

TRUST & SECURITY

How we protect your data and the platform.

A factual description of the controls in place today. Updated whenever they change.

Data we process

StatusDNS works with public data: DNS records, WHOIS/RDAP registration details, TLS certificates, HTTP responses and DNS-blacklist answers. You never give us credentials to your DNS provider, registrar or mail system. Account data is limited to what is needed to run your subscription and notify you (name, email, company, plan, the domains you monitor and the results of their checks).

Hosting and infrastructure

- The platform runs on OVHcloud infrastructure in Virginia, United States operated by InsideMaps Bulgaria EOOD.
- All traffic is encrypted in transit with TLS (Let's Encrypt certificates, HTTP/2, HSTS-ready).
- Lookups are performed by our own recursive resolver (Unbound) and our own DNS, SMTP, HTTP and RDAP clients — we do not route your queries through third-party DNS providers.
- The database is dumped daily and retained for 14 days on the same OVHcloud server.

Application security

- Passwords are hashed with Argon2id. API keys are stored as SHA-256 hashes and shown only once at creation.
- Every state-changing request is protected by a CSRF token; sessions use secure, HttpOnly, SameSite cookies.
- Rate limiting on authentication, registration, password reset, the contact form and all lookups.
- All database access uses bound parameters; user input never reaches a shell without strict validation and escaping.
- Security headers: X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy.
- Administrative actions are recorded in an audit log.

Email

Transactional email and alerts are sent through Resend, Inc. (sending region: EU) from statusdns.com, which publishes SPF, DKIM and DMARC. We never send marketing email to alert recipients.

Payments

Paid plans are sold through Paddle.com Market Ltd as Merchant of Record. Card details are entered on Paddle's checkout and never touch our servers.

Responsible disclosure

If you believe you have found a vulnerability, email support@statusdns.com. We acknowledge within two business days and keep you informed until the issue is resolved. Please do not run automated scanners against production and do not access data that is not yours.

Compliance

We process personal data as described in the Privacy Policy and comply with the GDPR. A data processing agreement is available on request for business customers. We do not currently hold a third-party certification such as ISO 27001 or SOC 2.