

Data Processing Agreement

Version 2026-09-22 · Effective 2026-09-22
<https://www.sandhed.com/dpa>

Application of this agreement

This Data Processing Agreement forms part of your agreement with Sandhed Group Ltd. It applies when Sandhed processes personal data on behalf of your organisation. Your Order, the enabled features and your documented instructions define the processing. If this agreement conflicts with other contract terms on personal-data processing, this agreement takes precedence. Existing separately signed data processing agreements continue to govern their covered services.

1. Scope, roles and duration

Your organisation is the controller, or a processor authorised by its controller, and Sandhed is the processor or subprocessor. Processing covers hosting, storing, organising, retrieving, displaying, analysing, transmitting, exporting and deleting data needed to provide the Sandhed service. It continues for the subscription and the applicable return, deletion and backup periods.

2. Data and people covered

Depending on the features you enable, data includes user names, business contact details, account identifiers, role and access records, device identifiers, operational records, equipment and location data, documents, images, support content, and AI inputs and outputs. Data subjects include your users, employees, contractors and people whose data you lawfully submit. Do not submit special-category or criminal-offence data unless a separate written agreement expressly covers it.

3. Documented instructions

Sandhed processes data only to provide the agreed service and follow your documented instructions, including instructions given through authorised users and configured integrations. You are responsible for the lawfulness of collection, notices, permissions and instructions. Sandhed informs you if an instruction appears to infringe data-protection law. If law requires other processing, Sandhed informs you before processing unless that law prohibits notice. Sandhed does not use Customer Data to train its own AI models.

4. Confidentiality and security

Sandhed limits access to authorised people who need it for their work and who are bound by confidentiality obligations. Sandhed maintains measures appropriate to the risk, including encrypted transport, role-based access, separation of customer access, protection of credentials, logging, backup and recovery procedures, vulnerability management and incident response. Sandhed reviews these measures and does not materially reduce the protection of Customer Data during the agreement. Customers control their user access, integration permissions and lawful use of location and employee data.

5. Personal-data breaches

Sandhed notifies your designated contact without undue delay after becoming aware of a personal-data breach affecting Customer Data. The notice describes the known nature and likely consequences, affected data and people where available, measures taken or proposed, and a contact for follow-up. Information may be supplied in stages as the investigation proceeds. Sandhed assists your response; you determine any notifications to authorities or individuals that fall within your responsibilities.

6. Rights, assistance and audits

Taking account of the processing and available information, Sandhed helps you respond to data-subject requests and meet your obligations concerning security, breach reporting, impact assessments and prior consultation. Requests received directly are referred to you unless law requires otherwise. Sandhed provides information needed to demonstrate compliance and permits audits, including inspections, by you or an independent auditor bound by confidentiality. Routine audits are arranged with reasonable notice and safeguards for security and other customers; these arrangements do not restrict urgent investigations or a supervisory authority's powers.

7. Subprocessors and transfers

You give general authorisation for the subprocessors listed on the linked provider page. Sandhed gives at least 30 days' notice before adding or replacing a subprocessor, allowing you to object on reasonable data-protection grounds. The parties work to resolve an objection before the change applies to your data; if no reasonable alternative is available, you may terminate the affected service before that change. Sandhed imposes equivalent data-protection obligations and remains responsible for its subprocessors' performance. Transfers outside the EEA use an applicable adequacy decision or appropriate safeguards, including standard contractual clauses and supplementary measures where required. Relevant UK transfers use safeguards recognised under UK law.

8. Return, deletion and retained records

At the end of processing, you may choose return or deletion of Customer Data, subject to applicable law. Available export functions remain usable during the contractual recovery period. For self-service subscriptions, the access, export, warning and deletion timetable in section 21 of the Terms applies. Backup copies are isolated from normal use and removed under the applicable backup cycle. Where law requires retention, Sandhed limits further processing to that purpose. Sandhed acts as an independent controller for its own billing, tax, account-security and business-contact records; those records follow the Privacy Policy.

9. Contact and governing terms

Send processing instructions, security concerns and requests concerning this agreement to legal@sandhed.com. The liability and governing-law provisions of your agreement with Sandhed apply, subject to mandatory data-protection law and the rights of individuals and supervisory authorities.

Subprocessor list

Contracting company

Sandhed Group Ltd. Unit No. S140, SOHO The Strand, Fawwara Building, Triq L-Imsida, Gzira GZR1401, Malta

Company registration: C116249 VAT number: MT33018730

Related documents

[Terms of Service](#) · [Subprocessor list](#) · [Privacy Policy](#)

Questions about these documents? Contact legal@sandhed.com.