Data Processing Agreement (DPA)

Last updated: 28 February 2026

Processor: DNScale OÜ, operating Postscale

Registry code: 16776331

Registered address: Harju maakond, Tallinn, Lasnamäe linnaosa, Sepapaja tn 6, 15551, Estonia

Contact: info@dnscale.eu

Need a signed copy?

Some customers require a countersigned DPA for their compliance records. The Customer may request a signed copy by contacting Postscale at info@dnscale.eu and providing the Customer's legal entity name, registered address, account email, legal contact email, and authorised signatory details.

This Data Processing Agreement ("DPA") forms part of the agreement between DNScale OÜ, operating Postscale ("Postscale", "Processor", "we", "us", or "our"), and the customer using the Postscale services ("Customer", "Controller", "you", or "your"). This DPA applies when Postscale processes Customer Personal Data on behalf of the Customer in connection with the Services.

1. Definitions

1.1. **Agreement** means the Postscale Terms of Service, any applicable order form, service agreement, statement of work, online terms, product documentation, and any other agreement governing the Customer's use of the Services.

1.2. **Applicable Data Protection Law** means the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), applicable Estonian data protection laws, applicable EU Member State data protection laws, the ePrivacy Directive and national laws implementing it where relevant to electronic communications, and any other privacy or data protection law applicable to the processing of Customer Personal Data under this DPA.

1.3. **Customer Personal Data** means any personal data processed by Postscale on behalf of the Customer as Processor or Subprocessor in connection with the Services.

1.4. **Data Subject Request** means a request from a data subject to exercise rights under Applicable Data Protection Law, including rights of access, rectification, erasure, restriction, portability, objection, or withdrawal of consent.

1.5. **Personal Data Breach** means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.

1.6. **Services** means Postscale's email infrastructure services and related products, APIs, dashboards, tools, documentation, and support made available under the Agreement, including transactional email sending via REST API or SMTP relay, inbound email receiving and webhook processing, masked email functionality, email delivery tracking, domain authentication, DKIM signing, SPF and DMARC support, suppression management, templates, webhooks, logs, and related email infrastructure functionality.

1.7. **Subprocessor** means a third party engaged by Postscale to process Customer Personal Data on behalf of the Customer for the purpose of providing the Services.

1.8. The terms "controller", "processor", "subprocessor", "personal data", "processing", "data subject", "supervisory authority", and "third country" have the meanings given to them in the GDPR.

2. Scope and Application

2.1. This DPA applies only to Postscale's processing of Customer Personal Data as Processor or, where the Customer acts as a processor for a third-party controller, as Subprocessor.

2.2. The Customer determines the purposes and means of processing Customer Personal Data. Postscale processes Customer Personal Data only on documented instructions from the Customer, including instructions provided through the Agreement, API requests, SMTP submissions, dashboard settings, templates, domain configuration, webhook configuration, support requests, and other use of the Services.

2.3. The subject matter, duration, nature, purpose, types of personal data, and categories of data subjects are described in Annex 1.

2.4. Postscale may process certain data as an independent controller, including account registration data, business contact information, billing and tax records, security logs, fraud and abuse prevention information, and communications with the Customer. Such processing is governed by Postscale's Privacy Policy and is outside the scope of this DPA, except to the extent the same data is processed by Postscale on behalf of the Customer as part of the Services.

2.5. Postscale may create and use aggregated, anonymised, or de-identified information for service analytics, security, reliability, abuse prevention, and product improvement, provided that such information does not identify the Customer, any data subject, or any natural person.

3. Customer Obligations

3.1. The Customer shall comply with Applicable Data Protection Law in connection with its use of the Services and its processing of Customer Personal Data.

3.2. The Customer shall ensure that it has all necessary rights, permissions, notices, consents, lawful bases, and authorisations to provide Customer Personal Data to Postscale and to instruct Postscale to process Customer Personal Data as described in this DPA and the Agreement.

3.3. The Customer is responsible for the accuracy, quality, legality, and content of Customer Personal Data, including email content, sender details, recipient details, templates, merge fields, attachments, webhook payloads, domain configurations, and any identifiers or metadata submitted to the Services.

3.4. The Customer shall not use the Services to send unlawful, unsolicited, abusive, deceptive, fraudulent, or non-compliant communications. The Customer is responsible for complying with applicable rules relating to electronic communications, marketing, transactional messages, consent, sender identity, unsubscribe mechanisms, and anti-spam requirements.

3.5. The Customer shall not intentionally submit special categories of personal data, personal data relating to criminal convictions or offences, financial account credentials, government identification numbers, health data, or other highly sensitive personal data through the Services unless the Customer has a valid lawful basis, has implemented appropriate safeguards, and Postscale has expressly agreed to such

processing in writing or the processing is clearly supported by the relevant Service.

3.6. Where the Customer acts as a processor on behalf of a third-party controller, the Customer represents and warrants that its instructions to Postscale are authorised by the relevant controller and that the Customer's agreement with that controller permits the appointment of Postscale as a subprocessor.

3.7. The Customer is responsible for responding to Data Subject Requests and for communicating with supervisory authorities, except to the extent Postscale is required to assist under this DPA.

4. Postscale Obligations as Processor

4.1. Postscale shall process Customer Personal Data only on documented instructions from the Customer unless required to do otherwise by Union or Member State law applicable to Postscale. If such law requires Postscale to process Customer Personal Data other than on the Customer's instructions, Postscale shall inform the Customer before processing unless that law prohibits such information on important grounds of public interest.

4.2. Postscale shall promptly inform the Customer if, in Postscale's opinion, an instruction infringes Applicable Data Protection Law.

4.3. Postscale shall ensure that persons authorised to process Customer Personal Data are bound by confidentiality obligations or are subject to an appropriate statutory obligation of confidentiality.

4.4. Postscale shall implement and maintain appropriate technical and organisational measures designed to protect Customer Personal Data, as described in Annex 2.

4.5. Postscale shall assist the Customer, taking into account the nature of the processing and information available to Postscale, with the Customer's obligations under Applicable Data Protection Law relating to Data Subject Requests, security of processing, Personal Data Breaches, data protection impact assessments, and prior consultations with supervisory authorities.

4.6. Postscale shall make available to the Customer information reasonably necessary to demonstrate compliance with this DPA, subject to Section 13.

4.7. Postscale shall delete or return Customer Personal Data after the end of the provision of Services in accordance with Section 12.

5. Details of Processing

5.1. The details of processing are set out in Annex 1.

5.2. The Customer acknowledges that the Services are used to transmit emails and related data to recipients, recipient mail servers, mailbox providers, and other destinations selected by the Customer, the recipient, or the recipient's domain. Such third-party mail systems are not Subprocessors of Postscale merely because they receive, route, filter, scan, store, or display emails sent at the Customer's instruction.

5.3. The Customer is responsible for determining whether the content, recipients, and routing of emails submitted to the Services comply with Applicable Data Protection Law and other applicable legal requirements.

6. Security Measures

6.1. Postscale shall implement and maintain appropriate technical and organisational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access.

6.2. The measures shall be designed to provide a level of security appropriate to the risk, taking into account the state of the art, implementation costs, nature, scope, context, and purposes of processing, and the risks to the rights and freedoms of natural persons.

6.3. Postscale's current technical and organisational measures are described in Annex 2. Postscale may update those measures from time to time, provided the updated measures do not materially reduce the overall level of protection for Customer Personal Data.

6.4. The Customer is responsible for securing its accounts, API keys, SMTP credentials, webhook endpoints, domain DNS settings, devices, systems, and integrations used with the Services.

7. Subprocessors

7.1. The Customer grants Postscale general written authorisation to engage Subprocessors to process Customer Personal Data for the purpose of providing, securing, supporting, and maintaining the Services.

7.2. Postscale shall maintain a current list of Subprocessors at https://postscale.io/subprocessors or another URL notified to the Customer. The list shall identify the Subprocessor, the processing purpose, the location of processing, and the relevant transfer safeguard where applicable.

7.3. Postscale shall enter into a written agreement with each Subprocessor that imposes data protection obligations no less protective than those in this DPA, to the extent applicable to the Subprocessor's processing of Customer Personal Data.

7.4. Postscale shall remain responsible to the Customer for the performance of its Subprocessors' obligations relating to Customer Personal Data.

7.5. Postscale shall notify the Customer of any intended addition or replacement of a Subprocessor at least 30 calendar days before the new or replacement Subprocessor begins processing Customer Personal Data, unless earlier use is required for security, continuity, legal compliance, or urgent operational reasons. Notice may be provided by email, dashboard notice, publication on the Subprocessor list, or another reasonable method.

7.6. The Customer may object to a new or replacement Subprocessor on reasonable data protection grounds within 15 calendar days after notice. If the Customer objects, the parties shall work in good faith to resolve the objection. If no commercially reasonable resolution is available, the Customer may terminate the affected Services by written notice.

7.7. Third-party mail servers, mailbox providers, DNS providers, recipient domain operators, filtering systems, and recipients to whom Customer emails are sent or routed at the Customer's instruction are not Subprocessors of Postscale. They are recipients or independent third parties designated by the Customer, the recipient, or the recipient's domain.

7.8. Service providers used by Postscale for Postscale's own business operations, such as payment processing, corporate communications, internal analytics, or legal and accounting services, are not Subprocessors under this DPA unless they process Customer Personal Data on behalf of the Customer in connection with the Services.

8. International Data Transfers

8.1. Postscale's primary infrastructure for the Services is hosted in the European Union or European Economic Area. Postscale shall not intentionally transfer Customer Personal Data outside the European Economic Area except as described in this DPA, the Subprocessor list, the Agreement, or as instructed by the Customer.

8.2. If Postscale transfers Customer Personal Data to a third country or international organisation, Postscale shall ensure that the transfer is subject to an adequacy decision, Standard Contractual Clauses approved by the European Commission, binding corporate rules, an approved code of conduct, an approved certification mechanism, a valid derogation, or another transfer mechanism permitted by Applicable Data Protection Law.

8.3. Where required by Applicable Data Protection Law, Postscale shall conduct and document a transfer impact assessment and implement supplementary measures appropriate to the transfer.

8.4. Email delivery to recipients, recipient mail servers, mailbox providers, forwarding addresses, or other destinations outside the European Economic Area may occur where the Customer instructs Postscale to send, route, or process email to or through such destinations. The Customer is responsible for determining whether such recipient-directed transfer or disclosure is lawful.

8.5. If Postscale receives a legally binding request from a public authority for disclosure of Customer Personal Data, Postscale shall, to the extent legally permitted, notify the Customer and provide reasonable information to allow the Customer to seek protective measures.

9. Data Subject Requests

9.1. If Postscale receives a Data Subject Request relating to Customer Personal Data, Postscale shall, where legally permitted, forward the request to the Customer or direct the data subject to contact the Customer.

9.2. Postscale shall not respond substantively to a Data Subject Request relating to Customer Personal Data unless instructed by the Customer or required by applicable law.

9.3. Taking into account the nature of the processing and information available to Postscale, Postscale shall provide reasonable assistance to the Customer in fulfilling the Customer's obligation to respond to Data Subject Requests.

9.4. If the Customer requires assistance beyond the self-service functionality of the Services, the Customer shall provide sufficient information for Postscale to identify the relevant Customer Personal Data and the action requested.

10. Personal Data Breaches

10.1. Postscale shall notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data.

10.2. Where reasonably practicable, Postscale shall provide notice within 48 hours after becoming aware of the Personal Data Breach.

10.3. The notice shall include, to the extent known and available to Postscale at the time of notice:

- the nature of the Personal Data Breach;
- the categories and approximate number of affected data subjects;
- the categories and approximate number of affected personal data records;
- the likely consequences of the Personal Data Breach;
- measures taken or proposed to address, contain, and mitigate the Personal Data Breach; and
- a contact point for further information.

10.4. Postscale may provide information in phases where complete information is not available at the same time.

10.5. Postscale shall take reasonable steps to contain, investigate, remediate, and mitigate the effects of a Personal Data Breach affecting Customer Personal Data.

10.6. Notification of a Personal Data Breach shall not be construed as an admission of fault or liability by Postscale.

11. Assistance with Security, DPIAs, and Prior Consultation

11.1. Taking into account the nature of the processing and information available to Postscale, Postscale shall provide reasonable assistance to the Customer with the Customer's obligations under Articles 32 to 36 of the GDPR, including security of processing, Personal Data Breach notification, data protection impact assessments, and prior consultation with supervisory authorities.

11.2. Postscale may satisfy this obligation by providing relevant documentation, technical information, security summaries, answers to reasonable questionnaires, or other information reasonably available to Postscale.

12. Return and Deletion of Customer Personal Data

12.1. During the term of the Services, the Customer may delete, export, or retrieve certain Customer Personal Data through available Service functionality.

12.2. Upon termination or expiry of the Services, Postscale shall, at the Customer's choice, delete or return Customer Personal Data, unless Union or Member State law requires storage of the personal data.

12.3. The Customer shall provide written deletion or return instructions within 14 calendar days after termination or expiry of the Services. If the Customer does not provide instructions within that period, Postscale may delete Customer Personal Data in accordance with its standard retention practices.

12.4. Where the Customer requests return of Customer Personal Data, Postscale shall provide the data in a reasonable format supported by the Services or otherwise agreed by the parties.

12.5. Postscale may retain Customer Personal Data in backups, logs, archives, suppression lists, or security records for a limited period where deletion is technically impracticable, necessary for security, necessary to prevent abuse, or required by law. Such retained data shall remain protected under this DPA and shall be deleted or overwritten in accordance with Postscale's normal retention cycle.

12.6. Postscale may retain account records, billing records, tax records, legal records, security records, fraud prevention records, and abuse prevention records to the extent required or permitted by applicable law.

13. Audits and Compliance Information

13.1. Postscale shall make available to the Customer information reasonably necessary to demonstrate compliance with this DPA.

13.2. Upon reasonable request, Postscale may provide security documentation, responses to reasonable security questionnaires, summaries of relevant policies, technical and organisational measures, or third-party audit reports or certifications where available.

13.3. If the information provided under Section 13.2 is insufficient to demonstrate compliance with this DPA, the Customer may request an audit. The audit shall be limited to Postscale's processing of Customer Personal Data and shall be subject to reasonable confidentiality, safety, operational, and security requirements.

13.4. Audits must be:

- requested with at least 45 calendar days' prior written notice;
- limited to once in any 12-month period, unless required by a supervisory authority or following a confirmed Personal Data Breach affecting Customer Personal Data;
- conducted during normal business hours;
- conducted by the Customer or an independent auditor that is not a competitor of Postscale;
- limited to systems, records, and personnel relevant to Customer Personal Data;
- conducted in a manner that does not compromise the confidentiality, availability, or security of Postscale systems or other customers' data; and
- subject to confidentiality obligations acceptable to Postscale.

13.5. The Customer shall bear the costs of any audit unless the audit reveals a material breach of this DPA by Postscale.

13.6. Postscale may refuse or limit audit access where the requested access would compromise security, confidentiality, trade secrets, legal privilege, or the rights of other customers or third parties. In such case, Postscale shall use reasonable efforts to provide alternative information sufficient to demonstrate compliance.

14. Confidentiality of Compliance Materials

14.1. Any security documentation, audit reports, certifications, policies, questionnaires, technical information, or other compliance materials provided by Postscale under this DPA are confidential information of Postscale.

14.2. The Customer shall use such materials only to verify Postscale's compliance with this DPA and shall not disclose them to any third party except to the Customer's legal, compliance, security, or professional advisers who are bound by confidentiality obligations, or where disclosure is required by law or a supervisory authority.

15. Government and Legal Requests

15.1. Postscale shall not voluntarily disclose Customer Personal Data to a public authority unless legally required or instructed by the Customer.

15.2. If Postscale receives a subpoena, court order, law enforcement request, regulatory request, or other legal demand relating to Customer Personal Data, Postscale shall, to the extent legally permitted, notify the Customer before disclosure and provide reasonable cooperation to allow the Customer to seek protective measures.

15.3. Nothing in this DPA prevents Postscale from disclosing information where required by applicable law, to protect the security or integrity of the Services, to prevent abuse, or to protect the rights, safety, and property of Postscale, its customers, data subjects, or third parties.

16. Liability

16.1. Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement, unless prohibited by applicable law.

16.2. Nothing in this DPA limits or excludes liability that cannot be limited or excluded under Applicable Data Protection Law or other applicable law.

16.3. Where Applicable Data Protection Law imposes direct liability on either party, such liability shall be determined in accordance with Applicable Data Protection Law.

17. Order of Precedence

17.1. If there is a conflict between this DPA and the Agreement regarding the processing of Customer Personal Data, this DPA shall prevail to the extent of the conflict.

17.2. If Standard Contractual Clauses or another mandatory transfer mechanism applies to a transfer of Customer Personal Data and conflicts with this DPA, the Standard Contractual Clauses or mandatory transfer mechanism shall prevail to the extent of the conflict.

17.3. The Agreement remains in full force except as modified by this DPA.

18. Term and Termination

18.1. This DPA becomes effective when the Customer accepts the Agreement, uses the Services, signs this DPA, or otherwise agrees to this DPA electronically or in writing.

18.2. This DPA remains in effect for as long as Postscale processes Customer Personal Data on behalf of the Customer.

18.3. Obligations that by their nature should survive termination shall survive for as long as Postscale retains Customer Personal Data.

19. Amendments

19.1. Postscale may update this DPA from time to time.

19.2. If Postscale makes material changes that reduce the protection of Customer Personal Data, Postscale shall provide at least 30 calendar days' notice by email, dashboard notice, publication through the Services, or another reasonable method.

19.3. If the Customer objects to a material change on reasonable data protection grounds, the Customer may terminate the affected Services before the change takes effect. Continued use of the Services after the

effective date of an updated DPA constitutes acceptance of the updated DPA.

19.4. Postscale may make changes that are required by law, required by a supervisory authority, necessary for security, or do not materially reduce the protection of Customer Personal Data with shorter or no prior notice where appropriate.

20. Governing Law and Jurisdiction

20.1. This DPA is governed by the laws of the Republic of Estonia, unless Applicable Data Protection Law requires otherwise.

20.2. Any dispute arising from or relating to this DPA shall be resolved in accordance with the dispute resolution and jurisdiction provisions of the Agreement.

21. Contact

Privacy and data protection questions may be sent to:

DNScale OÜ
Harju maakond, Tallinn, Lasnamäe linnaosa
Sepapaja tn 6, 15551, Estonia
Email: info@dnscale.eu

Annex 1 - Details of Processing

A. Subject Matter

Postscale processes Customer Personal Data to provide, secure, maintain, support, and improve the Services used by the Customer.

B. Duration

Postscale processes Customer Personal Data for the duration of the Customer's use of the Services and thereafter only as necessary for deletion, return, backup retention, legal compliance, security, fraud prevention, abuse prevention, dispute resolution, or as otherwise permitted by this DPA or the Agreement.

C. Nature of Processing

The processing may include collection, receipt, transmission, routing, sending, delivery, forwarding, storage, hosting, retrieval, access, display, filtering, scanning, logging, indexing, organisation, structuring, alteration, analysis, suppression, deletion, and other processing necessary to provide the Services.

D. Purposes of Processing

The purposes of processing include:

- sending transactional emails and other Customer-initiated emails;
- receiving and processing inbound emails;
- routing, forwarding, and delivering emails;
- operating REST API and SMTP relay functionality;
- managing masked email aliases and privacy-protective forwarding functionality;
- authenticating sending domains and supporting SPF, DKIM, and DMARC configuration;
- signing email using DKIM and supporting deliverability controls;
- storing templates and processing template variables or merge fields;
- generating, sending, and retrying webhooks;
- tracking delivery events such as queued, sent, delivered, bounced, complained, opened, clicked, unsubscribed, or suppressed events where enabled;
- maintaining suppression lists and abuse prevention controls;
- maintaining service logs, diagnostics, rate limits, and performance metrics;
- detecting, preventing, and responding to spam, abuse, fraud, security threats, and unauthorised use;
- providing customer support and troubleshooting;
- complying with applicable legal obligations; and
- performing other processing instructed by the Customer through the Services.

E. Types of Personal Data

Customer Personal Data may include:

- sender and recipient names;
- sender and recipient email addresses;
- sender domain names and reply-to addresses;
- email subject lines;

- email body content, including HTML and plain text content;
- email attachments, where supported or submitted;
- email headers and routing metadata;
- message IDs, customer IDs, user IDs, account IDs, order IDs, loyalty IDs, invoice IDs, and other identifiers included by the Customer;
- template variables, merge fields, and dynamic content;
- inbound email content and metadata;
- masked email alias data and forwarding data;
- webhook payloads, endpoint URLs, event data, timestamps, and retry data;
- IP addresses and network information;
- device, browser, and email client information where generated by tracking or logs;
- delivery, bounce, complaint, open, click, unsubscribe, suppression, and reputation data;
- domain configuration data, DNS records, authentication status, SPF, DKIM, and DMARC-related data;
- API usage logs, authentication logs, performance logs, and diagnostic logs;
- support communications that include Customer Personal Data; and
- any other personal data submitted by the Customer or processed at the Customer's instruction through the Services.

F. Categories of Data Subjects

Data subjects may include:

- the Customer's end users;
- email recipients;
- email senders;
- customers, prospects, subscribers, members, loyalty programme participants, account holders, and business contacts of the Customer;
- employees, contractors, representatives, administrators, and users of the Customer;
- individuals who communicate with the Customer by email;
- individuals whose personal data is included in email content, templates, attachments, webhooks, logs, or other Service data; and
- any other individual whose personal data is submitted to or processed through the Services by or on behalf of the Customer.

G. Special Categories of Data

The Services are not designed to require the processing of special categories of personal data. The Customer is responsible for determining whether Customer Personal Data includes special categories of personal data or other highly sensitive data and for ensuring that such processing is lawful and subject to appropriate safeguards.

Annex 2 - Technical and Organisational Measures

Postscale shall maintain appropriate technical and organisational measures for the protection of Customer Personal Data. The measures below apply to the extent relevant to the Services and the nature of processing.

1. Access Control

- access to production systems restricted to authorised personnel;
- role-based access controls and least-privilege principles;
- authentication controls for administrative access;
- secure management of API keys, credentials, tokens, and secrets;
- periodic review of privileged access where appropriate;
- procedures for revoking access when no longer required.

2. Confidentiality and Personnel Controls

- confidentiality obligations for personnel with access to Customer Personal Data;
- internal policies restricting access to Customer Personal Data;
- access to Customer Personal Data only where needed to provide, secure, maintain, or support the Services;
- security and privacy awareness appropriate to personnel roles.

3. Encryption and Transport Security

- encryption of data in transit using TLS or comparable secure transport mechanisms;
- encryption at rest where supported by the relevant storage system;
- DKIM signing and domain authentication functionality for email integrity and deliverability;
- secure handling of secrets and credentials.

4. System and Network Security

- network security controls designed to protect production systems;
- secure configuration and hardening of relevant systems;
- vulnerability management and patching practices;
- monitoring and logging of relevant production systems;
- controls designed to detect and prevent spam, abuse, fraud, and unauthorised use.

5. Availability, Resilience, and Recovery

- backup and recovery procedures appropriate to the Services;
- controls designed to support ongoing confidentiality, integrity, availability, and resilience of processing systems;
- incident response procedures;
- capacity, continuity, and operational monitoring controls appropriate to the Services.

6. Data Minimisation and Retention

- retention of Customer Personal Data only as needed for the Services or as required or permitted by law;
- deletion or overwriting of data in accordance with applicable retention periods and Service functionality;
- retention controls for logs, backups, suppression records, security records, and abuse prevention records.

7. Customer Separation

- logical separation of customer accounts and data;
- controls designed to prevent unauthorised access between customer environments;
- separation of production and non-production access where appropriate.

8. Secure Development and Change Management

- controlled deployment and change management practices;
- review of material changes affecting production systems;
- testing or validation of security-impacting changes where appropriate;
- documentation of relevant operational procedures.

9. Subprocessor Management

- due diligence for Subprocessors that process Customer Personal Data;
- written data processing terms with Subprocessors;
- review of Subprocessor security and data protection measures where appropriate;
- maintenance of a Subprocessor list and notification process.

10. Incident Management

- procedures for identifying, escalating, investigating, and remediating security incidents;
- notification procedures for Personal Data Breaches affecting Customer Personal Data;
- documentation of incidents and remedial actions;
- post-incident review where appropriate.

Signature Block for Countersigned Copies

This DPA may be accepted electronically. If a countersigned copy is required, the parties may sign below.

Customer / Controller

Legal entity: _____

Registered address: _____

Account email: _____

Representative name: _____

Title: _____

Signature: _____

Date: _____

DNScale OÜ / Postscale / Processor

Legal entity: DNScale OÜ
Registry code: 16776331
Registered address: Harju maakond, Tallinn, Lasnamäe linnaosa, Sepapaja tn 6, 15551, Estonia

Representative name: _____

Title: _____

Signature: _____

Date: _____