

LEGAL

Data Processing Addendum

The GDPR Article 28 terms under which StatusDNS processes personal data on behalf of business customers.

Last updated: 16 September 2026 · v1.0 · [Download PDF](#)

This Data Processing Addendum ("**DPA**") supplements the Terms of Service (the "Agreement") between the customer identified on the StatusDNS account ("**Customer**", "Controller") and **InsideMaps Bulgaria EOOD**, EIK 205550879, Graf Ignatiev St 44-A, fl. 4, 1000 Sofia, Bulgaria ("**StatusDNS**", "Processor"). It applies whenever StatusDNS processes personal data on behalf of a Customer that uses the Service for business purposes. It is accepted automatically by such use; Customers who need a countersigned copy for their records may request one at support@statusdns.com. Terms such as "personal data", "processing", "controller", "processor" and "supervisory authority" have the meanings given in Regulation (EU) 2016/679 ("**GDPR**") and, for UK Customers, the UK GDPR.

1. Parties and Roles

For Customer Data that the Customer submits to the Service (domains, host names, IP addresses, DNS records, DMARC reports, notification recipients, names and emails of the Customer's team members), the Customer is the controller and StatusDNS is the processor. For the Customer's own account data (the account holder's name, email, billing status), StatusDNS is an independent controller as described in the Privacy Policy. Each party will comply with its obligations under applicable data-protection law.

2. Details of Processing

Subject matter	Provision of DNS, email and domain diagnostics, monitoring, alerting and API services.
Duration	The term of the Agreement plus the deletion period in Section 10.
Nature and purpose	Storing the Customer's configuration; querying public DNS, mail, web, certificate, blacklist and registry sources for the domains the Customer submits; storing results and history; sending alerts and reports to recipients configured by the Customer; providing the API.

Types of personal data	Names and email addresses of the Customer's users and alert recipients; webhook/Slack URLs; IP addresses and domain names that may relate to identifiable individuals (for example a sole trader's domain, a personal mail server, or sending IP addresses contained in uploaded DMARC reports); WHOIS/RDAP contact data returned by registries where not redacted. Most Customer Data is infrastructure data that does not identify a person.
Categories of data subjects	The Customer's employees, contractors and clients; operators of the domains and mail systems the Customer checks; senders whose IP addresses appear in DMARC reports.
Special categories	None. The Customer must not submit special-category data.

3. Processor Obligations

StatusDNS shall: (a) process personal data only on the Customer's documented instructions, which are the Agreement, this DPA and the Customer's use of the Service's features, unless required otherwise by EU or Member State law (in which case StatusDNS informs the Customer unless prohibited); (b) ensure that persons authorised to process the data are bound by confidentiality; (c) implement the security measures in Section 6; (d) engage sub-processors only in accordance with Section 5; (e) assist the Customer, taking into account the nature of the processing, in responding to data-subject requests (Section 8) and in meeting its obligations regarding security, breach notification and data-protection impact assessments (Sections 7 and 9); (f) delete or return personal data at the end of the services (Section 10); (g) make available the information necessary to demonstrate compliance and allow audits (Section 7); and (h) inform the Customer immediately if, in its opinion, an instruction infringes data-protection law.

4. Customer Obligations

The Customer warrants that it has a lawful basis for the processing it instructs, that it has a legitimate interest in every domain, host and IP address it submits, that it has obtained any notices or consents required from its own users and alert recipients, and that its instructions comply with applicable law. The Customer is responsible for the accuracy and lawfulness of Customer Data and for configuring the Service (retention plan, notification recipients, team members) appropriately.

5. Sub-processors

The Customer gives general authorisation for StatusDNS to engage the sub-processors listed at statusdns.com/subprocessors (currently OVH SAS for hosting, Resend Inc. for transactional

email, Cloudflare Inc. for DNS and reverse proxy; Paddle.com Market Ltd acts as an independent controller for payments and is not a sub-processor of Customer Data). StatusDNS will give at least **30 days' notice** of any intended addition or replacement by updating that page and emailing account holders. The Customer may object on reasonable data-protection grounds within that period; if the objection cannot be resolved, the Customer may terminate the affected services and receive a pro-rata refund of prepaid fees. StatusDNS imposes data-protection obligations on each sub-processor that are no less protective than this DPA and remains liable for their performance.

6. Security Measures (Annex II summary)

- **Encryption in transit:** TLS for all web, API and email traffic; HTTPS-only site.
- **Access control:** Argon2id password hashing; hashed API keys shown once; secure, HttpOnly, SameSite session cookies; CSRF protection; single administrative role with audit logging of administrative actions; least-privilege service accounts.
- **Application security:** parameterised database access, strict input validation and shell-argument escaping, rate limiting on authentication and all lookups, security headers.
- **Availability and recovery:** daily database dumps retained for 14 days; monitoring of the scheduler and email queue; hosting on OVHcloud infrastructure.
- **Data minimisation and retention:** automatic deletion of history per plan retention, 90-day lookup and server logs, deletion within 30 days of account closure.
- **Organisational:** access limited to personnel who need it for operating the Service; confidentiality obligations; change review before deployment.

Details are published on the [Security page](#) and updated when measures change. StatusDNS may update measures provided the overall level of protection is not reduced.

7. Audits and Information

On written request, not more than once per year (unless required by a supervisory authority or following a personal-data breach), StatusDNS will provide the Customer with the information reasonably necessary to demonstrate compliance with Article 28 GDPR, including responses to reasonable security questionnaires. Where this is insufficient, the Customer may conduct, at its own cost and on 30 days' notice, an audit of the relevant processing during business hours, by itself or by an independent auditor bound by confidentiality, without unreasonable disruption to StatusDNS's operations.

8. Data Subject Requests

StatusDNS will forward to the Customer without undue delay any request it receives from a data subject relating to Customer Data, and will not respond to it except on the Customer's instruction or where required by law. Taking into account the nature of the processing, StatusDNS assists the Customer through the self-service features of the Service (editing and deleting domains, recipients, team members and reports) and, where needed, by manual assistance at support@statusdns.com.

9. Personal Data Breach

StatusDNS will notify the Customer without undue delay, and in any event within **72 hours** of becoming aware of a personal-data breach affecting Customer Data, by email to the account holder. The notification will describe, as far as known, the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point. StatusDNS will cooperate with the Customer's investigation and any notifications to authorities or data subjects.

10. Deletion and Return

The Customer can export Results through the web interface and API and delete domains, reports and recipients at any time. Within 30 days after termination of the Agreement or closure of the account, StatusDNS deletes all Customer Data from production systems; backups are overwritten within a further 14 days. StatusDNS may retain data required by law (for example billing records) for the period required, protected by this DPA.

11. International Transfers

Personal data is stored on OVHcloud infrastructure in Virginia, United States, and processed by the sub-processors in Section 5. Transfers from the EEA/UK are made under the EU Standard Contractual Clauses (Commission Decision (EU) 2021/914, Module 2 controller-to-processor and Module 3 processor-to-processor as applicable), which are incorporated into this DPA by reference with the Customer as data exporter and StatusDNS as data importer, and, for UK Customers, the UK International Data Transfer Addendum; or, where the recipient is certified, under the EU-US Data Privacy Framework. Annex I of the SCCs is completed by Section 2 of this DPA and Annex II by Section 6. Copies are provided on request.

12. Liability

Each party's liability under this DPA is subject to the limitations and exclusions in Section 13 of the Terms of Service, except to the extent that mandatory law (including Article 82 GDPR)

provides otherwise.

13. Term, Precedence and Governing Law

This DPA takes effect on the Customer's first business use of the Service and continues until all Customer Data has been deleted. In case of conflict with the Agreement, this DPA prevails for personal-data matters; in case of conflict with the SCCs, the SCCs prevail. This DPA is governed by the laws of the Republic of Bulgaria and the courts of Sofia, Bulgaria, without prejudice to the governing-law clause of the SCCs. Contact: support@statusdns.com.