runbox

# Data Processing Agreement

**in accordance with Norwegian Personal Data Act that incorporates the GDPR**

Last modified: November 1, 2026

This Data Processing Agreement (this **Agreement**) is in accordance with GDPR Art. 28, and is a supplement to the **Contract for Services** between the **Customer** (a Natural Person or as a Company or organization of any legal form, referred to as the **Controller**) and Runbox Solutions AS (**Runbox,** referred to as the **Processor**), accepted by the **Customer** by signing up for the **Services,** and explicitly accepted the **Terms of Service.**

In this **Agreement**, the **Controller** (Customer) and **Processor** (Runbox) together are referred to as the **Parties**.

The **Personal Data Act** (*personopplysningsloven*) is the Norwegian law that regulates how the personal data of natural persons shall be processed. The law incorporates the EU General Data Protection Regulation (GDPR) in Norwegian law. The Regulation is thus part of the Personal Data Act and applies as Norwegian law.

## The Agreement

### 1. Background and scope

1.1 The **Controller** uses **Runbox**'s email, domain, web hosting, file storage, or related services (**Services**). In providing the **Services**, **Runbox** may process personal data on behalf of the Controller.

1.2 This DPA regulates such processing in accordance with the GDPR, as implemented and applicable in Norway through the EEA framework and the Norwegian Personal Data Act.

### 2. Defintions and Interpretations

2.1 The terms Controller, Processor, Data Subject, Personal Data, Processing, Subprocessor. Supervisory Authority shall have the same meaning as in the Norwegian Personal Data Act/GDPR.

2.2 The terms Account Content, Account information, Main account, Processes or Process, Sub-Account, and User Data shall have the same meaning as in the **Runbox**' **Terms of Service** and **Privacy Policy**.

### 3. Roles of the Parties

For personal data processed in the **Customer**'s account, mailbox, hosted domain, web hosting environment, file storage, address books, logs, or other Customer-controlled content, the **Customer** is the **Controller** and **Runbox** is the **Processor**.

**Runbox** may act as an independent controller for limited processing necessary for its own business purposes, such as account administration, billing, abuse prevention, legal compliance, security, and customer support, as described in Runbox's applicable privacy information.

### 4. Categories of Data Subjects and their rights

The **Controller**'s data subjects may include:

- The Controller's customers, family members, employees, contractors, representatives, suppliers, or other contacts.
- Senders and recipients of email handled through the Services.
- Visitors to websites hosted by or for the Controller.
- Authorized users of the Controller's account or domain.

This list is not meant to be exhaustive.

The **Processor** shall within reasonable technical and organizational measures, fulfill its obligations to Data Subject as given by the **Personal Data Act**/GDPR, including rights of access, rectification, erasure, restriction, portability, and objection, taking into account the nature of the processing and type of **Controller** (i.e. person, company).

## 5. Controller's obligations

The **Controller** shall:

1. Ensure that it has a valid legal basis for the personal data processed through the **Services**.
2. Provide lawful, documented instructions to Runbox.
3. Ensure that users are informed about processing where required.
4. Be responsible for the accuracy, legality, and retention of Customer-controlled personal data.
5. Configure the Services appropriately for its intended use, including account access, user permissions, authentication, domain settings, and retention practices.
6. Not submit personal data to the Services in violation of applicable law or the service agreement.

## 6. Processor's obligations

**Processor** shall:

1. Process personal data only on documented instructions from the **Controller**, unless necessary according to the **Contract for Services**, or required by applicable law.
2. Ensure that persons authorized to process the personal data are subject to confidentiality obligations.
3. Implement reasonable and appropriate technical and organizational security measures, taking into account the nature of the Services, risks to data subjects, and the state of the art.
4. Assist the Controller, insofar as reasonably possible, with data subject requests, security obligations, breach notifications, data protection impact assessments, and consultations with supervisory authorities.
5. Notify the Controller if, in Runbox's opinion, an instruction infringes applicable data protection law.
6. Delete or return personal data after termination as described in **Terms of Service**.

## 7. Security measures

In accordance with the GDPR Art. 32 (1) and (2), Runbox shall maintain appropriate technical and organizational measures designed to protect personal data against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration, or disclosure.

For details, see Runbox' website, www.runbox.com

## 8. Subprocessing

The **Controller** gives **Processor** general authorization to use sub-processors where necessary to provide, secure, support, or maintain the **Services**.

Processor shall ensure that sub-processors are bound by written agreement that contains requirements at a similar level as the Processor regarding processing of personal data, taken into consideration the tasks sub-processor it entitled to perform.

Processor shall make information about relevant sub-processors available to the Controller upon request.

## 9. International transfers

**Processor** shall not transfer personal data outside Norway, the EEA, or countries recognized as providing an EU adequate level of protection unless a valid transfer mechanism is in place, such as an EU approved Standard Contractual Clauses, or another lawful basis by GDPR.

Where a transfer is required by law, Processor shall inform the **Controller** before the transfer unless legally prohibited from doing so.

## 10. Personal data breaches

**Processor** shall notify the **Controller** without undue delay after becoming aware of a personal data breach affecting personal data processed on behalf of the Controller.

The notification shall, where reasonably available, include the nature of the breach, the categories and approximate number of data subjects and records affected, likely consequences of the breach, and measures taken or proposed to address the breach.

The **Controller** is responsible for assessing whether notification to Norwegian Data Protection Authorithy (Datatilsynet) or affected data subjects is required.

## 11. Return and deletion of data

Upon termination of the **Services**, Runbox shall, at the **Controller**'s choice and subject to the functionality of the Services, delete or make available for export personal data processed on behalf of the Controller within reasonable technical methods.

**Processor** may retain copies only where required by law, necessary for legitimate dispute handling, security, accounting, or compliance purposes, or where data remains in backups until overwritten according to established backup retention policies.

For more information, see **Runbox' Privacy Policy**.

## 12. Audit and documentation

**Processor** shall, upon written request and with good cause from the **Controller**, make available information reasonably necessary to demonstrate compliance with this DPA.

Audits or inspections may be conducted by the Controller or an independent auditor agreed by the **Parties**, provided that the audit is limited to processing relevant to the Controller, reasonable prior notice is given, and the audit does not compromise the security, confidentiality, or availability of Processor's systems or other customer's data.

The audit is conducted during normal business hours and at the Controller's cost, unless otherwise required by law.

**Runbox** may satisfy audit requests by providing relevant security and policies documentation, summaries, or written responses where appropriate.

## 13. Confidentiality

Each **Party** shall keep confidential any non-public information received from the other Party in connection with this DPA, including security information, technical documentation, business information, and personal data.

## 14. Liability

Liability under this DPA shall be governed by the **Contract for Services** between the **Parties**, unless otherwise required by applicable law.

Nothing in this DPA limits either **Party**'s liability where such limitation is prohibited by GDPR, the Norwegian Personal Data Act, or other applicable law.

runbox

## 14. Governing law and jurisdiction

This DPA is governed by Norwegian law, including the GDPR as applicable in Norway through the EEA framework and the Norwegian Personal Data Act.

In the case of disputes, the **Parties** shall seek solution(s) by negotiations. If the Parties, in spite of good will, is not able to solve the dispute, the dispute shall be handled by Norwegian court of competent jurisdiction.

## 15. Order of presedence

In the event of conflict between this DPA and the main service agreement, this DPA shall prevail with respect to the processing of personal data on behalf of the **Controller**. The **Contract for Services** shall continue to apply to commercial, technical, payment, and service-specific matters.

## 16. Communication between the Parties

All communication given under this **Agreement** must be in writing, sent by email or ordinary post to the addresses given on page 1 of this Agreement.

Each **Party** are obliged to notify the other Party in case of address changes.

## 17. Signatures

This DPA shall become effective when signed by both **Parties**.