Data Processing Agreement

Version 1.1.0, in force from 10 October 2026

Puraderi AB, organisation number 559435-0257, c/o Primepack, Orrekulla Industrigata 55B, 425 36 Hisings Kärra

---

1. Parties and background

1.1 Parties

This data processing agreement (the “DPA”) applies between the organisation that has accepted the Customer Terms (https://kungora.com/legal/customer-terms) for Kungora (the “Customer”), as controller, and Puraderi AB, organisation number 559435-0257, c/o Primepack, Orrekulla Industrigata 55B, 425 36 Hisings Kärra (the “Supplier”), as processor.

1.2 Background

The Supplier provides the Service under the Customer Terms. When the Supplier processes personal data on the Customer’s behalf, the DPA applies, which meets the requirements of Article 28(3) of the General Data Protection Regulation.

1.3 Precedence

The DPA prevails over the Customer Terms in matters of processing personal data on the Customer’s behalf. Terms defined in the Customer Terms have the same meaning here.

2. Definitions

Terms such as personal data, processing, controller, processor, data subject, personal data breach and supervisory authority have the same meaning as in Regulation (EU) 2016/679 of the European Parliament and of the Council (the “GDPR”). “Data Protection Law” means the GDPR, the Swedish Act (2018:218) with supplementary provisions to the GDPR and other legislation on personal data that applies to the processing. “Sub-processor” means another processor the Supplier engages for processing on the Customer’s behalf.

3. Scope of the processing

3.1 Processing on the Customer’s behalf

The Supplier processes personal data on the Customer’s behalf to the extent described in clause 17 (Annex 1), mainly the Customer’s contacts and contact lists, sends to them, the events of those sends, preview links and personal data in the Customer’s unpublished content until it is published.

3.2 Processing not covered

The DPA does not cover processing for which the Supplier is itself the controller, for example user accounts, followers and subscribers, journalist accounts, visitor statistics, the suppression list of unsubscribed addresses, security logs, the handling of notices and personal data in published content for the archive, search and the Supplier’s company-information service. That processing is described in the Supplier’s Privacy Policy (https://kungora.com/legal/privacy-policy) and Privacy Notice for Contacts and Journalists (https://kungora.com/legal/privacy-contacts-journalists).

3.3 The Customer's responsibility

The Customer is responsible for there being a legal basis for the processing, for the data subjects having been informed and for the data being accurate. The Customer may not provide special categories of personal data, data on criminal offences or personal identity numbers for processing under the DPA.

4. Instructions

4.1 Documented instructions

The Supplier processes personal data only on the Customer's documented instructions. The instructions consist of the DPA, the Customer Terms and the choices and actions the Customer and its users make in the Service, for example importing contacts, sending a send or deleting a contact. Further instructions must be given in writing and be compatible with the Service's features.

4.2 Unlawful instructions

If the Supplier considers that an instruction infringes Data Protection Law, the Supplier shall immediately inform the Customer and may wait before following the instruction.

4.3 Processing required by law

If the Supplier is required to process the personal data under Union or Swedish law, the Supplier shall inform the Customer before the processing begins, unless the law prohibits such information.

4.4 No own purposes

The Supplier may not process the personal data for its own purposes, combine it with other data the Supplier processes or disclose it to anyone other than Sub-processors, except where the law requires it.

5. Confidentiality

The Supplier shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under a statutory obligation of confidentiality, and that they have access to the data only to the extent needed for their work. Every access by the Supplier's staff to the Customer's private workspace is logged with a stated reason.

6. Security

The Supplier shall take the technical and organisational measures required under Article 32 of the GDPR. The measures are described in clause 18 (Annex 2) and in the Supplier's Security Policy (https://kungora.com/legal/security-policy). The Supplier may change the measures provided the level of protection is not reduced.

7. Sub-processors

7.1 General authorisation

The Customer gives the Supplier a general prior authorisation to engage Sub-processors. The Sub-processors engaged when the DPA is entered into are listed in clause 19 (Annex 3).

7.2 List

The Supplier keeps an up-to-date list of Sub-processors on the Sub-processors (https://kungora.com/legal/subprocessors) page, with name, purpose, categories of data, locations of processing and the safeguard for transfers. The list is also available in machine-readable form at https://kungora.com/legal/subprocessors.json and as a news feed at https://kungora.com/legal/subprocessors.rss.

7.3 Advance notice

The Supplier shall notify the Customer at least 30 days before a new Sub-processor is engaged or an existing one is replaced, by email to the account owner and in the list.

7.4 Objection

The Customer may object to a new Sub-processor on reasonable grounds relating to the protection of personal data, no later than when the period in clause 7.3 ends. The parties shall then try to find a solution. If no solution is found, the Customer may terminate the agreement at no cost with effect before the new Sub-processor starts processing the Customer's personal data.

7.5 Urgent replacement

If a Sub-processor must be replaced sooner for security reasons or to maintain the Service, the Supplier shall notify the Customer as soon as possible. The Customer then has the same right to object as under clause 7.4.

7.6 Terms for Sub-processors

The Supplier shall enter into written agreements with Sub-processors imposing obligations equivalent to those under the DPA. The Supplier is liable to the Customer for the processing of Sub-processors as for its own.

8. Transfers to third countries

The Supplier processes and stores the personal data within the EU and EEA, except where a Sub-processor in the list processes it outside the EU and EEA. A Sub-processor may process personal data in, or access it from, a country outside the EU and EEA only with a valid safeguard under Chapter V of the GDPR, for example an adequacy decision, such as the EU-U.S. Data Privacy Framework for a certified recipient, or the European Commission's standard contractual clauses (Implementing Decision (EU) 2021/914) together with an assessment of the transfer's impact and any supplementary measures needed. The list states for each Sub-processor where it processes the data and the safeguard.

9. Data subjects' rights

9.1 Tools in the Service

The Customer can itself find, export, rectify and delete contacts and their history in the Service, and thereby answer most requests from data subjects.

9.2 Requests received by the Supplier

If the Supplier receives a request from a data subject concerning data the Supplier processes on the Customer's behalf, the Supplier shall without undue delay, and no later than within five working days, forward the request to the Customer and not answer it on the merits itself, unless the Customer has

instructed the Supplier to do so.

9.3 Unsubscribes and erasure across customers

A data subject who unsubscribes from all sends through the Service or requests erasure from the Supplier is blocked from sends from all customers. If the data subject requests erasure or access, the Supplier also notifies the customers who have the data subject on their contact lists, so they can handle the request in their own systems.

9.4 Other assistance

The Supplier shall otherwise assist the Customer with appropriate technical and organisational measures so that the Customer can fulfil its obligations under Chapter III of the GDPR.

10. Personal data breaches

10.1 Notification

The Supplier shall notify the Customer of a personal data breach affecting the Customer's personal data without undue delay and no later than 48 hours after becoming aware of it. The notification is sent by email to the account owner and administrators.

10.2 Content

The notification shall, to the extent the information is available, describe the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences and the measures taken or proposed. Information not available at the first notification is provided as soon as it becomes known.

10.3 Assistance

The Supplier shall assist the Customer with the information needed for the Customer's notification to the supervisory authority and communication to the data subjects, and record the breach in its register of breaches.

11. Impact assessments and prior consultation

Taking into account the nature of the processing and the information available to the Supplier, the Supplier shall assist the Customer with data protection impact assessments and prior consultation with the supervisory authority.

12. Deletion and return

12.1 During the agreement

The Customer can export and delete personal data the Supplier processes on its behalf at any time.

12.2 When the agreement ends

The Customer can export the personal data during the agreement and also after the closure has been carried out under clause 18.4 of the Customer Terms (https://kungora.com/legal/customer-terms#c-18-4), until it is deleted. The Supplier deletes the personal data no later than 30 days after the account has been closed. Copies in backups are overwritten within a further 30 days, that is no later than 60 days after the closure.

12.3 Exceptions

The Supplier may keep personal data longer only where Union or Swedish law requires it, and then only for that purpose.

12.4 Confirmation

At the Customer's request, the Supplier shall confirm in writing that the deletion has taken place.

13. Information and audits

13.1 Information

The Supplier shall make available to the Customer the information needed to demonstrate compliance with Article 28 of the GDPR, including the Security Policy, the list of Sub-processors and available attestations and certifications of Sub-processors.

13.2 Audits

If the information under clause 13.1 is not sufficient, the Customer may have an audit carried out of the Supplier's processing on its behalf, itself or through an independent auditor bound by confidentiality. Audits may take place at most once in any twelve-month period, after at least 30 days' written notice, during office hours and without disrupting the Service or giving access to other customers' data. The Customer bears its own costs and the Supplier's reasonable costs, unless the audit shows that the Supplier has materially breached the DPA.

13.3 Supervisory authorities

The limitations in clause 13.2 do not apply to audits requested by a supervisory authority.

14. Liability

Between the parties, the limitations of liability in clause 15 of the Customer Terms also apply to the DPA. They do not apply to loss the Supplier has caused by intentionally or grossly negligently processing personal data in breach of the DPA. Liability to data subjects under Article 82 of the GDPR is not affected. Each party bears any administrative fines imposed on it.

15. Term

The DPA applies as long as the Supplier processes personal data on the Customer's behalf.

16. Governing law and disputes

Swedish law governs the DPA. Disputes are settled under clause 22 of the Customer Terms.

17. Annex 1: Description of the processing

Area	Description

Purposes	Providing the Service to the Customer: storing and managing the Customer's contacts and contact lists, importing and exporting contacts, sending the Customer's sends, recording delivery, bounces, complaints, unsubscribes, opens and clicks, showing contacts' activity, handling preview links under embargo and storing unpublished content until publication.
Categories of data subjects	The Customer's contacts, for example journalists, newsrooms, analysts, investors, customers and partners; recipients of the Customer's direct sends and test sends; recipients of preview links; people appearing in the Customer's unpublished content.
Categories of personal data	Email address, name, title, organisation or outlet, phone number, language, links, lists and tags, the source and legal basis the Customer has recorded, which user confirmed the import, send history and events of the sends, shortened IP address and browser identification when preview links are opened, and images, quotes and other data about people in unpublished content.
Special categories of data	None. The Customer may not provide such data.
Nature of the processing	Collection by import or entry, storage, structuring, searching, use for sends, transmission to the recipients' email providers, export and erasure.
Duration	During the agreement and thereafter under clause 12.
Retention in the Service	Contacts and lists: until the Customer deletes them or the account is closed. Records of individual recipients of sends: 13 months. Email events per recipient: 13 months, then aggregated. Imported files and export files: 7 days. Preview links and their view log: 12 months.
Locations of processing	Germany (hosting and storage); the Netherlands (encrypted backups); email delivery through the email provider that is configured: Sweden (Amazon Simple Email Service, AWS region eu-north-1) or Ireland (Resend, region eu-west-1), Resend keeping the messages and their delivery events in the United States for 30 days.

18. Annex 2: Technical and organisational security measures

1. **Separation**: the Customer's private workspace is stored in a separate database schema with row-level access control per organisation. It never leaves the primary database and is never part of statistics, exports to third parties or the Supplier's company-information service.
2. **Permissions**: database roles with least privilege; the public web servers have no access to private data; the Supplier's staff have no direct access to contacts and receive only aggregated data through dedicated functions that log every access.

3. **Encryption**: TLS 1.2 or later for all traffic; encrypted disks for the database; encrypted backups; secrets encrypted at rest.
4. **Sign-in**: passwords of at least 12 characters checked against known breached passwords; two-factor authentication and passkeys; the organisation's owner can require two-factor authentication for everyone; staff sign-in requires a passkey and happens only over an encrypted private network.
5. **Logging**: an audit log that cannot be changed, sealed every night with a chain of hashes and kept for 12 months; a log of staff access with a stated reason; shortened IP addresses in access logs.
6. **Backups**: continuous archiving of the database's transaction log and regular full copies, encrypted and stored in another location within the EU for 30 days; documented restore tests.
7. **Files**: uploaded files are scanned for malware; unpublished files are stored privately at random addresses and shown only through short-lived signed links.
8. **Development**: code review, automated tests of database permissions, dependency updates, scanning for leaked secrets and security scanning.
9. **Incidents**: a documented incident response procedure and a register of incidents.
10. **Staff**: confidentiality undertakings, training and permissions that are removed when no longer needed.

19. Annex 3: Sub-processors when the DPA is entered into

Sub-processor	Purpose	Location	Transfer safeguard
Hetzner Online GmbH, Germany	Server hosting and storage	Germany	No transfer
Backblaze, Inc., United States	Storage of encrypted backups	Netherlands	EU-U.S. Data Privacy Framework
Amazon Web Services EMEA SARL, Luxembourg	Email delivery (Amazon Simple Email Service) when SES is the configured email provider	Sweden (eu-north-1)	European Commission standard contractual clauses 2021 and a transfer impact assessment
Resend, Inc., United States	Email delivery when Resend is the configured email provider	Ireland (sending, eu-west-1); United States (messages and delivery events, 30 days)	EU-U.S. Data Privacy Framework

After that, the list under clause 7.2 applies.

20. Signatures

The DPA applies once the Customer has accepted it in the Service. If the Customer wants a signed copy, this document can be downloaded as a PDF, signed by the Customer and sent to dpo@kungora.com. The Supplier signs and returns it.

	Customer	Supplier
Organisation		Puraderi AB
Organisation number		559435-0257

Place and date		
Signature		
Name in print and title		

Signatures

The customer (controller)

Signature _____

Name in block letters _____

Title _____

Place and date _____

Puraderi AB (processor)

Signature _____

Name in block letters _____

Title _____

Place and date _____

SHA-256 of the text: f88dd91dc9c7cf9c8feb08ea57c1e72985cf4b641d04fd6afd877c2d8bd88327