LEGAL

Data Processing Agreement

FyneDesk — Last updated: May 28, 2026

This Data Processing Agreement ("**DPA**") forms part of the Terms of Service (the "**Agreement**") between FyneDesk ("**FyneDesk**", "**we**", "**us**", or "**our**") and the customer that has accepted the Agreement ("**Customer**" or "**you**"). It governs FyneDesk's processing of Customer Personal Data in connection with the Service.

By accepting the Agreement, you accept this DPA. If you are accepting on behalf of an organization, you represent that you have authority to bind that organization. This DPA applies automatically and requires no signature; however, a signed counterpart is available on written request to support@fynedesk.io.

This DPA reflects the parties' agreement on the processing of Customer Personal Data under (a) the EU General Data Protection Regulation (Regulation (EU) 2016/679, "**GDPR**"); (b) the United Kingdom Data Protection Act 2018 and the UK GDPR (collectively, "**UK GDPR**"); (c) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, "**CCPA**"); and (d) other applicable data protection and privacy laws (together, "**Data Protection Laws**").

1. Definitions

Capitalized terms not defined in this DPA have the meanings given to them in the Agreement.

- **"Customer Personal Data"** means Personal Data submitted to or generated within the Service by or on behalf of Customer, including ticket content, contact records, end-user profiles, and metadata.
- **"Personal Data"**, **"Processing"**, **"Controller"**, **"Processor"**, **"Data Subject"**, **"Supervisory Authority"**, and **"Personal Data Breach"** have the meanings given in the GDPR, and apply equally to equivalent concepts under UK GDPR.
- **"Business"**, **"Service Provider"**, **"Consumer"**, **"Sensitive Personal Information"**, **"sell"**, and **"share"** have the meanings given in the CCPA.
- **"Sub-processor"** means any third party engaged by FyneDesk to Process Customer Personal Data in connection with the Service, other than FyneDesk personnel.
- **"Standard Contractual Clauses"** or **"SCCs"** means the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, set out in Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
- **"UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018, in force from 21 March 2022.

2. Scope and roles

For Customer Personal Data Processed by FyneDesk in connection with the Service:

- Customer is the **Controller** (under GDPR/UK GDPR) and the **Business** (under CCPA);
- FyneDesk is the **Processor** (under GDPR/UK GDPR) and the **Service Provider** (under CCPA).

FyneDesk acts as an independent Controller in relation to a limited set of administrative and operational data, including account contact information, billing details, authentication logs, security telemetry, aggregated usage analytics, and other data we generate to operate, secure, and improve the Service. The use of that data is described in our Privacy Policy and is outside the scope of this DPA.

The subject matter, duration, nature, purpose, categories of Data Subjects, and types of Customer Personal Data are described in **Annex I**.

3. FyneDesk's obligations as Processor

3.1 Documented instructions

FyneDesk Processes Customer Personal Data only on Customer's documented instructions, including with regard to transfers to a third country or international organization, unless required to do otherwise by applicable law. Customer's documented instructions are (a) this DPA and the Agreement, (b) the configuration and use of the Service by Customer's authorized users, and (c) written instructions communicated to FyneDesk through the Service or to support@fynedesk.io. If FyneDesk is required by law to Process Customer Personal Data outside Customer's instructions, FyneDesk will notify Customer before Processing unless prohibited by law on important grounds of public interest.

FyneDesk will inform Customer if, in its opinion, an instruction infringes applicable Data Protection Laws. FyneDesk is not obliged to follow instructions that, in its reasonable opinion, would cause it to violate applicable law or that fall outside the Service as described in the Agreement.

3.2 Confidentiality

FyneDesk ensures that personnel authorized to Process Customer Personal Data are bound by written confidentiality obligations or are under an appropriate statutory obligation of confidentiality. Access to Customer Personal Data is limited to personnel who require such access to perform the Service.

3.3 Security

FyneDesk implements appropriate technical and organizational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to such data, and against all other unlawful forms of Processing. These measures are described in **Annex II** and are reviewed at least annually. FyneDesk may update its security measures from time to time, provided the updates do not materially diminish the level of protection.

3.4 Assistance with Data Subject rights

FyneDesk provides Customer with functionality through the Service to enable Customer to respond to Data Subject requests to exercise their rights under Data Protection Laws (including access, rectification, erasure, restriction, portability, and objection). If FyneDesk receives a request directly from a Data Subject, FyneDesk will, where it can reasonably identify the relevant Customer, redirect the Data Subject to that Customer without responding to the substance of the request, and will notify Customer. Where the in-product functionality is insufficient to enable Customer to respond, FyneDesk will provide reasonable assistance at Customer's reasonable, documented cost, taking into account the nature of the Processing and the information available to FyneDesk.

3.5 Assistance with security, breach response, and DPIAs

FyneDesk assists Customer in ensuring compliance with Customer's obligations under Articles 32 to 36 GDPR (and equivalent obligations under UK GDPR), taking into account the nature of the Processing and the information available to FyneDesk. This includes providing Customer with information reasonably necessary to conduct a Data Protection Impact Assessment in connection with the Service and, where applicable, to consult with the relevant Supervisory Authority. The level of assistance FyneDesk is required to provide is proportionate to FyneDesk's role as Processor and is subject to reasonable cost reimbursement for non-routine requests.

3.6 Return and deletion

Following termination of the Agreement, at Customer's choice, FyneDesk will (a) return Customer Personal Data to Customer in a commonly used machine-readable format, or (b) delete Customer Personal Data from FyneDesk's production systems within thirty (30) days, except to the extent retention is required by applicable law. Backups containing Customer Personal Data are retained in accordance with FyneDesk's standard backup retention schedule (no longer than ninety (90) days) and will be overwritten or deleted on rotation. Certain inbound-mail and integration Sub-processors apply standard server-side retention windows that may extend beyond the foregoing; FyneDesk will instruct each such Sub-processor to delete promptly upon Customer's instruction, and Customer acknowledges that final deletion at those Sub-processors may take up to one hundred and eighty (180) days from FyneDesk's deletion instruction. FyneDesk will provide one written certification of deletion at no charge on Customer's written request following termination; additional certifications may be subject to reasonable cost reimbursement.

3.7 Records and demonstration of compliance

FyneDesk maintains records of Processing as required by Article 30 GDPR (and equivalent UK GDPR provisions) and will make available to Customer, on reasonable written notice, the information reasonably necessary to demonstrate compliance with this DPA. FyneDesk satisfies its information obligation primarily by providing copies of its current third-party audit reports (including SOC 2 Type II where available), its security summary, and its sub-processor list. Customer's audit rights are addressed in Section 7.

4. Sub-processors

Customer provides general authorization for FyneDesk to engage Sub-processors in connection with the Service, subject to this Section 4 and to FyneDesk's compliance with the requirements set out below.

4.1 Categories of Sub-processors

Customer authorizes FyneDesk to engage Sub-processors in the following categories, and to add or replace Sub-processors within these categories from time to time, subject to the notice and objection process below:

- **Cloud infrastructure and hosting** — the platforms on which the Service runs;
- **Database, authentication, and storage** — the systems that hold Customer Personal Data and authenticate users;
- **Transactional email and messaging** — providers that deliver email and other transactional messages on behalf of Customer or FyneDesk;
- **Inbound email and integration services** — providers that route inbound communications (such as email-to-ticket) into the Service;

- **Artificial intelligence and machine learning inference** — providers that perform inference on ticket and message content to power Service features;
- **Payment processing** — providers that process subscription fees and other payments;
- **Error monitoring, logging, and observability** — providers that capture diagnostic data to maintain Service reliability;
- **Product analytics** — providers that capture aggregated usage data to maintain and improve the Service;
- **Customer support tools used by FyneDesk** — tools used by FyneDesk personnel to support Customer's use of the Service.

A current list of named Sub-processors, including each Sub-processor's purpose, primary processing region, and a link to its own data protection terms, is published at fynedesk.io/subprocessors. The current list forms part of this DPA by reference.

4.2 Notice of new or replacement Sub-processors

FyneDesk will provide Customer with at least thirty (30) days' prior notice of the addition or replacement of any Sub-processor that will Process Customer Personal Data. Notice is provided by updating the list at fynedesk.io/subprocessors, and (where Customer has subscribed to updates) by email to the address Customer designates. Customer is responsible for subscribing to update notifications if it wishes to receive them by email.

4.3 Right to object

Customer may object to the addition or replacement of a Sub-processor on reasonable grounds related to data protection by giving written notice to support@fynedesk.io within thirty (30) days of the notice. The parties will discuss the objection in good faith for up to thirty (30) days. If the parties cannot reach a resolution, FyneDesk may, in its sole discretion, (a) elect not to engage the proposed Sub-processor with respect to Customer's Customer Personal Data, in which case Customer's objection will be deemed resolved; or (b) continue to engage the proposed Sub-processor, in which case Customer's sole and exclusive remedy is to terminate the affected portion of the Service on written notice. Termination under this Section 4.3 entitles Customer to a pro-rated refund of any prepaid fees for the period after the effective date of termination, will not trigger any early-termination fee under the Agreement, and will be accompanied by reasonable transition assistance under Section 3.6. Termination on this ground does not give rise to any further liability of FyneDesk to Customer.

4.4 Sub-processor obligations

FyneDesk imposes data protection obligations on each Sub-processor by written agreement (which may be the Sub-processor's standard terms incorporating data protection commitments) that are designed to provide a level of protection materially equivalent to those set out in this DPA, taking into account the nature of the Sub-processor's services. With respect to Personal Information of California Consumers, FyneDesk's Sub-processor agreements include the contractual terms required by Cal. Code Regs. tit. 11, § 7053 where applicable. FyneDesk remains responsible to Customer for the performance of each Sub-processor's obligations to the extent set out in this DPA, subject to the limitation of liability provisions of the Agreement and Section 10 of this DPA.

4.5 AI and machine learning restrictions

Where FyneDesk engages a Sub-processor in the artificial intelligence and machine learning inference category to Process Customer Personal Data, FyneDesk will require that Sub-processor to be contractually prohibited from using Customer Personal Data to train, fine-tune, or otherwise develop generally-available models. FyneDesk does not use Customer Personal Data to train its own models.

5. Security and breach notification

5.1 Security measures

FyneDesk's technical and organizational measures, including measures to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing systems and services, are described in **Annex II**. FyneDesk personnel undergo background checks (where permitted by law), security training on hire and annually thereafter, and are bound by confidentiality obligations as described in Section 3.2.

5.2 Personal Data Breach

FyneDesk will notify Customer of a Personal Data Breach affecting Customer Personal Data without undue delay after becoming aware of the breach, and in any event within seventy-two (72) hours of confirming the occurrence of the breach, in sufficient time to enable Customer to comply with its own notification obligations under applicable Data Protection Laws. A delay required by binding instructions from law enforcement or a competent authority will not constitute an undue delay.

FyneDesk's notification will include the information reasonably available to FyneDesk at the time of notice, including (where known) the nature of the breach, the categories and approximate number of affected Data Subjects and records, the likely consequences, and the measures taken or proposed to address the breach. Initial notice may include only information then reasonably available; further information will be provided in subsequent communications as it becomes available.

As between Customer and FyneDesk, and for purposes of liability allocation under Section 10, FyneDesk's notification of a Personal Data Breach is not an admission of fault or liability for the breach. This sentence does not limit FyneDesk's obligations to Customer, to Data Subjects, or to Supervisory Authorities under applicable Data Protection Laws.

Customer is responsible for notifying Supervisory Authorities and affected Data Subjects of any Personal Data Breach to the extent required by applicable Data Protection Laws. FyneDesk will provide reasonable assistance to Customer in connection with these notifications, taking into account the nature of the Processing and the information available to FyneDesk.

6. Customer's obligations and warranties

Customer represents, warrants, and undertakes that:

- Customer has provided all notices and obtained all consents, authorizations, and other rights necessary under applicable Data Protection Laws for FyneDesk (and its Affiliates and Sub-processors) to Process Customer Personal Data as described in the Agreement and this DPA;
- Customer's instructions to FyneDesk concerning the Processing of Customer Personal Data comply with applicable Data Protection Laws;
- Customer is solely responsible for the accuracy, quality, content, and legality of Customer Personal Data and the means by which Customer acquired it;
- Customer has a lawful basis for transferring Customer Personal Data to FyneDesk and authorizing FyneDesk to engage Sub-processors located in the regions identified at fynedesk.io/subprocessors;

- Customer is solely responsible for assessing whether the Service, including the security measures described in Annex II, meets Customer's requirements under applicable Data Protection Laws, and for configuring the Service in a manner that satisfies those requirements;
- Customer is solely responsible for its own obligations to notify Supervisory Authorities and Data Subjects in respect of any Personal Data Breach, and for complying with applicable Data Protection Laws in connection with such notifications;
- The Service is not designed or intended for the Processing of categories of Personal Data that require specific safeguards under Article 9 GDPR or equivalent provisions (including health data, genetic data, biometric data for unique identification, or data revealing racial or ethnic origin, political opinions, religious beliefs, trade-union membership, or sex life or sexual orientation), and Customer will not upload, submit, or otherwise cause FyneDesk to Process such data through the Service unless the parties have separately agreed in writing.

FyneDesk is not obliged to monitor, review, or assess the lawfulness of Customer's instructions or Customer Personal Data on an ongoing basis. Nothing in this Section 6 limits FyneDesk's obligation under Section 3.1 to inform Customer where FyneDesk forms the opinion that an instruction infringes applicable Data Protection Laws.

7. Audits

FyneDesk demonstrates compliance with this DPA primarily by making available to Customer, on reasonable written request and subject to mutually agreed confidentiality obligations:

- a copy of FyneDesk's most recent independent third-party security audit report (including any SOC 2 Type II report, ISO 27001 certification, or equivalent), dated within the prior thirteen (13) months;
- FyneDesk's summary of technical and organizational measures (as set out in Annex II, as updated from time to time); and
- responses to a standard security questionnaire (which may be FyneDesk's pre-completed standard questionnaire).

Where Customer reasonably determines that the foregoing materials are insufficient to demonstrate FyneDesk's compliance with this DPA, and to the extent required by applicable Data Protection Laws (including Article 28(3)(h) GDPR), Customer may, on at least thirty (30) days' prior written notice, audit FyneDesk's compliance with this DPA. Each such audit is subject to the following: (a) no more than one Customer-initiated audit per calendar year per Customer; (b) the audit is conducted during FyneDesk's normal business hours at FyneDesk's premises (or, at FyneDesk's election, remotely); (c) the audit is conducted by an independent, mutually agreed auditor that is not a competitor of FyneDesk and that is bound by confidentiality obligations no less protective than those binding Customer under the Agreement; (d) the audit is reasonable in scope and duration, takes into account the nature of FyneDesk's services to its other customers, and does not unreasonably interfere with FyneDesk's operations; (e) the audit does not provide access to other customers' data, to any data subject to legal privilege or third-party confidentiality obligations, or to areas that would compromise the security of FyneDesk's facilities or other customers; (f) Customer bears the reasonable costs of the audit, including reasonable cost reimbursement of FyneDesk's personnel time; and (g) audit reports and other information disclosed in connection with the audit are FyneDesk's Confidential Information. Audits required by a binding direction of a Supervisory Authority or other competent authority are not subject to the once-per-year limit in clause (a) or the cost provisions in clause (f), and FyneDesk will cooperate with such direction to the extent required by applicable law.

8. International data transfers

8.1 Mechanisms

FyneDesk is established in the United States. To the extent FyneDesk Processes Customer Personal Data that is subject to the GDPR or UK GDPR and the Processing involves a transfer of such data to a country outside the European Economic Area, Switzerland, or the United Kingdom (each, a "**Restricted Transfer**"), the transfer is subject to the safeguards in this Section 8.

FyneDesk transfers Customer Personal Data in reliance on the following mechanisms, in the order set out below:

- where the destination country is covered by a current European Commission adequacy decision (including the EU-U.S. Data Privacy Framework, while in effect), the adequacy decision;
- otherwise, the Standard Contractual Clauses (Module 2: Controller-to-Processor) for transfers from the EEA, and the UK Addendum for transfers from the United Kingdom, as described in **Annex IV**;
- otherwise, any other lawful transfer mechanism mutually agreed in writing.

8.2 Onward transfers to Sub-processors

For onward transfers from FyneDesk to its Sub-processors, FyneDesk uses Module 3 (Processor-to-Processor) of the Standard Contractual Clauses, the UK Addendum, or another lawful transfer mechanism. Customer is a third-party beneficiary of the data-protection clauses in FyneDesk's Module 3 SCCs with Sub-processors to the extent required by Clause 3 of the SCCs.

8.3 Transfer Impact Assessment cooperation

FyneDesk will provide Customer with the information reasonably necessary for Customer to conduct a Transfer Impact Assessment in respect of transfers under this DPA, including information about applicable laws of the destination country, supplementary measures in place, and FyneDesk's experience (if any) of government access requests.

9. CCPA: California-specific terms

This Section 9 applies where Customer is a "Business" and Customer Personal Data includes Personal Information (as defined in the CCPA) of California Consumers. The terms of this Section 9 are intended to satisfy the contractual requirements of Cal. Civ. Code § 1798.140(ag) and the California Privacy Protection Agency's regulations at Cal. Code Regs. tit. 11, §§ 7050–7053. To the extent of any conflict between this Section 9 and the rest of this DPA with respect to such data, this Section 9 controls.

FyneDesk is a "Service Provider" within the meaning of Cal. Civ. Code § 1798.140(ag). FyneDesk receives Personal Information from Customer for the limited and specified business purpose of providing the Service to Customer in accordance with the Agreement. **FyneDesk certifies that it understands the restrictions set forth in Cal. Civ. Code § 1798.140(ag)(1)(A) through (D) and in this Section 9, and that it will comply with those restrictions.**

FyneDesk shall not:

- **Sell or share** Personal Information received from or on behalf of Customer (as those terms are defined in the CCPA);
- **Retain, use, or disclose** the Personal Information for any purpose other than for the business purposes specified in the Agreement, including for any commercial purpose other than the business purpose, or outside of the direct business relationship between Customer and FyneDesk;

- **Combine** the Personal Information that FyneDesk receives from or on behalf of Customer with Personal Information that FyneDesk receives from another source, except as permitted by the CCPA;
- **Use** the Personal Information for FyneDesk's own commercial purposes other than to perform the Service.

FyneDesk shall provide the same level of privacy protection to Personal Information as is required of businesses by the CCPA and its implementing regulations. Customer has the right, on reasonable notice, to take reasonable and appropriate steps to ensure that FyneDesk uses Personal Information transferred under the Agreement in a manner consistent with Customer's obligations under the CCPA. These steps are satisfied by Customer's exercise of the audit rights described in Section 7 of this DPA.

FyneDesk will notify Customer if FyneDesk determines that it can no longer meet its obligations under the CCPA. On notice from Customer following such a determination, or following Customer's reasonable determination that FyneDesk is making unauthorized use of Personal Information, Customer may take reasonable and appropriate steps to stop and remediate the unauthorized use, including by exercising rights under the Agreement.

FyneDesk will assist Customer in responding to verifiable consumer requests under the CCPA in accordance with Section 3.4. With respect to Sensitive Personal Information, FyneDesk will not use, retain, or disclose such information for any purpose other than those expressly permitted under Cal. Code Regs. tit. 11, § 7027(m), and will not derive information from Sensitive Personal Information for the purpose of inferring characteristics about a Consumer.

10. Liability and indemnification

10.1 Aggregate cap

Each party's total cumulative liability arising out of or related to this DPA (including all Annexes, the Standard Contractual Clauses, and the UK Addendum), whether in contract, tort, or under any other theory of liability, is subject to the exclusions and limitations of liability set out in the Agreement, including the limitation of liability in Section 13 of the Terms of Service. The liability cap and exclusions in the Agreement apply in aggregate to all claims under the Agreement and this DPA taken together, and not separately. As between the parties, claims under or in connection with the Standard Contractual Clauses or the UK Addendum (other than claims brought directly by a Data Subject) are subject to the same aggregate cap. Nothing in this Section 10.1 limits the rights of Data Subjects under Clause 12 of the Standard Contractual Clauses, Article 82 GDPR, or equivalent statutory provisions.

10.2 Regulatory fines

Each party is responsible for any administrative fines imposed on it directly by a Supervisory Authority under Article 83 GDPR, Article 84 GDPR, the UK GDPR, the CCPA, or any equivalent provision of applicable Data Protection Laws, and neither party is liable to the other for fines imposed on the other party, except where (and to the extent that) such fine was caused by the other party's documented breach of this DPA. Any contribution or recovery between the parties under this Section 10.2 is in all cases subject to the limitations of liability in Section 10.1.

10.3 Statutory data subject rights

Nothing in this DPA or the Agreement limits or excludes any right that a Data Subject may have to compensation from a controller or processor under Article 82 GDPR, Article 82 UK GDPR, or equivalent statutory provisions. As between the parties, allocation of responsibility for Article 82 claims follows the responsibility for the underlying breach under this DPA, subject to the limitations of liability in Section 10.1.

10.4 Mutual indemnification

Customer's indemnity. Customer will defend, indemnify, and hold harmless FyneDesk and its Affiliates, and their respective officers, directors, employees, and agents, from and against any third-party claims, demands, actions, proceedings, losses, damages, fines, penalties, liabilities, costs, and expenses (including reasonable legal fees) arising out of or in connection with: (a) the content of Customer Personal Data submitted to the Service by or on behalf of Customer, including any claim that Customer Personal Data infringes any third-party right or violates applicable law; (b) Customer's instructions to FyneDesk, including instructions that infringe applicable Data Protection Laws; (c) Customer's failure to provide all notices and obtain all consents, authorizations, and other rights required under applicable Data Protection Laws; (d) Customer's failure to comply with its own notification obligations under applicable Data Protection Laws; or (e) Customer's breach of Section 6 of this DPA. Customer's indemnity does not apply to claims to the extent caused by FyneDesk's Willful Misconduct or breach of this DPA.

FyneDesk's indemnity. FyneDesk will defend, indemnify, and hold harmless Customer from and against direct third-party claims to the extent caused by FyneDesk's Willful Misconduct in the performance of this DPA. FyneDesk's indemnity under this Section 10.4 is subject to the limitations of liability in Section 10.1.

Procedures. The party seeking indemnification (the "Indemnified Party") will: (i) promptly notify the indemnifying party (the "Indemnifying Party") in writing of any claim for which indemnification is sought; (ii) grant the Indemnifying Party sole control of the defense and settlement of the claim, provided that no settlement that imposes any non-monetary obligation, admission, or unindemnified financial obligation on the Indemnified Party may be entered without the Indemnified Party's prior written consent (not to be unreasonably withheld); and (iii) provide reasonable cooperation, at the Indemnifying Party's expense. Failure to provide prompt notice will not relieve the Indemnifying Party of its obligations except to the extent the Indemnifying Party is materially prejudiced by the delay.

10.5 Definitions and statutory carve-outs

"**Willful Misconduct**" means conduct intentionally undertaken with knowledge that the conduct is substantially certain to cause, or with conscious and reckless disregard of the probability that the conduct will cause, harm to the other party. For clarity, an ordinary breach of contract, including a breach known to be likely at the time of performance, does not constitute Willful Misconduct.

Nothing in this DPA, the Agreement, or any limitation of liability operates to exclude or limit any liability that cannot be excluded or limited under applicable law, including liability for fraud, willful injury to the person or property of another, or violation of law where applicable law prohibits exclusion or limitation of such liability (including under California Civil Code § 1668).

11. Term and termination

This DPA takes effect on the date Customer accepts the Agreement and continues for the duration of the Agreement. The following Sections survive termination or expiry of the Agreement: Section 1 (Definitions), Section 3.6 (Return and deletion) for so long as FyneDesk retains Customer Personal Data, Section 6 (Customer's obligations and warranties), Section 7 (Audits) for the period during which Customer Personal Data is retained, Section 9 (CCPA) with respect to Personal Information then retained, Section 10 (Liability and indemnification), Section 11, Section 12 (General), the Standard Contractual Clauses and the UK Addendum to the extent applicable, and any other terms that by their nature should survive.

12. General

12.1 Order of precedence

In the event of any conflict between this DPA and the Agreement, this DPA controls solely with respect to the Processing of Customer Personal Data. The Standard Contractual Clauses and the UK Addendum (where applicable) prevail over any conflicting term of this DPA or the Agreement to the extent of the conflict. Section 9 (CCPA) prevails over any conflicting term of this DPA solely with respect to Personal Information of California Consumers.

12.2 Changes

FyneDesk may modify this DPA from time to time. Where the modification is not material, FyneDesk will update the "Last updated" date. Where the modification is material — including any change that materially diminishes Customer's rights or FyneDesk's obligations under this DPA — FyneDesk will provide at least thirty (30) days' prior notice to Customer (which may be by email or by posting an updated DPA on this page and notifying Customer of the change), and the modification will take effect at the end of that period unless Customer terminates the affected portion of the Service before then, in which case Customer will receive a pro-rated refund of any prepaid fees for the period after termination. Continued use of the Service after a modification takes effect constitutes acceptance of the updated DPA. FyneDesk will not modify Annex II (Technical and Organizational Measures) in a manner that materially diminishes the level of protection without Customer's consent, except where required by applicable law. FyneDesk will not make any modification that conflicts with the Standard Contractual Clauses or the UK Addendum.

12.3 Governing law

This DPA is governed by the laws of the State of California, United States, in accordance with Section 16 of the Terms of Service, except that the Standard Contractual Clauses are governed by the law specified in Annex IV, and the UK Addendum is governed by the laws of England and Wales. Nothing in this Section 12.3 limits the rights of Data Subjects under applicable Data Protection Laws.

12.4 Entity status and assignment

"FyneDesk" is the operating name under which the Service is currently offered. The legally-bound counterparty under this DPA and the Agreement is the operator of FyneDesk identified at the address in Section 13, doing business as "FyneDesk." FyneDesk intends to incorporate a successor legal entity to assume the operator's rights and obligations under the Agreement and this DPA, and may assign this DPA and the Agreement to any such successor entity (including following incorporation, reorganization, or merger) on notice to Customer. From the effective date of such assignment, references to "FyneDesk" in this DPA refer to the successor entity. Customer may not assign this DPA or the Agreement without FyneDesk's prior written consent, except to an Affiliate or in connection with a merger, acquisition, or sale of all or substantially all of Customer's business.

13. Contact

Questions about this DPA, including requests for a signed counterpart, security documentation, audit support, or assistance with Data Subject requests, may be directed to:

FyneDesk — Data Protection
San Jose, California, United States
Email: support@fynedesk.io
Sub-processor list: fynedesk.io/subprocessors

Privacy Policy: fynedesk.io/privacy

Annex I — Details of Processing

Subject matter and duration

Subject matter: FyneDesk's provision of the helpdesk and ITSM Service to Customer, including ticket management, customer portal, knowledge base, live chat, email-to-ticket, AI-assisted features, asset management, and related functionality as described in the Agreement. Duration: the term of the Agreement, plus the return/deletion period set out in Section 3.6.

Nature and purpose

Nature: hosting, transmission, storage, retrieval, indexing, analysis, and related Processing of Customer Personal Data necessary to operate the Service. Purpose: enabling Customer to manage support and service requests and related operations.

Categories of Data Subjects

- Customer's employees, contractors, and authorized agents (helpdesk operators and administrators);
- Customer's end users and customers who submit support requests or otherwise interact with the Service;
- Other individuals whose Personal Data appears in tickets, messages, attachments, contact records, or other Customer-submitted content.

Categories of Personal Data

- Identification and contact data (name, email address, phone number, job title, organization);
- Authentication and account data (user IDs, login timestamps, IP addresses, multi-factor authentication data);
- Ticket and message content, including any Personal Data that Data Subjects voluntarily include in such content;
- Attachments and other files uploaded to the Service;
- Asset, device, and configuration records where Customer uses the ITSM/asset features;
- Service usage data (pages viewed, actions taken, session metadata);
- Any other Personal Data that Customer or its Data Subjects choose to submit to the Service.

Special categories of Personal Data

The Service is not designed for the Processing of special-category Personal Data within the meaning of Article 9 GDPR. Customer represents and warrants in Section 6 that it will not submit such data unless separately agreed.

Frequency of Processing

Continuous, for the term of the Agreement.

Retention

For the term of the Agreement, plus the return/deletion period set out in Section 3.6 and any longer retention required by applicable law or by Sub-processor standard deletion timelines.

Annex II — Technical and Organizational Measures

FyneDesk implements and maintains the technical and organizational measures described below. These measures apply to FyneDesk's Processing of Customer Personal Data. Specific measures may be updated from time to time provided that the level of protection is not materially diminished.

Encryption

- Customer Personal Data is encrypted in transit using TLS 1.2 or higher.
- Customer Personal Data at rest is encrypted using industry-standard algorithms (AES-256 or equivalent), including database storage and backups.
- Authentication credentials are stored using one-way hashing with industry-accepted key derivation functions.

Access controls and identity management

- Role-based access control restricts FyneDesk personnel access to Customer Personal Data to those who require it for their role.
- Multi-factor authentication is required for FyneDesk personnel access to production systems.
- Access is reviewed periodically and revoked promptly on role change or termination.
- Customer-facing administrators may configure roles, permissions, and (on supported plans) single sign-on and multi-factor authentication for their own users.

Confidentiality, integrity, availability, and resilience

- Personnel are bound by written confidentiality obligations.
- Production systems are logically segregated from development and test environments.
- Customer Personal Data is logically segregated by Customer (multi-tenant isolation).
- Backups are taken at least daily and tested periodically.
- Disaster recovery procedures are documented and reviewed at least annually.

Pseudonymization and minimization

- Where feasible, FyneDesk pseudonymizes Personal Data in logs, analytics, and diagnostic systems.
- Data minimization principles are applied to system telemetry and operational logging.

Network and infrastructure security

- Production infrastructure is hosted on enterprise-grade cloud providers with established security certifications (such as SOC 2 Type II and ISO 27001).
- Network access is restricted by allowlists, security groups, and least-privilege principles.
- Web application defenses, including WAF and rate limiting, protect against common application-layer attacks.
- Logging and monitoring detect anomalous activity; alerts are reviewed by FyneDesk personnel.

Vulnerability management

- Software dependencies are scanned for known vulnerabilities; remediation is prioritized by severity.
- Penetration testing is conducted at least annually by qualified third parties.
- Critical operating-system and platform updates are applied on a defined cadence.

Personnel

- Pre-employment background checks are conducted where permitted by law.
- Security and privacy training is delivered on hire and annually thereafter.
- Personnel access to Customer Personal Data is logged.

Vendor and Sub-processor management

- Sub-processors are subject to written data protection commitments designed to provide a level of protection materially equivalent to those in this DPA.
- FyneDesk maintains and publishes a current Sub-processor list at fynedesk.io/subprocessors.

Incident response

- Documented incident response procedures cover detection, containment, eradication, recovery, and post-incident review.
- Personal Data Breaches are notified to Customer in accordance with Section 5.2.

Deletion and decommissioning

- Production and backup deletion follow Section 3.6 of this DPA.
- Decommissioned media is sanitized or destroyed in accordance with industry guidance.

Annex III — Sub-processor Categories

The categories of authorized Sub-processors are set out in Section 4.1 of this DPA. The current list of named Sub-processors, including each Sub-processor's purpose, primary processing region, and a link to its own data protection terms, is published at fynedesk.io/subprocessors and forms part of this DPA by reference. The list is updated from time to time in accordance with Sections 4.2 and 4.3.

Annex IV — Transfer Mechanisms

Standard Contractual Clauses (EU)

Where the Standard Contractual Clauses apply under Section 8, the parties incorporate the Standard Contractual Clauses set out in Commission Implementing Decision (EU) 2021/914 by reference. Module 2 (Controller-to-Processor) applies as between Customer (as data exporter) and FyneDesk (as data importer). Module 3 (Processor-to-Processor) applies as between FyneDesk and its Sub-processors.

- **Clause 7 (Docking clause):** applies.

- **Clause 9 (Use of sub-processors):** Option 2 (general written authorization) applies, with the thirty (30) days' notice period set out in Section 4.2.
- **Clause 11 (Redress) optional language:** does not apply.
- **Clause 17 (Governing law):** Option 1 — the laws of Ireland.
- **Clause 18 (Choice of forum and jurisdiction):** the courts of Ireland.
- **Annex I.A (List of Parties):** Customer is the data exporter; FyneDesk is the data importer. Contact details are those provided in the Agreement and (for FyneDesk) in Section 13 above.
- **Annex I.B (Description of Transfer):** as set out in Annex I of this DPA.
- **Annex I.C (Competent Supervisory Authority):** the supervisory authority of the EU/EEA Member State in which the data exporter is established; where the data exporter is not established in the EU/EEA, the Irish Data Protection Commission (DPC) is the default competent Supervisory Authority pursuant to Clause 13 of the Standard Contractual Clauses.
- **Annex II (Technical and Organizational Measures):** as set out in Annex II of this DPA.
- **Annex III (List of Sub-processors):** as published at fynedesk.io/subprocessors.

UK Addendum

Where the UK Addendum applies under Section 8, the parties incorporate the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0) by reference, with the following completions:

- **Table 1 (Parties):** Customer (data exporter) and FyneDesk (data importer); contact details as set out in the Agreement and Section 13.
- **Table 2 (Selected SCCs, Modules and Selected Clauses):** the SCCs as referenced above, with Module 2 (and Module 3 as applicable), Clause 7 in, Clause 9 Option 2 (30-day notice), Clause 11 optional out, Clause 17 Option 1 governed by Ireland.
- **Table 3 (Appendix Information):** the Annexes to the SCCs are completed as set out in Annex I and Annex II of this DPA, and at fynedesk.io/subprocessors.
- **Table 4 (Ending this Addendum when the Approved Addendum Changes):** the data exporter may end the Addendum pursuant to Section 19 of the Approved Addendum.

Swiss FADP

Where Customer Personal Data is subject to the Swiss Federal Act on Data Protection ("FADP"), the Standard Contractual Clauses apply with the following adaptations: (a) references to the GDPR are read as references to the FADP where relevant; (b) the supervisory authority is the Swiss Federal Data Protection and Information Commissioner; and (c) the term "Member State" is read to include Switzerland.

This DPA is provided as a working legal document. It does not constitute legal advice. Customers operating in regulated industries or processing higher-risk categories of data should obtain independent legal advice and may request a signed counterpart by contacting support@fynedesk.io.