Data Processing Agreement

HOW THIS DPA TAKES EFFECT

This Data Processing Agreement (“DPA”) forms part of the Terms of Service between Shiftic AB, 5594512666 (“Shiftic”) and the legal entity or individual (“Customer”) that accesses or uses Shiftic’s subscription plans.

- This DPA does not require a physical signature.
- It enters into force automatically when the Customer activates a self-serve or enterprise subscription, whether through account creation, payment, or commencement of use of the Service.
- By using the Service, the Customer acknowledges that it has read, understood, and agrees to be bound by this DPA.
- If you are entering into this DPA on behalf of a company or other legal entity, you represent that you have authority to bind that entity.

1. Parties

This DPA is entered into between Shiftic AB , Reg. No. 559451-2666, Plantagegatan 19, 216 16 Limhamn, Sweden (“Shiftic”, “Processor”), and the Customer as identified in the self-serve or enterprise subscription account (“Controller”). The Parties are hereinafter jointly referred to as the “Parties”.

2. Background

The Customer has subscribed to Shiftic’s services under Shiftic’s Terms of Service (the “Subscription Agreement”), which require Shiftic to process certain Personal Data on behalf of the Customer.

This DPA sets out the requirements and conditions under which Shiftic will process Personal Data when providing services under the Subscription Agreement. It contains the mandatory clauses required by Article 28(3) of Regulation (EU) 2016/679 (GDPR) for contracts between controllers and processors.

3. Definitions

The following terms have the meanings set out below:

Applicable Data Protection Legislation	All laws applicable to any personal data processed under or in connection with this DPA.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Processing, Supervisory Authority	Have the meanings given to them in the Applicable Data Protection Legislation.
Service / Services	The Shiftic platform and related services provided by Shiftic under the Subscription Agreement.
Subscription Agreement	The Terms of Service agreed to by the Customer upon account creation or subscription activation.

4. Description of Processing

In relation to the processing of personal data carried out by Shiftic on behalf of Customer:

- The subject matter, nature, categories of personal data, and relevant data subjects are set out in Annex A.
- The purpose of the processing is to enable Shiftic to perform the Services under the Subscription Agreement.
- The duration of the processing will be throughout the period within which Shiftic provides the Services under the Subscription Agreement.
- The obligations and rights of the data controller in relation to the processing are set out in this DPA.

5. Compliance with Applicable Data Protection Legislation

Each of the Customer and Shiftic will comply with (and shall ensure that its staff and/or subcontractors comply with) all obligations applying directly to that Party under the applicable data protection legislation.

6. Relationship and Roles of the Parties

The Customer and Shiftic agree and acknowledge that for the purpose of the Data Protection Legislation:

- The Customer is the Controller and Shiftic is the Processor.
- The Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to providing any required notices and obtaining any required consents, and for the written processing instructions it gives to Shiftic.
- Annex A describes the subject matter, duration, nature and purpose of the processing, and the Personal Data categories and Data Subject types in respect of which Shiftic may process the Personal Data to fulfil the agreed purpose.

7. Processing of Personal Data by Shiftic on Behalf of Customer

In relation to the processing of personal data by Shiftic on behalf of the Customer, the following terms shall apply:

7.1 Documented Instructions from Customer (Article 28(3)(a) GDPR)

Shiftic will process the personal data only on documented instructions from the Customer, including with regard to transfers of the personal data to a third country, unless required to do so by UK, EU, or member state law to which Shiftic is subject. In such a case, Shiftic will inform the Customer of the relevant legal requirement unless the law prohibits Shiftic from doing so for reasons of important public interest.

7.2 Confidentiality (Article 28(3)(b) GDPR)

Shiftic will ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, unless the Customer or this DPA specifically authorises the disclosure, or as required by Applicable Data Protection Legislation, court, or regulator.

Shiftic will ensure that all of its employees:

- are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data; and
- are aware of both Shiftic's duties and their personal duties and obligations under the Data Protection Legislation and this DPA.

7.3 Technical and Organisational Measures (Article 28(3)(c) and Article 32 GDPR)

Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood

and severity for the rights and freedoms of natural persons, Shiftic shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to the personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Shiftic has implemented the security measures set out in Annex B.

7.4 Engagement of Sub-Processors (Article 28(3)(d) and Article 28(2) GDPR)

Shiftic maintains a list of approved sub-processors available shiftic.com/legal/sub-processors. Shiftic will notify Customers by email at least 30 days prior to engaging any new sub-processor. If a Customer reasonably objects to a new sub-processor on data protection grounds, the Customer may notify Shiftic in writing within that 30-day period and the Customer may terminate the Subscription Agreement on written notice without penalty. In all cases, Shiftic will:

- provide the Customer with reasonable advance notice of any new sub-processor, including the name, location, and nature of processing; and
- Shiftic enters into a written contract with the sub-processor that contains terms substantially the same as those set out in this DPA, in particular in relation to requiring appropriate technical and organisational data security measures, and, upon the Customer's written request, provides the Customer with copies of the relevant excerpts from such contracts.

Those sub-processors approved as at the commencement of this DPA are as set out in Annex A.

7.5 Obligations of Sub-Processors (Article 28(3)(d) and Article 28(4) GDPR)

Where Shiftic engages another processor for carrying out specific processing activities on behalf of the Customer, the same data protection obligations as set out in this clause 7 shall be imposed on that other processor by way of a contract which, in particular, provides sufficient guarantees to implement appropriate technical and organisational measures. Where that other processor fails to fulfil its data protection obligations, Shiftic shall remain liable to the Customer for the performance of that processor's obligations.

7.6 Assistance with Data Subject Rights (Article 28(3)(e) GDPR)

Taking into account the nature of the processing, Shiftic will assist the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising data subjects' rights laid down in Chapter III GDPR.

7.7 Assistance with Compliance (Article 28(3)(f) GDPR)

Upon reasonable written request and subject to Shiftic's reasonable resource constraints, Shiftic will assist the Customer in ensuring compliance with the Customer's obligations under Articles 32 to 36 GDPR to:

- ensure the security of the processing;
- notify the relevant supervisory authority, and any data subject(s) where relevant, of any breaches relating to personal data;
- carry out any data protection impact assessments of the impact of the processing on the protection of personal data; and
- consult the relevant supervisory authority prior to any processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the Customer to mitigate that risk;

taking into account the nature of the processing and the information available to Shiftic.

7.8 Return or Deletion of Personal Data (Article 28(3)(g) GDPR)

Upon termination or expiry of the Subscription Agreement, Shiftic will delete all Personal Data processed on behalf of the Customer within a reasonable period, unless EU or member state law requires continued storage. Where the Service includes a data export feature, the Customer is responsible for exporting any Personal Data they wish to retain prior to termination.

7.9 Demonstrating Compliance (Article 28(3)(h) GDPR)

Shiftic will make available to the Customer all information reasonably necessary to demonstrate compliance with the obligations set out in this clause 7, including by sharing relevant security certifications, audit reports , or responses to standard security questionnaires upon written request. Physical audits or on-site inspections are not available under self-serve plans unless required by applicable mandatory law; Customers requiring audit access should contact Shiftic to discuss enterprise arrangements.

7.10 Personal Data Breach (Article 33(2) GDPR)

Shiftic shall notify the Customer without undue delay (and in any event within 72 hours) after becoming aware of a personal data breach in relation to the personal data

processed by Shiftic on behalf of the Customer and shall, to the extent known by Shiftic:

- describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of Shiftic's data protection contact point where more information can be obtained;
- describe the likely consequences of the personal data breach; and
- describe the measures taken or proposed to be taken by Shiftic to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Shiftic's initial notification will contain the details of the breach then known to Shiftic. Where it is not possible to provide all required information at the same time, Shiftic shall provide the remaining information in phases as it becomes available and without undue further delay.

8. Term and Termination

This DPA will remain in full force and effect so long as:

- the Subscription Agreement remains in effect; or
- Shiftic retains any Personal Data related to the Subscription Agreement in its possession or control in accordance with the Subscription Agreement.

9. Liability

The Parties acknowledge that their respective liability towards data subjects, as well as their exposure to administrative fines from a supervisory authority, shall be governed by the applicable provisions of the GDPR, including Article 82. The limitations set forth in this clause shall not apply to such fines or to the Parties' liability towards data subjects.

- Subject to the exclusions below, Shiftic's total aggregate liability to the Customer, whether in contract, tort (including negligence), or otherwise, arising out of or in connection with any breach of this DPA or any Personal Data Breach, shall be limited to the higher of an amount equal to the total fees paid or payable by the Customer to Shiftic under the Subscription Agreement in the twelve (12) month period preceding the event giving rise to the claim and 1 000 EUR..

The limitation of liability set out in this clause 9 shall not apply to liability arising from:

- a Party's wilful misconduct or gross negligence; or
- any breach of its confidentiality obligations under the Subscription Agreement.

In no event shall Shiftic be liable to the Customer under this DPA for any indirect, incidental, or consequential damages, including but not limited to loss of profits, revenue, data, or business opportunities.

Where both Parties are responsible for the event giving rise to the damage, the liability shall be apportioned between them according to their respective degree of responsibility.

10. Changes to this DPA

Shiftic may update this DPA from time to time to reflect changes in applicable law, regulatory guidance, or our processing activities. Where changes are material, Shiftic will provide notice to Customers via email or through the Service at least 30 days prior to the changes taking effect. Continued use of the Service after the effective date of an updated DPA constitutes acceptance of the updated terms.

The current version of this DPA is published at shiftic.com/legal/dpa and the effective date is indicated at the top of the document.

11. Governing Law

This DPA shall be governed by and construed in accordance with the laws of Sweden. Any disputes arising under or in connection with this DPA shall be subject to the exclusive jurisdiction of the Swedish courts, unless otherwise required by applicable data protection law.

12. Contact

For questions about this DPA or to exercise any rights in connection with it, please contact Shiftic at: Shiftic AB, Plantagegatan 19, 216 16 Limhamn, Sweden, privacy@shiftic.com

ANNEX A

Details of Processing Activities

A.1 Subject Matter and Purpose

The subject matter of the processing is the provision of the Shiftic platform — an AI-powered platform for organisational change management. The purpose of the processing is to enable Shiftic to deliver the Services to the Customer.

A.2 Duration

Processing will continue throughout the term of the Subscription Agreement and any post-termination period during which Shiftic retains Personal Data in accordance with clause 7.8 of this DPA.

A.3 Nature of Processing

Collection, storage, use, retrieval, and deletion of personal data as necessary to provide the Services. This may include hosting, analysis of usage data, AI-assisted processing of content entered by users, and communications related to the Services.

A.4 Categories of Personal Data

Depending on how the Customer and its users interact with the Service, the following categories of personal data may be processed:

- Identification and contact data: names, work email addresses, job titles.
- Account and usage data: login credentials (hashed), activity logs, feature usage.
- Content data: text, notes, or other content entered by users into the platform.
- Communications data: email correspondence related to support or service delivery.

A.5 Categories of Data Subjects

Data subjects may include:

- Employees, contractors, or agents of the Customer who are registered as users of the Service.
- Other individuals whose personal data is entered into the platform by the Customer or its users.

A.6 Approved Sub-Processors

As at the effective date of this DPA, Shiftic uses the following categories of sub-processors:

- Cloud infrastructure providers (for hosting and data storage).
- AI model providers (for AI-assisted features within the platform).
- Analytics and monitoring providers (for platform performance and security monitoring).
- Email delivery providers (for transactional communications).

A current list of approved sub-processors is available at shiftic.com/legal/sub-processors

ANNEX B

Technical and Organisational Security Measures

Shiftic has implemented the following technical and organisational measures to protect Personal Data:

B.1 Access Controls

- Individual user accounts enforced for all personnel, provisioned on the principle of least privilege. Access rights are reviewed quarterly and all changes are logged.
- Multi-factor authentication (MFA) required for all personnel accessing systems that handle Personal Data, enforced via a centralised identity provider.
- Centralised logging via Azure Log Analytics Workspace, with comprehensive monitoring of security events across production systems.
- Privileged Identity Management (PIM) implemented via Microsoft Entra, with privileged accounts separated from standard operational accounts. Password policies meet industry standards for length, complexity, and rotation.

B.2 Data Security

- Encryption of Personal Data in transit using TLS 1.2/1.3. Encryption of Personal Data at rest using AES-256. Secure key storage is in place.
- Network segmentation via isolated virtual networks per environment and service. DDoS mitigation in place. Endpoints are monitored via Vanta agent; remote work governed by endpoint security and device encryption policies.
- Vulnerability management using Static Application Security Testing (Snyk), Dynamic Application Security Testing (OWASP ZAP), dependency scanning via GitHub Dependabot, malware scanning on Blob Storage, and vulnerability scanning of container images. Penetration testing is performed regularly and after significant changes. Microsoft Defender for Cloud is active across infrastructure.

B.3 Organisational Measures

- Mandatory security awareness training at onboarding, with annual refreshers. Training completion rates are tracked as a key performance indicator.
- Written confidentiality agreements for all employees and contractors. A documented offboarding process ensures prompt access revocation and return of equipment upon departure.

- Documented incident response plan with defined escalation procedures and assigned key personnel. An Information Security Management System (ISMS) aligned with ISO/IEC 27001 principles is in place, supported by Vanta, with the COO serving as security responsible. Risk assessments are conducted quarterly against a maintained risk register.

B.4 Business Continuity

- Regular backups of Personal Data with documented and tested restoration procedures. Backup policies have been reviewed and tested.
- Business continuity and disaster recovery plans in place for core systems. Change management is handled through a structured Git-based process with mandatory peer review and full audit trails. Infrastructure uses ephemeral servers to reduce recovery time.

B.5 Vendor Management

- Security assessment of all sub-processors prior to onboarding. Cloud infrastructure is hosted in ISO 27001-certified data centres.
- Contractual data protection obligations imposed on all sub-processors. Only the minimum data necessary to fulfil contractual obligations is collected and processed. Synthetic or anonymised data is used in test and development environments; no customer Personal Data is used for development or testing purposes.

B.6 Secure Development Lifecycle

- Security is embedded throughout the product development cycle. All code changes require mandatory peer review before deployment.
- Continuous integration and deployment (CI/CD) pipelines with automated security checks, including static code analysis, dependency vulnerability scanning (GitHub Dependabot), and semi-automated patch management.
- Containers are hardened, version-controlled, and run on ephemeral servers. Service principal authentication is used in preference to API keys or secret-based authentication where applicable.

The specific measures implemented may be updated over time to reflect improvements in security practices.