# Data Processing Agreement (DPA)

Version: 2.1
(Updated: 20/08/2026)

This Data Processing Agreement ("DPA") forms part of the Terms of Service between:

ProRedLine ("Processor")
Chamber of Commerce (KvK): 95892494
VAT: NL005177436B09
Registered business address: Repelstraat 10, 3295CM ‘s-Gravendeel, Netherlands
Correspondence address: P.O. Box 5449, 3299ZG Maasdam, Netherlands
Email: info@proredline.com
Website: https://proredline.com

and its Customers ("Controllers"), together referred to as the Parties.

This DPA applies where ProRedLine processes personal data on behalf of the Controller within the scope of the European Union General Data Protection Regulation (GDPR).

## 1. Subject Matter and Duration

This DPA governs the processing of personal data by ProRedLine as Processor on behalf of the Customer as Controller, solely to the extent such processing is necessary to provide web hosting, email hosting, DNS hosting, managed hosting infrastructure, backup and disaster recovery services, and other related technical infrastructure services.

This DPA does not apply to personal data ProRedLine processes as Data Controller for its own business purposes, including webshop orders, billing administration, payment processing, fraud prevention, customer support administration, legal compliance, security management, and other internal business operations as further described in the Privacy Policy.

The duration of this DPA corresponds to the duration of the contractual relationship between the Parties, plus any limited retention periods required for backups, security logs, disaster recovery processes, legal obligations, or other applicable retention requirements as described in this DPA, the Privacy Policy, and other applicable ProRedLine policies.

## 2. Instructions

The Processor shall process personal data only on documented instructions from the Controller. If the Processor believes that an instruction infringes GDPR or other applicable law, it shall inform the Controller.

## 3. Confidentiality

The Processor shall ensure that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. These obligations remain in effect after termination.

## 4. Technical and Organisational Measures

The Processor shall implement appropriate TOMs to ensure a level of security appropriate to the risk. Details of the TOMs applied by ProRedLine are set out in Annex II.

## 5. Data Subject Rights

Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as possible, in fulfilling the Controller's obligations to respond to requests for exercising Data Subject rights under GDPR. The Processor shall notify the Controller promptly if it receives a request directly from a Data Subject.

## 6. Personal Data Breach Notification

The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach affecting personal data processed on behalf of the Controller.

The notification shall contain all information reasonably available at the time to enable the Controller to comply with Articles 33 and 34 GDPR. Where all information cannot be provided simultaneously, it may be supplied in phases without undue delay as additional information becomes available.

The Processor shall reasonably cooperate with the Controller in investigating, mitigating and documenting the breach.

# 7. Subprocessors

The Controller authorises the Processor to engage subprocessors as listed in Annex I.

The Processor shall ensure that each authorised subprocessor is subject to data protection obligations that are substantially equivalent to those set out in this DPA.

Where the Processor intends to add or replace a subprocessor in a manner that materially affects the processing of personal data under this DPA, the Processor shall inform the Controller through its website, customer portal or email. The Controller may raise reasonable objections where required under applicable data protection law.

## 7a. International Data Transfers

ProRedLine primarily processes Customer Content within the European Economic Area (EEA).

Certain geographically distributed DNS infrastructure may operate outside the EEA, including in the United Kingdom and the United States. These systems are used for authoritative DNS services and do not store Customer website content, databases, mailboxes or other hosted Customer Content.

Where limited personal data or technical metadata is processed outside the EEA in connection with such infrastructure, ProRedLine shall ensure that the processing and any international transfer takes place in accordance with Chapter V of the GDPR.

Transfers may take place on the basis of an applicable adequacy decision adopted by the European Commission or, where required, appropriate safeguards such as the European Commission's Standard Contractual Clauses (SCCs).

# 8. Audits

Upon reasonable written request, the Processor shall make available information reasonably necessary to demonstrate compliance with this DPA.

Where such information is insufficient to satisfy applicable legal requirements, the Parties may agree upon an appropriate audit or inspection.

Any audit shall:

- take place during normal business hours;
- be limited to once per calendar year unless required by law or a Supervisory Authority;
- not unreasonably interfere with the Processor's operations;
- be subject to appropriate confidentiality obligations; and
- be carried out at the Controller's expense unless otherwise required by law.

## 9. Return and Deletion of Data

Upon termination of the Services, the Processor shall delete or return personal data processed on behalf of the Controller in accordance with the Controller's instructions, unless Union or Member State law requires continued storage.

Where a Subscription ends because a renewal has not been paid by the Due Date, the Service may terminate immediately in accordance with the Terms of Service. No contractual grace period applies.

Customer data associated with the terminated Service may be deleted after termination in accordance with ProRedLine's operational deletion procedures.

Limited copies of personal data may remain temporarily within secured backup rotations, disaster recovery systems, security logs or other technical systems until overwritten or deleted in accordance with the applicable retention schedule.

Any continued retention shall be limited to what is reasonably necessary for backup rotation, security, legal compliance, dispute resolution or other applicable legal obligations.

After deletion from active systems and expiry of applicable backup retention periods, ProRedLine has no obligation to retain or restore Customer data.

## 10. Liability and Governing Law

The liability limitations set out in the Terms of Service apply to this DPA. This DPA is governed by the laws of the Netherlands. Consumers retain their mandatory EU rights, including the right to bring proceedings in their own EU member state. Business Customers must resolve disputes individually in the competent courts of the Netherlands.

## 11. Miscellaneous

If any provision of this DPA is held invalid or unenforceable, the remaining provisions shall remain in full force and effect. In case of conflict between this DPA and the Terms of Service, this DPA prevails with respect to the processing of personal data. This DPA may be updated from time to time, with material changes communicated via ProRedLine's website or email notifications.

## 12. Related Policies

This DPA should be read in conjunction with the following ProRedLine policies:

- Terms of Service: https://proredline.com/legal/terms-of-service/

- Privacy Policy: https://proredline.com/legal/privacy-policy/
- Cookie Policy: https://proredline.com/legal/cookie-policy/
- Refund Policy: https://proredline.com/legal/refund-policy/
- Acceptable Use Policy: https://proredline.com/legal/acceptable-use-policy/
- Contact & Support Policy: https://proredline.com/legal/contact-support-policy/

# Annex I – Authorised Subprocessors

The following subprocessors may be engaged by ProRedLine where necessary for the provision of the Services covered by this DPA:

Infrastructure

- Contabo GmbH (Germany, with infrastructure located in Germany, the United Kingdom and the United States) – hosting infrastructure, servers, storage, networking and related infrastructure services.
  Contabo infrastructure located in the United Kingdom and the United States is used only for geographically distributed authoritative DNS infrastructure. Customer website content, databases and mailboxes are not hosted on these systems.

Domain Registration

- OpenProvider B.V. (Netherlands) – domain registration, registrar services and related registry communications.

Telecommunications

- CheapConnect B.V. (Netherlands) – telephony and VoIP connectivity where applicable to the Services purchased by the Customer.

Payment Processing

- WooPayments / Stripe / Klarna – payment processing for ProRedLine's own commercial transactions. These providers generally act independently as Data Controllers for payment processing activities and are not engaged as subprocessors for Customer Content hosted through the Services.

Communications

- WhatsApp / Meta – only where the Customer voluntarily communicates with ProRedLine through WhatsApp for support purposes. Meta may process communications and related metadata under its own privacy terms.

Marketing Communications

- Brevo – newsletter delivery, contact management and communications relating to ProRedLine's own business operations. Brevo is generally not used as a subprocessor for Customer Content processed under this DPA.

Self-hosted Software

The following software is operated entirely on ProRedLine-controlled infrastructure and does not transfer Customer Content to the software developers as part of its normal operation:

- cPanel & WHM
- SupportCandy
- FreePBX
- Uptime Kuma
- Internal ProRedLine software and plugins

# Annex II – Technical and Organisational Measures (TOMs)

ProRedLine implements appropriate Technical and Organisational Measures ("TOMs") to ensure a level of security appropriate to the risks associated with the processing of personal data, taking into account Article 32 GDPR, the nature of the Services, the state of the art, implementation costs, and the risks to the rights and freedoms of natural persons.

1. Access Control
    a. Role-based access following the principle of least privilege.
    b. Administrative access is limited to authorised personnel only.
    c. Multi-factor authentication (MFA) is enabled where supported.
    d. Strong password requirements are enforced where applicable.
    e. SSH administrative access is protected using public-key authentication and additional security controls.
2. Encryption and Secure Communications
    a. TLS/SSL encryption is used for publicly accessible services where applicable.
    b. Secure protocols are used for remote administration and service management.
    c. Email transmission supports encrypted transport where supported by the receiving party.
    d. Sensitive credentials submitted for technical support are encrypted before storage.
3. Network and Infrastructure Security
    a. Firewalls are implemented to restrict unauthorised network access.
    b. Network services are limited to required ports and protocols.
    c. DNS infrastructure is geographically distributed to improve resilience and availability.
    d. Infrastructure components are monitored for availability and abnormal behaviour.
    e. Security updates are applied on a regular basis.

4. Malware Prevention and System Hardening
    a. Anti-malware software is deployed where appropriate.
    b. Intrusion prevention and brute-force protection mechanisms are implemented.
    c. Operating systems and publicly exposed services are hardened according to internal security standards.
    d. Unnecessary services and software are disabled or removed where practical.
5. Logging and Monitoring
    a. Security-relevant events are logged where appropriate.
    b. Infrastructure availability is continuously monitored.
    c. Monitoring data is used for security, operational continuity and incident response.
    d. Logs are protected against unauthorised access and retained only as long as necessary.
6. Backup and Disaster Recovery
    a. Regular backups are performed in accordance with ProRedLine's backup policy.
    b. Backups are stored securely with restricted administrative access.
    c. Backup integrity and restoration procedures are tested periodically.
    d. Off-site backups may be maintained for disaster recovery purposes.
    e. Backup data is retained only for the periods defined in ProRedLine's backup retention schedule.
7. Incident Response
    a. Personal data breaches are handled through documented incident response procedures.
    b. Customers are notified without undue delay where required under this DPA.
    c. Where applicable, supervisory authorities are notified in accordance with Articles 33 and 34 GDPR.
8. Personnel and Confidentiality
    a. Persons authorised to process personal data are subject to confidentiality obligations.
    b. Administrative access is granted only where necessary for operational duties.
    c. Access rights are reviewed and removed when no longer required.
9. Physical and Infrastructure Security
    a. Infrastructure is hosted in professionally managed data centres operated by trusted infrastructure providers.
    b. Physical access controls are implemented by the infrastructure provider.
    c. Redundancy measures are applied where appropriate to improve service availability.

These measures may be updated from time to time to reflect technological developments, changes to the Services, evolving security threats, or improvements to ProRedLine's security programme, provided that the overall level of protection is not materially reduced.

# Annex III – Processing Details

1. Categories of Data Subjects
   Depending on the Services purchased by the Customer, the following categories of Data Subjects may be processed:
   a. Customer account users.
   b. Employees or authorised representatives of the Customer.
   c. Visitors to the Customer's hosted websites.
   d. End users of applications or services hosted by the Customer.
   e. Email correspondents communicating with Customer-managed mailboxes.
   f. Support contacts acting on behalf of the Customer.
   g. Any other individuals whose personal data the Customer chooses to store or process through the Services.
2. Categories of Personal Data
   Depending on the Customer's use of the Services, the following categories of personal data may be processed:
   a. Identification data (such as names, usernames, company information and contact details).
   b. Contact information (including email addresses, telephone numbers and postal addresses).
   c. Technical data (including IP addresses, browser information, device identifiers, timestamps and access logs).
   d. Authentication-related information processed by the Customer.
   e. Email-related data, including routing information, headers and stored mailbox contents where applicable.
   f. Website and application data stored by the Customer, including databases, uploaded files, user accounts, contact form submissions and other Customer Content.
   g. Security logs, abuse-related logs and system-generated operational logs where necessary for security and service operation.
   h. Any additional categories of personal data intentionally uploaded or processed by the Customer through the Services.
3. Nature and Purpose of Processing
   Processing may include, where applicable:
   a. Provision of web hosting services.
   b. Provision of DNS hosting services.
   c. Provision of email hosting services.
   d. Storage of Customer Content.
   e. Transmission, routing and delivery of electronic communications.
   f. Backup, replication and disaster recovery.
   g. Security monitoring and abuse prevention.

h. Technical maintenance and troubleshooting.
i. System administration necessary to operate the Services.
j. Incident detection, response and recovery.

Processing is performed solely for the purpose of providing, maintaining, securing and supporting the Services requested by the Customer, in accordance with the Customer's documented instructions and the applicable service agreement.

4. Duration of Processing

Personal data is processed for the duration of the applicable Services provided under the agreement between the Parties.

Following termination of the Services, Customer data will be deleted in accordance with this DPA, the applicable Terms of Service, backup retention schedules and any applicable legal retention obligations. Limited retention within secured backups or security logs may continue only for the period reasonably necessary to satisfy backup rotation, disaster recovery, security or legal compliance requirements.