Stratline
NETWORKS

LEGAL DOCUMENT
SLN-LGL-003

DATA PROTECTION NOTICE

Privacy Policy

Information on the processing of personal data pursuant to Articles 13 and 14 of the General Data Protection Regulation (GDPR).

Issued by	Stratline Networks
Document	SLN-LGL-003
Version	1.0
Effective date	6 November 2026
Applies to	Website visitors, customers, prospects and network contacts
Website	stratline.net

Stratline Networks
stratline.net
contact@stratline.net

CONTENTS

1. Controller and Contact
2. Definitions and Legal Framework
3. Visiting our Website
4. Contacting Us by Email
5. Requests for Quotes and Customer Relationships
6. Network Operation, Traffic Data and Security
7. Abuse Reports
8. Peering and Interconnection
9. Publication in Registry Databases
10. Recipients of Personal Data
11. Transfers to Third Countries
12. Retention and Deletion
13. Your Rights
14. Obligation to Provide Data
15. Data Security
16. Changes to this Privacy Policy

ABOUT THIS DOCUMENT

We take the protection of personal data seriously. This Privacy Policy explains which personal data we process when you visit our website, contact us, become a customer, peer with our network or report abuse, why we process it, how long we keep it and what rights you have.

Our website does not use analytics, advertising trackers or marketing cookies. Our services are offered to businesses; nevertheless, we process personal data of individual contact persons at those businesses.

Where we process personal data on behalf of our customers (for example data stored on customer servers), the customer is the controller of that data and we process it only on the customer's behalf to provide the services, as described in the *Terms of Service*.

1. Controller and Contact

1.1 The controller within the meaning of Art. 4(7) GDPR is Stratline Networks, which can be reached by email at contact@stratline.net.

1.2 For all questions regarding data protection and to exercise your rights, please contact us at contact@stratline.net with the subject line "Data protection".

1.3 Stratline is not currently required to designate a data protection officer under Art. 37 GDPR and § 38 BDSG. Should this requirement arise, the contact details of the data protection officer will be published in this policy.

2. Definitions and Legal Framework

2.1 This policy uses the terms defined in Art. 4 GDPR, in particular **personal data**, **processing**, **controller**, **processor** and **recipient**.

2.2 We process personal data in accordance with the GDPR, the German Federal Data Protection Act (BDSG), the Telecommunications Digital Services Data Protection Act (TDDDG) and, where we act as a provider of telecommunications services, the data protection provisions of the German Telecommunications Act (TKG).

3. Visiting our Website

3.1 Our website stratline.net is a static website. It is delivered via the content delivery network of Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA (**Cloudflare**), which acts as our processor.

3.2 When you access our website, the following data is processed automatically for technical reasons and to protect the website against attacks:

a. IP address of the requesting device;

b. date and time of the request;

c. requested URL and HTTP status code;

d. amount of data transferred;

e. referrer URL, where transmitted by your browser; and

f. browser type, operating system and user-agent string.

3.3 The legal basis is Art. 6(1)(f) GDPR. Our legitimate interest lies in the secure, stable and efficient delivery of the website and in the detection and defence of attacks, including denial-of-service attacks. Access to information stored on your device is limited to what is strictly necessary to provide the service you have expressly requested (§ 25(2) no. 2 TDDDG).

3.4 Cloudflare may set technically necessary cookies to distinguish legitimate visitors from automated attacks. These cookies do not identify you personally and are deleted at the end of the session or after a short period. No cookies are set for analytics or marketing purposes.

3.5 Log data processed by Cloudflare is retained for no longer than is necessary for the purposes described, generally not exceeding thirty (30) days, unless retention is required to investigate a specific security incident.

3.6 Our website loads all fonts and resources from our own domain. No connections are made to Google Fonts or other third-party content providers when you visit our website.

4. Contacting Us by Email

4.1 When you contact us by email, we process the information you provide, including your name, email address, company and the content of your message, in order to handle your enquiry and any follow-up questions.

4.2 The legal basis is Art. 6(1)(b) GDPR where your enquiry relates to the conclusion or performance of a contract, and otherwise Art. 6(1)(f) GDPR, our legitimate interest being the effective handling of enquiries addressed to us.

4.3 We delete enquiries once they have been fully handled, unless statutory retention obligations apply (for example where the correspondence constitutes a commercial letter under § 257 HGB) or the correspondence is required for the establishment, exercise or defence of legal claims.

5. Requests for Quotes and Customer Relationships

5.1 For the preparation of offers and the conclusion and performance of contracts with our business customers, we process personal data of the customer's contact persons, in particular:

a. master data: name, position, business email address, business telephone number and company affiliation;

b. account data: control panel user name, hashed passwords, two-factor authentication data and login history;

c. contract data: ordered services, contract terms, service configuration and correspondence;

d. billing data: billing address, VAT identification number, bank details, payment history and invoices; and

e. support data: tickets, fault reports and communications with our support and network operations teams.

5.2 The legal basis is Art. 6(1)(b) GDPR insofar as the contact person is the contractual partner, and otherwise Art. 6(1)(f) GDPR, our legitimate interest being communication with the representatives of our business customers for the performance of the contract.

5.3 To prevent fraud and the misuse of our network, we may verify the identity and business registration of new customers by consulting public registers (such as the commercial register and the EU VIES VAT database) and sanctions lists. The legal basis is Art. 6(1)(c) GDPR in conjunction with applicable sanctions regulations, and Art. 6(1)(f) GDPR, our legitimate interest being the prevention of fraud and abuse.

5.4 We do not use automated decision-making, including profiling, within the meaning of Art. 22 GDPR.

6. Network Operation, Traffic Data and Security

6.1 As an operator of an IP network, we process traffic data to the extent necessary for the provision, billing and security of our services. Traffic data includes IP addresses, port numbers, protocol information, timestamps, data volumes and interface counters. We do not inspect the content of communications.

6.2 We collect sampled flow data (for example sFlow or IPFIX) and interface statistics to manage capacity, bill usage-based services (including 95th percentile bandwidth billing), detect and mitigate denial-of-service attacks and investigate faults.

6.3 The legal basis for this processing is Art. 6(1)(b) GDPR for billing, Art. 6(1)(c) GDPR in conjunction with the provisions of the TKG and TDDDG governing traffic data, and Art. 6(1)(f) GDPR, our legitimate interest being the security and stability of our network and the networks of third parties.

6.4 Sampled flow data is retained for a maximum of seven (7) days. Aggregated usage data required for billing is retained until the end of the billing dispute period, and in any case for no longer than six (6) months after the invoice is issued, unless longer retention is required by statutory retention obligations or for the defence of legal claims.

6.5 Logs of our network devices and servers containing IP addresses are retained for a maximum of fourteen (14) days, unless they are required to investigate a specific security incident.

7. Abuse Reports

7.1 When you send us an abuse report to abuse@stratline.net, we process the information contained in your report, including your name, email address, and any evidence provided such as log extracts and IP addresses, to investigate and remedy the reported abuse.

7.2 To enable our customer to remedy the abuse, we forward the report to the responsible customer. We remove your personal contact details before forwarding unless you have asked us to include them or they are required for the customer to respond, for example in the case of copyright notices where the identity of the rights holder is relevant.

7.3 The legal basis is Art. 6(1)(c) GDPR in conjunction with Articles 16 and 17 of the Digital Services Act, and Art. 6(1)(f) GDPR, our legitimate interest being the protection of our network, third parties and the wider Internet against misuse.

7.4 Abuse reports and related correspondence are retained for twenty-four (24) months to identify repeated violations, and thereafter deleted unless required for legal proceedings.

8. Peering and Interconnection

8.1 When network operators request peering with us at peering@stratline.net, we process the business contact details of their network engineers and NOC staff, together with technical information such as AS numbers, IP addresses and routing policies, to establish and operate interconnections.

8.2 Much of this information is publicly available in PeeringDB and the RIPE Database. The legal basis is Art. 6(1)(f) GDPR, our legitimate interest being the operation of interconnections in accordance with industry practice.

8.3 We retain peering contact data for as long as the interconnection exists and for twelve (12) months thereafter.

9. Publication in Registry Databases

9.1 As a member or end user of the RIPE NCC, we are required to register assignments of IP address space and autonomous system numbers in the RIPE Database. This includes the organisation name, address and abuse contact details of the holder of the resources.

9.2 Where customers are assigned IP address space, we register assignments as required by RIPE NCC policy. We use role objects and business contact details wherever possible and avoid publishing personal data of natural persons. The legal basis is Art. 6(1)(c) and (f) GDPR.

9.3 The RIPE Database is operated by the RIPE NCC, Stationsplein 11, 1012 AB Amsterdam, the Netherlands, as an independent controller. Information on its processing is available in the RIPE NCC's privacy statement.

10. Recipients of Personal Data

10.1 Within Stratline, only those employees who need access to personal data for the purposes described have access to it.

10.2 We use carefully selected service providers who process personal data on our behalf under data processing agreements pursuant to Art. 28 GDPR, in particular:

CATEGORY	PURPOSE	LOCATION
Content delivery and DNS	Website delivery, DDoS protection	EU / USA (EU-US Data Privacy Framework)
Email and collaboration	Business communication	EU
Accounting and invoicing	Billing and bookkeeping	Germany
Payment service providers	Processing of payments	EU
Data centre operators	Physical hosting of infrastructure	Locations of our points of presence

A current list of providers is available on request.

10.3 We transfer personal data to other recipients only where this is necessary for the performance of a contract, where we are legally obliged to do so (for example to tax authorities, auditors or law enforcement authorities on the basis of a valid legal order), or where we have a legitimate interest in doing so, such as the engagement of legal advisers for the enforcement of claims.

11. Transfers to Third Countries

11.1 Some of our service providers are located outside the European Economic Area or may access data from outside the EEA. We transfer personal data to third countries only where the requirements of Articles 44 et seq. GDPR are met.

11.2 For transfers to the United States, we rely on the adequacy decision of the European Commission of 10 July 2023 for companies certified under the EU-US Data Privacy Framework. Where a recipient is not certified, or for transfers to other third countries without an adequacy decision, we conclude the European Commission's Standard Contractual Clauses (Implementing Decision (EU) 2021/914) and implement supplementary measures where necessary.

11.3 Network traffic originating from or destined to our customers is, by the nature of the Internet, routed through third-country networks where the communicating parties are located there. This routing is not a transfer by Stratline within the meaning of Chapter V GDPR.

12. Retention and Deletion

12.1 We process and store personal data only for as long as necessary for the purposes for which it was collected, or as required by statutory retention obligations.

12.2 The following retention periods apply in particular:

DATA	RETENTION PERIOD	BASIS
Website access logs	Up to 30 days	Art. 6(1)(f) GDPR
Network device and server logs	Up to 14 days	Art. 6(1)(f) GDPR
Sampled flow data	7 days	Art. 6(1)(c), (f) GDPR
Commercial letters and contract documents	6 years	§ 257 HGB
Invoices and accounting records	8 years (from 2025 onwards)	§ 147 AO, § 257 HGB
Abuse reports	24 months	Art. 6(1)(f) GDPR
Enquiries without contract	Deleted after handling, max. 12 months	Art. 6(1)(f) GDPR

12.3 Retention periods begin at the end of the calendar year in which the relevant event occurred. Once the retention period has expired, data is deleted or anonymised in accordance with our deletion policy.

13. Your Rights

13.1 Subject to the statutory requirements, you have the following rights in relation to your personal data:

a. the right of access under Art. 15 GDPR;
b. the right to rectification under Art. 16 GDPR;
c. the right to erasure under Art. 17 GDPR;
d. the right to restriction of processing under Art. 18 GDPR;
e. the right to data portability under Art. 20 GDPR; and
f. the right to withdraw consent at any time with effect for the future under Art. 7(3) GDPR, where processing is based on consent.

13.2 **Right to object (Art. 21 GDPR).** Where we process your personal data on the basis of Art. 6(1)(f) GDPR, you have the right to object at any time, on grounds relating to your particular situation, to the processing of your personal data. We will then no longer process the data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing serves the establishment, exercise or defence of legal claims. Where we process personal data for direct marketing purposes, you may object to such processing at any time without stating reasons.

13.3 To exercise your rights, contact us using the details in section 1. We will respond within one month of receipt of your request; this period may be extended by two further months where necessary, taking into account the complexity and number of requests. We may ask you to verify your identity.

13.4 **Right to lodge a complaint.** You have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, place of work or the place of the alleged infringement (Art. 77 GDPR). Within Germany, a list of the competent supervisory authorities is published by the Federal Commissioner for Data Protection and Freedom of Information (BfDI).

14. Obligation to Provide Data

14.1 The provision of personal data is neither legally nor contractually required for visiting our website. For the conclusion and performance of a contract, the provision of the contact, billing and identification data marked as mandatory is required; without this data, we are unable to conclude a contract with you.

15. Data Security

15.1 We implement appropriate technical and organisational measures in accordance with Art. 32 GDPR to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. These measures include encryption in transit (TLS), access controls based on the principle of least privilege, multi-factor authentication for administrative access, logging of administrative actions and regular security updates.

15.2 Our measures are reviewed regularly and adapted to technological developments. A summary of our technical and organisational measures is available on request at contact@stratline.net.

16. Changes to this Privacy Policy

16.1 We may update this Privacy Policy to reflect changes to our services, our processing or the legal framework. The current version is always available on our website. Where changes affect processing based on your consent, we will request your consent again where required.

Stratline Networks · stratline.net · contact@stratline.net
End of document · SLN-LGL-003 v1.0