as detailed in Section 5.
- **Rigorous Access Control and Isolation:** Identity-based roles (including for our application hosting service), identity policies (including those on private endpoints), network firewalls, and network segmentation within the virtual private cloud (private network segments) are meticulously configured to ensure that only authorised services and users can access restricted data sets, adhering to the principle of least

privilege. Dedicated DynamoDB tables and object storage buckets per customer further enhance this.

- **Comprehensive Audit Trails:** Cloud resource audit logs provide comprehensive records of all API calls and configuration changes. Network traffic logs and application logs contribute to the audit picture, providing essential audit trails for compliance reporting (e.g., HIPAA), internal reviews, and regulatory requirements. Application-level actions related to complaints or case data are also logged.
- **HIPAA-Eligible Service Utilisation:** We exclusively utilise AWS services that are HIPAA-eligible and covered by the AWS Business Associate Addendum (BAA), enabling us to meet the requirements for handling PHI in accordance with HIPAA.

8. Resilience, Scale, and Data Management

Our platform is designed for high availability, fault tolerance, and scalability, ensuring reliable service delivery.

8.1. Built for Resilience and Scale

- **Multi-Availability Zone Deployment:** Our virtual private cloud is configured across multiple Availability Zones, providing a multi-AZ deployment for network segments. Key services like our application hosting service, DynamoDB tables, and data warehouse are designed for high availability and automatically manage resources across multiple AZs within a region. This provides robust protection against localised data centre failures.
- **Autoscaling Capabilities:** Our application hosting service is managed and automatically handles deployment, scaling (both up and down), and availability of our backend application in response to demand. Our data warehouse and DynamoDB tables also automatically scale capacity to meet workload needs.
- **Global Content Delivery:** Our content delivery network is a globally distributed service, ensuring low-latency access to static assets and API endpoints for users worldwide.
- **Redundancy and Failover:** Critical services incorporate built-in redundancy and automated failover mechanisms. For example, DynamoDB provides inherent data durability by replicating data across multiple AZs. Our data warehouse is also designed for high availability.

8.2. Data Separation

To ensure strong data isolation for each customer:

- **Transactional Data (Amazon DynamoDB tables):** Each customer's transactional data is stored in a dedicated, separate DynamoDB table. Access to these tables is strictly controlled by identity policies specific to each customer's resources, ensuring that the application instance serving a particular tenant can only access that tenant's table.
- **File Storage:** Files and documents uploaded by a customer are stored in a dedicated, separate bucket within our secure object storage service for that customer. Again, access to these buckets is governed by distinct identity policies tied

to the tenant context. This physical separation at the table and bucket level provides a robust boundary, ensuring that one customer cannot access another's data. For Business Intelligence, data in our data warehouse is segregated through separate database schemas and access controls.

8.3. Data Backups

- **DynamoDB tables:** We utilise Point-In-Time Recovery (PITR), allowing us to restore data to any point in time within the preceding 35 days. On-demand backups can also be taken for long-term archival.
- **Secure Object Storage (Amazon S3):** Data in object storage is versioned, and cross-region replication can be configured for additional durability and disaster recovery.
- **Data Warehouse (Amazon Redshift Serverless):** Automatically takes snapshots of data, enabling point-in-time restores.
- **Centralised Backup Management (AWS Backup):** In addition to the native backup capabilities of individual services, we utilise a centralised backup service (AWS Backup) to define and manage backup policies for our DynamoDB tables and object storage buckets. This allows for consistent backup scheduling, retention management, and recovery testing across these resources. All backups are encrypted.

8.4. Disaster Recovery (DR)

Our multi-Availability Zone architecture provides high availability within an AWS region. For disaster recovery across regions, AWS services like our object storage, DynamoDB tables, and data warehouse support cross-region replication features. In the event of a regional outage, we have procedures in place to restore services in an alternative AWS region. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are defined and regularly reviewed as part of our business continuity planning.

8.5. Data residency

We are committed to meeting the data residency, compliance, and performance needs of our customers. Our platform offers secure endpoint hosting in the United States, Europe, Australia, and the United Kingdom, enabling you to choose the region that best aligns with your regulatory requirements and latency expectations. Once a region is selected, all data is processed and stored exclusively within that geographic boundary, ensuring that no customer data ever crosses location borders. This approach supports adherence to local data protection laws and reinforces your control over sensitive information.

9. Security Policies and Practices

9.1. Input Controls

Our React application, built with TypeScript, incorporates robust input validation both client-side and server-side (within our API layer on the application hosting service) to check for data type, length, format, and range. The web application firewall at the content delivery network edge provides an additional layer of defence against common web exploits such as

SQL injection, cross-site scripting (XSS), and other common web attack patterns. We also employ mechanisms to prevent Cross-Site Request Forgery (CSRF) attacks.

9.2. Email integration

mycomplaints.ai integrates with your organisation's existing email infrastructure for sending case-related communications. We connect to your Microsoft 365 or Google Workspace email services using secure OAuth 2.0 authorisation flows via their respective APIs. This ensures that emails are sent from your own trusted mail servers, leveraging your existing configurations for sender authentication (DKIM, SPF, DMARC) and security policies. Options for whitelisting email domains for outbound messages can be configured for data loss prevention, where applicable, through your own mail service settings.
Incoming emails to mycomplaints.ai are handled through AWS SES and accepted only from nominated sender domains using a configurable whitelist. Every message is virus- and spam-scanned, then authenticated using SPF, DKIM, and DMARC. If any of these checks fail, the email is treated as potentially spoofed and is not processed, ensuring mail comes only from authorised servers and approved organisational domains.
Each tenant is allocated a tenant-specific inbound email address. Emails received through that address are triaged automatically and may either result in a new case being created or the email being attached to an existing case.
Production: tenantid@mycomplaints.ai
Staging: tenantid@s.mycomplaints.ai
Development: tenantid@d.mycomplaints.ai
In addition, we also provide dedicated inbound address for receiving already completed or resolved cases:
Production: tenantid.completed@mycomplaints.ai
Staging: tenantid.completed@s.mycomplaints.ai
Development: tenantid.completed@d.mycomplaints.ai

9.3. Security Testing

mycomplaints.ai is committed to rigorous security testing:

- **Internal Vulnerability Assessments:** We conduct regular internal vulnerability assessments, particularly after significant code releases or infrastructure updates. This includes checks for input validation flaws, common injection vulnerabilities, broken authentication/session management, insecure direct object references, and CSRF vulnerabilities.
- **Independent External Testing:** We engage accredited third-party security firms to conduct annual penetration tests of our platform. Quarterly ASV (Approved Scanning Vendor) vulnerability scans are also performed in line with PCI DSS requirements. Findings from these tests are reviewed, prioritised, and remediated accordingly.

9.4. Data Loss and Security Breach Reporting

All mycomplaints.ai staff are trained to report any actual or suspected data loss or security incidents to senior management immediately. In the event of an incident affecting customer data, impacted customers will be notified in accordance with our incident response plan and

applicable legal/regulatory obligations. We take appropriate actions to mitigate the impact of any incident and prevent recurrence. Customer data is not printed or stored on removable media by our staff as a standard practice.

10. Staff Security Awareness and Vetting

mycomplaints.ai places significant emphasis on the security awareness and trustworthiness of its personnel.

- **Security Training:** All employees undergo comprehensive information security awareness and data protection (e.g., GDPR) training during their induction and receive annual refresher courses.
- **Confidentiality Agreements:** All staff are bound by employment contracts that include strict confidentiality clauses and require compliance with mycomplaints.ai's information security and data protection policies, including an Acceptable Use Policy.
- **Access Revocation:** Upon termination of employment, all access to company systems and data is immediately revoked.
- **Background Vetting:** All mycomplaints.ai employees undergo background screening appropriate to their roles and responsibilities, which may include criminal records checks. Employees handling highly sensitive data or requiring access to specific government systems may be subject to additional security clearances as needed.
- **Policy Enforcement:** Violations of security policies may result in disciplinary action, up to and including termination of employment.

11. Compliance Monitoring

Compliance with internal security policies and external regulatory requirements is overseen by mycomplaints.ai senior management in conjunction with our dedicated compliance team. Regular internal audits and reviews are conducted to ensure adherence to our security controls and to identify areas for continuous improvement. The use of Infrastructure as Code helps maintain a consistent, auditable, and version-controlled infrastructure configuration, supporting compliance efforts.

12. Conclusion

mycomplaints.ai delivers enterprise-grade security capabilities to organisations of all sizes. We are dedicated to ensuring that our platform is effective, resilient, and aligns with the highest global security and compliance standards. Our architecture, built on AWS, leverages defence-in-depth, strong encryption, granular access controls, and continuous monitoring to protect customer data. Whether you are implementing complaint management for the public sector, scaling internal case-handling processes, or launching a sensitive customer feedback channel, you can have complete confidence in our platform to keep your data safe and secure.