Data Processing Agreement (DPA)

Version: 1.0

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

ProRedLine ("Processor")
Chamber of Commerce (KvK): 95892494
VAT: NL005177436B09
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 on behalf of the Controller for the purpose of providing hosting, domain registration, and related services. The duration of this DPA corresponds to the duration of the contractual relationship between the Parties.

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. The notification shall contain sufficient detail to enable the Controller to comply with GDPR Articles 33 and 34.

7. Subprocessors

The Controller authorises the Processor to engage subprocessors as listed in Annex I. The Processor shall impose on each subprocessor the same data protection obligations as set out in this DPA. The Processor shall notify the Controller of intended changes to subprocessors, giving the Controller the opportunity to object.

8. Audits

The Controller may request information reasonably required to demonstrate compliance with this DPA. The Processor will provide documentation (e.g., security policies, certifications) upon request. On-site inspections are excluded except where required by law or supervisory authority. Any audits shall be limited to once per year and at the Controller's expense.

9. Return and Deletion of Data

Upon termination of the services, the Processor shall delete all personal data within seven (7) days after the end of the grace period, unless Union or Member State law requires longer storage. Backups shall be deleted according to retention policies.

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

Annex I – Subprocessors

The following subprocessors are engaged by ProRedLine:
- Contabo GmbH (Germany, EU) – infrastructure, servers, and object storage
- OpenProvider (Netherlands, EU) – domain registration services
- WooPayments / Stripe / Klarna – payment processing
- Google Analytics (via Site Kit), Jetpack, Google for WooCommerce – analytics
- Wordfence Security / Really Simple Security – security and logging
- SupportCandy – ticketing system
- WP Mail SMTP, Notification – email delivery
- cPanel/WHM (self-hosted) – web hosting
- Pterodactyl (self-hosted) – app/game servers
- Internal ProRedLine plugins – incident/maintenance, renewal, configurator (self-hosted, no external transfers)

Annex II – Technical and Organisational Measures (TOMs)

The following TOMs are implemented by ProRedLine to ensure data protection:

Access Control:
- Role-based access, least privilege
- Two-factor authentication (2FA) for all portals

Encryption:
- TLS/SSL for all websites and services
- STARTTLS for email

- Object storage encryption

Network Security:
- Firewalls (iptables, CSF/LFD)
- Port restrictions and whitelisting
- DDoS protection by Contabo

Malware and Intrusion Prevention:
- ClamAV (daily and weekly scans)
- Fail2ban for login attempts
- SSH via RSA keys with passphrase
- XRDP password protection

Monitoring and Logging:
- Uptime monitoring
- Incident and maintenance logs
- Wordfence logging on multisite

Backups and Retention:
- Weekly backups of servers
- Secure storage of backups
- Data deleted after 7-day grace period

Incident Response:
- Documented breach procedure
- Customers notified without undue delay
- Supervisory authority notified within 72 hours if required