DNScale Data Processing Agreement

Last updated: 28 February 2026
Provider: DNScale OÜ
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 Data Processing Agreement for their compliance records. The Customer may request a signed copy by contacting DNScale 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 ("DNScale", "Processor", "we", "us", or "our") and the customer using DNScale services ("Customer", "Controller", "you", or "your"). This DPA applies when DNScale processes Customer Personal Data on behalf of the Customer in connection with the Services.

This DPA is designed for DNScale's managed authoritative DNS platform and related DNS infrastructure services. It does not replace any product-specific data processing agreement for a separately branded service operated by DNScale OÜ, unless the applicable agreement expressly incorporates this DPA for that service.

1 Definitions

1.1 Agreement means the DNScale Terms of Service, any applicable order form, service agreement, 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, and any other privacy or data protection law applicable to the processing of Customer Personal Data under this DPA.

1.3 Customer DNS Data means DNS zones, DNS records, nameserver settings, DNSSEC configuration, query logs, analytics data, API requests, audit logs, and related configuration or operational data submitted to or generated by the Services on behalf of the Customer.

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

1.5 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.

1.6 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.

1.7 Services means DNScale's managed authoritative DNS hosting services and related products, APIs, dashboards, tools, documentation, and support made available under the Agreement, including DNS zone management, DNS record management, authoritative DNS hosting, EU-only and global anycast DNS networks, secondary DNS, DNSSEC, query analytics, DNS observability, DDoS-resilient DNS resolution, API access, Terraform or DNSControl integrations, multi-user account management, role-based access, and audit logging.

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

1.9 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 DNScale's processing of Customer Personal Data as Processor or, where the Customer acts as processor for a third-party controller, as Subprocessor.

2.2 The Customer determines the purposes and means of processing Customer Personal Data. DNScale processes Customer Personal Data only on documented instructions from the Customer, including instructions provided through the Agreement, dashboard settings, API requests, DNS zone configuration, record changes, region selection, DNSSEC configuration, analytics settings, 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 DNScale may process certain data as an independent controller, including account registration data, business contact information, billing and tax records, payment metadata, fraud and abuse prevention information, service communications, and corporate support records. Such processing is governed by DNScale's Privacy Policy and is outside the scope of this DPA, except to the extent the same data is processed by DNScale on behalf of the Customer as part of the Services.

2.5 DNScale may create and use aggregated, anonymised, or de-identified information for service analytics, reliability, security, abuse prevention, capacity planning, 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 DNScale and to instruct DNScale 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 DNS Data, including domain names, hostnames, record names, record values, TXT records, SPF, DKIM, DMARC, CAA, TLSA, HTTPS, SVCB, SRV, MX, NS, and other DNS data submitted to or managed through the Services.

3.4 The Customer acknowledges that DNS is a public, distributed naming system. DNS records published through the Services may be queried by resolvers, networks, devices, and users worldwide, may be cached by third parties according to TTLs and resolver behaviour, and may be logged by third-party recursive resolvers, ISPs, security providers, or other independent parties outside DNScale's control.

3.5 The Customer shall not intentionally publish personal data in DNS records unless the Customer has a valid lawful basis, has provided appropriate notices to data subjects where required, and has assessed the public and distributed nature of DNS publication.

3.6 The Customer shall not use the Services for illegal activities, malware, phishing, spam, abusive infrastructure, unlawful tracking, unauthorised access, DNS abuse, or activity that violates the Agreement or applicable law.

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

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

4 DNScale Obligations as Processor

4.1 DNScale 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 DNScale. If such law requires DNScale to process Customer Personal Data other than on the Customer's instructions, DNScale shall inform the Customer before processing unless that law prohibits such information on important grounds of public interest.

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

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

4.5 DNScale shall assist the Customer, taking into account the nature of the processing and information available to DNScale, 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 DNScale shall make available to the Customer information reasonably necessary to demonstrate compliance with this DPA, subject to Section 13.

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

5 DNS-Specific Processing

5.1 DNScale provides authoritative DNS hosting and related DNS management functionality. The Services may publish Customer DNS Data to authoritative nameservers and respond to DNS queries from recursive resolvers, networks, and end users.

5.2 DNS records, DNS responses, DNSSEC records, nameserver delegations, and related protocol data are processed to provide name resolution. Such data may be public by design and may be independently cached, logged, analysed, or redistributed by third parties that are not appointed by DNScale.

5.3 Recursive DNS resolvers, registries, registrars, TLD operators, root servers, ISPs, browser vendors, security products, monitoring services, and end users that query or use DNS data are not Subprocessors of DNScale merely because they receive or process DNS responses or DNS-related data.

5.4 If the Customer configures the Services to use the global anycast network, EU + Global regions, secondary DNS, API-based synchronisation, Terraform, DNSControl, or third-party integrations, DNScale may process Customer DNS Data as needed to provide that configuration.

5.5 If the Customer selects an EU-only DNS hosting option for a zone, DNScale shall process authoritative DNS hosting for that zone using its EU infrastructure, subject to DNS responses sent to querying resolvers or users, legally required disclosures, Customer instructions, and any subprocessors or support systems disclosed under this DPA.

6 Security Measures

6.1 DNScale 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 DNScale's current technical and organisational measures are described in Annex 2. DNScale 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, authentication factors, DNS zones, registrar access, nameserver delegations, Terraform or DNSControl configuration, CI/CD systems, devices, and integrations used with the Services.

7 Subprocessors

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

7.2 DNScale shall maintain a current list of Subprocessors at https://dnscale.eu/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 DNScale 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 DNScale shall remain responsible to the Customer for the performance of its Subprocessors' obligations relating to Customer Personal Data.

7.5 DNScale 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 DNS resolvers, registries, registrars, root or TLD operators, ISPs, networks, browser vendors, endpoint security providers, and users that query, cache, validate, or rely on DNS responses are not Subprocessors of DNScale.

7.8 Service providers used by DNScale for DNScale's own business operations, such as payment processing, corporate communications, internal analytics, legal services, 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 DNScale operates EU and global anycast DNS infrastructure. The region or network selected by the Customer for a DNS zone may affect where Customer DNS Data is processed for authoritative DNS resolution.

8.2 For zones configured to use EU-only DNS hosting, DNScale shall use EU infrastructure for authoritative DNS hosting of that zone, subject to the public and distributed nature of DNS responses, Customer instructions, support activities, legal requirements, and disclosed Subprocessors.

8.3 For zones configured to use global DNS hosting, EU + Global hosting, secondary DNS, or integrations with non-EEA services, DNScale may process Customer Personal Data in locations outside the European Economic Area as needed to provide the Services.

8.4 If DNScale transfers Customer Personal Data to a third country or international organisation as Processor, DNScale 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.

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

8.6 DNS responses sent to querying resolvers, networks, devices, or end users outside the European Economic Area are part of the Customer-directed DNS publication and resolution process and are not

treated as Subprocessor transfers by DNScale.

8.7 If DNScale receives a legally binding request from a public authority for disclosure of Customer Personal Data, DNScale 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 DNScale receives a Data Subject Request relating to Customer Personal Data, DNScale shall, where legally permitted, forward the request to the Customer or direct the data subject to contact the Customer.

9.2 DNScale 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 DNScale, DNScale 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 DNScale to identify the relevant Customer Personal Data and the action requested.

10 Personal Data Breaches

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

10.2 Where reasonably practicable, DNScale 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 DNScale 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 DNScale may provide information in phases where complete information is not available at the same time.

10.5 DNScale 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 DNScale.

11 Assistance with Security, DPIAs, and Prior Consultation

11.1 Taking into account the nature of the processing and information available to DNScale, DNScale 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 DNScale may satisfy this obligation by providing relevant documentation, technical information, security summaries, answers to reasonable questionnaires, or other information reasonably available to DNScale.

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, including DNS zones, DNS records, DNSSEC settings, API keys, user access controls, and account activity records where supported by the Services.

12.2 Upon termination or expiry of the Services, DNScale 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, DNScale may delete Customer Personal Data in accordance with its standard retention practices.

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

12.5 DNScale may retain Customer Personal Data in backups, logs, analytics systems, security records, or abuse prevention 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 DNScale's normal retention cycle.

12.6 DNScale 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.

12.7 DNScale cannot delete DNS data that has already been cached, stored, logged, indexed, or redistributed by third-party resolvers, networks, registries, registrars, monitoring systems, search engines, or other independent third parties outside DNScale's control.

13 Audits and Compliance Information

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

13.2 Upon reasonable request, DNScale 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 DNScale'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 DNScale;
- 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 DNScale systems or other customers' data; and
- subject to confidentiality obligations acceptable to DNScale.

13.5 The Customer shall bear its own costs and DNScale's reasonable, documented costs incurred in connection with any audit, unless the audit reveals a material breach of this DPA by DNScale.

13.6 DNScale may refuse or limit audit access where the requested access would compromise security, confidentiality, trade secrets, legal privilege, DNS infrastructure integrity, or the rights of other customers or third parties. In such case, DNScale 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, network architecture information, or other compliance materials provided by DNScale under this DPA are confidential information of DNScale.

14.2 The Customer shall use such materials only to verify DNScale'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 DNScale shall not voluntarily disclose Customer Personal Data to a public authority unless legally required or instructed by the Customer.

15.2 If DNScale receives a subpoena, court order, law enforcement request, regulatory request, or other legal demand relating to Customer Personal Data, DNScale 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 DNScale from disclosing information where required by applicable law, to protect the security or integrity of the Services, to prevent DNS abuse, to respond to threats, or to protect the rights, safety, and property of DNScale, 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 DNScale 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 DNScale retains Customer Personal Data.

19 Amendments

19.1 DNScale may update this DPA from time to time.

19.2 If DNScale makes material changes that reduce the protection of Customer Personal Data, DNScale 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 DNScale 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

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

B Duration

DNScale 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, DNS abuse prevention, dispute resolution, or as otherwise permitted by this DPA or the Agreement.

C Nature of Processing

The processing may include collection, receipt, hosting, publication, transmission, routing, replication, synchronisation, storage, retrieval, access, display, logging, indexing, organisation, structuring, alteration, analysis, monitoring, validation, signing, deletion, and other processing necessary to provide the Services.

D Purposes of Processing

The purposes of processing include:

- creating, importing, hosting, and managing DNS zones;
- creating, updating, deleting, validating, and serving DNS records;
- providing authoritative DNS resolution over EU-only, global, or EU + Global anycast networks selected by the Customer;
- providing secondary DNS, multi-provider DNS, API-based synchronisation, Terraform, DNSControl, and related automation workflows;
- providing DNSSEC signing, key management, DS/DNSKEY support, validation, and related DNS security functionality;
- processing query analytics, response codes, resolver information, latency metrics, traffic volumes, usage statistics, and DNS observability data;
- providing account access controls, multi-user permissions, role-based access, API keys, and audit logs;
- detecting, preventing, and responding to DNS abuse, DDoS attacks, fraud, security threats, unauthorised use, and operational incidents;
- maintaining service logs, diagnostics, rate limits, performance metrics, backups, and availability controls;
- 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:

- domain names, zone names, hostnames, subdomains, record names, and record values that may identify or relate to natural persons;
- DNS records, including A, AAAA, CNAME, MX, TXT, SPF, DKIM, DMARC, SRV, CAA, TLSA, HTTPS, SVCB, NS, SOA, and other supported record types;
- email addresses, names, identifiers, URLs, IP addresses, public keys, verification tokens, or other personal data included by the Customer in DNS records;
- DNSSEC configuration, DNSSEC public key material, DS/DNSKEY records, signing status, and related metadata;
- nameserver delegation data, registrar-related configuration, and zone import or migration data;
- DNS query logs and analytics data, including queried domain name, query type, timestamp, response code, response latency, point of presence, resolver IP address or resolver subnet, and network information;
- API requests, authentication events, API key metadata, user identifiers, account activity, and audit logs;
- usage data, billing usage metrics, query volumes, rate limits, and performance data;
- 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 administrators, employees, contractors, representatives, and account users;
- individuals whose names, email addresses, IP addresses, domains, hostnames, URLs, identifiers, or other personal data are included in Customer DNS Data;
- operators of systems, domains, services, or endpoints identified in DNS records;
- users, visitors, customers, subscribers, members, or business contacts of the Customer whose personal data is included in DNS records or related configuration;
- individuals associated with recursive resolvers, network operators, or endpoints represented in query logs or analytics where such information is personal 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

DNScale 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;
- multi-user account controls and role-based customer permissions where supported by the Services;
- two-factor authentication and WebAuthn or hardware security key support where supported by the Services;
- secure management of API keys, credentials, tokens, and secrets;
- periodic review of privileged access where appropriate; and
- 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; and
- 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 for dashboards, APIs, and administrative interfaces;
- encryption at rest where supported by the relevant storage system;
- DNSSEC functionality to support cryptographic validation of DNS data where enabled or supported; and
- secure handling of secrets, credentials, API keys, and authentication material.

4 DNS Infrastructure Security

- anycast architecture designed for resilient authoritative DNS resolution;

- DDoS mitigation and traffic absorption controls appropriate to authoritative DNS infrastructure;
- separation of EU and global DNS networks where applicable to the selected region;
- network monitoring, health checks, and operational alerting;
- capacity planning and redundancy controls for DNS availability; and
- controls designed to detect and respond to DNS abuse, unauthorised use, and operational anomalies.

5 System and Application 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; and
- controlled access to APIs, dashboards, administrative systems, and support tools.

6 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; and
- redundancy across authoritative DNS infrastructure consistent with the selected Service configuration.

7 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, analytics, backups, security records, and abuse prevention records; and
- aggregation or anonymisation of analytics data where appropriate and technically feasible.

8 Customer Separation

- logical separation of customer accounts, DNS zones, DNS records, API keys, and access permissions;
- controls designed to prevent unauthorised access between customer environments; and
- separation of production and non-production access where appropriate.

9 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; and
- documentation of relevant operational procedures.

10 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; and
- maintenance of a Subprocessor list and notification process.

11 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; and
- 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 / 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: _____