Data Processing Agreement

Version 1.1, 2026-11-05

This Data Processing Agreement ("DPA") is made between Verne Software and the customer named as data exporter in Annex I.A ("Customer").

1. Parties and application

1.1 **Verne Software** means Maksim Zhuk PR Novi Sad, an entrepreneur registered in the Republic of Serbia, doing business as Verne Software, Zheleznichka 20, Novi Sad, Vojvodina 21101, Serbia, VAT number RS113630704 ("Verne").

1.2 **Customer** means the person or entity named as data exporter in Annex I.A.

1.3 This DPA applies to a Customer that subscribes to the Pro plan or a higher plan of the Services when it signs this DPA. It takes effect on the date on which both parties have signed it (the "Effective Date"), and it supplements the Terms of Service published at https://vernesoft.com/terms-of-service (the "Terms") that apply between Verne and Customer.

2. Scope and roles

2.1 This DPA applies to personal data that Verne processes on behalf of Customer in providing the Services ("Customer Personal Data").

2.2 For Customer Personal Data, Customer is the controller and Verne is the processor. Where Customer itself acts as a processor on behalf of a third party, Verne is Customer's sub-processor, and this DPA applies accordingly.

2.3 This DPA does not apply to personal data that Verne processes as a controller: Customer's account, billing and contact details, and analytics on Verne's own websites. That processing is described in Verne's Privacy Policy at https://vernesoft.com/privacy-policy.

2.4 "Services" means Verne's hosted services as described in the Terms: user authentication and identity management (Gate Identity), sign-in with Telegram (Passepartout), webhook delivery (Relay), and scheduled and delayed jobs (Clockwork).

2.5 Terms defined in Regulation (EU) 2016/679 ("GDPR") have the same meaning in this DPA.

3. Instructions

3.1 Verne processes Customer Personal Data only on Customer's documented instructions. The Terms, this DPA, and Customer's configuration of the Services through the dashboard or the API constitute those instructions.

3.2 Verne will inform Customer if, in its opinion, an instruction infringes applicable data protection law.

4. Confidentiality

Verne ensures that every person authorised to process Customer Personal Data is bound by an obligation of confidentiality.

5. Security

5.1 Verne implements the technical and organisational measures described in Annex II.

5.2 Verne may update these measures, provided the update does not materially decrease the overall level of protection.

6. Sub-processors

6.1 Customer gives Verne general written authorisation to engage the sub-processors listed in Annex III, Part A.

6.2 Verne will notify Customer by email, at the data protection contact named in Annex I.A, at least 30 days before adding or replacing a sub-processor. Customer may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, Customer may terminate the affected Services and, notwithstanding any provision of the Terms on refunds, receive a refund of prepaid fees for the period after termination.

6.3 Verne engages each sub-processor under a written contract that imposes on it, in substance, the same data protection obligations as this DPA, and remains responsible to Customer for the sub-processor's performance.

6.4 Sign-in providers that Customer chooses to enable, such as Telegram, Google or GitHub, are not engaged by Verne as sub-processors. They are listed in Annex III, Part B, for transparency. Recipients that receive limited data from Verne and act as controllers of it are listed in Annex III, Part C.

7. Assistance

7.1 Verne provides API endpoints to retrieve, correct and delete end-user identities and to revoke their sessions, so that Customer can respond to data subject requests. Where these are insufficient, Verne will provide reasonable further assistance.

7.2 Verne will provide reasonable assistance with data protection impact assessments and prior consultations with supervisory authorities, taking into account the nature of processing and the information available to Verne.

8. Personal data breaches

8.1 Verne will notify Customer, at the data protection contact named in Annex I.A, without undue delay after becoming aware of a personal data breach affecting Customer Personal Data.

8.2 The notification will describe, as far as the information is available, the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed. Verne will provide further information as it becomes available.

9. Deletion and return

9.1 Before the Services end, Customer may export Customer Personal Data through the API.

9.2 The Services end when Customer's account is closed, at Customer's request or under the Terms. Within 30 days after the Services end, Verne will delete Customer Personal Data, unless Union or Member State law, or the law of Serbia, requires its storage. Verne deletes it in every place it keeps it, except encrypted backups, which expire as set out in 9.5:

(a) in Verne's databases: Customer's account and projects, API keys, scheduled and delayed jobs and their history, queued webhook events, outgoing emails waiting to be sent, Telegram sign-in settings and the bot token, the records of end users' activity, Customer's automatic-deletion rules and the record of their actions, and the audit log with its retention setting;

(b) in the identity service: the identities, credentials and sessions of Customer's end users, the authentication emails sent to them or to Customer's account, and unfinished sign-in and recovery requests;

(c) in the webhook delivery service: Customer's applications and endpoints, the messages and their payloads, and the delivery attempts;

(d) in the cache that holds API-key records, counters and session state, and in the analytics store.

Other persons whose accounts were members of Customer's projects lose that membership; their own accounts are not Customer Personal Data and are not deleted.

9.3 After deleting, Verne checks each of those places again, and records the deletion: the date, and the number of items found in each place before and after, which is nothing. The record contains no personal data. On request, Verne will confirm the deletion in writing, giving the date and stating that the check found nothing left.

9.4 The following are outside the deletion. Reverse-proxy access logs, which cannot be searched by Customer, expire by themselves within the period stated in Annex II. Application and monitoring logs, which may contain identifiers of Customer and its end users and IP addresses, are kept on a rolling basis on Verne's own servers and are not searched. Verne's correspondence with Customer, and payment and invoice records that Verne keeps as controller under 2.3 and for accounting, are kept as the law requires.

9.5 Copies of Customer Personal Data in Verne's backups (Annex II) are not deleted one by one. They are kept encrypted, are not restored except to recover the platform, and are deleted when the backup expires: a backup is kept for 30 days after it was made and is then removed by the storage provider's expiry rule, which the provider applies asynchronously, usually within a day, so a copy is gone no later than 35 days after it was made and therefore no later than 35 days after the deletion under 9.2. If a backup is restored, the deletion under 9.2 is repeated for every Customer that has left since the backup was made.

10. Audits

10.1 Verne makes available to Customer the information necessary to demonstrate compliance with this DPA, including this DPA, Annex II and the current list of sub-processors.

10.2 Where that information is insufficient, Customer may have an audit carried out by an independent auditor bound by confidentiality, on at least 30 days' written notice, at Customer's cost, and no more than once in any 12-month period unless required by a supervisory authority or following a personal data breach.

10.3 Nothing in this Section limits Customer's rights under Clause 8.9 of the SCCs.

11. International transfers

11.1 Customer Personal Data is hosted in France. Verne is established in Serbia, for which the European Commission has not adopted an adequacy decision. Access to Customer Personal Data by Verne from Serbia is therefore a transfer to a third country.

11.2 **European Economic Area.** The standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 (the "SCCs") are incorporated into this DPA by reference: Module Two where Customer is a controller, and Module Three where Customer is a processor. For the purposes of the SCCs:

(a) Clause 7 (docking clause) applies;

(b) under Clause 9(a), Option 2 (general written authorisation) applies, with the notice period set out in Section 6.2;

(c) the optional wording in Clause 11(a) does not apply;

(d) under Clause 13, the competent supervisory authority is determined as set out in Annex I.C;

(e) under Clause 17, Option 1 applies, and the SCCs are governed by the laws of France;

(f) under Clause 18(b), disputes are resolved by the courts of France;

(g) Annexes I, II and III of this DPA constitute Annexes I, II and III of the SCCs.

The SCCs are available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

11.3 **United Kingdom.** For transfers subject to UK data protection law, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner (version B1.0) is incorporated. Its Tables 1 to 3 are completed with the information in the Annexes of this DPA, and for Table 4 either party may end the Addendum.

11.4 **Switzerland.** For transfers subject to the Swiss Federal Act on Data Protection, the SCCs apply with these changes: references to the GDPR are read as references to that Act; the Federal Data Protection and Information Commissioner is the competent supervisory authority; and "Member State" is not interpreted so as to prevent data subjects in Switzerland from bringing claims in their place of habitual residence.

11.5 Transfers by Verne to sub-processors outside the European Economic Area are made under the safeguards listed in Annex III.

12. Liability

Each party's liability under this DPA is subject to the limitations in the Terms, except that nothing in this DPA or the Terms limits liability that cannot be limited under the SCCs or applicable law.

13. Governing law, disputes and precedence

13.1 This DPA is governed by the law that governs the Terms, except that the SCCs are governed as set out in Section 11.2(e).

13.2 Disputes arising from the SCCs are resolved as set out in Section 11.2(f). Other disputes under this DPA are resolved as set out in the Terms.

13.3 In case of conflict, the SCCs prevail over this DPA, and this DPA prevails over the Terms.

14. Term and changes

14.1 This DPA remains in effect for as long as Verne processes Customer Personal Data on behalf of Customer, including after any later change of Customer's plan.

14.2 This DPA may be changed only in writing signed by both parties, except that Verne may update Annex II under Section 5.2 and Annex III under Section 6.2. A change to the Terms does not reduce Customer's rights under this DPA.

15. Signatures

Each person signing below confirms that they are authorised to sign for the party they represent. The Effective Date is the later of the two dates below.

For Customer	For Verne
Signature:	Signature:
Name:	Name: Maksim Zhuk
Title:	Title: Entrepreneur, owner of Maksim Zhuk PR Novi Sad
Date:	Date:

Annex I — Parties and description of processing

A. List of parties

Data exporter	
Name	
Address	
Registration or VAT number	
Email of the Verne account	
Contact for data protection (name, position, email)	
Activities relevant to the transfer	Use of the Services.
Role	☐ Controller (Module Two) ☐ Processor on behalf of a third party (Module Three)
Signature and date	As in Section 15.

Data importer	
Name	Maksim Zhuk PR Novi Sad, doing business as Verne Software
Address	Zheleznichka 20, Novi Sad, Vojvodina 21101, Serbia
VAT number	RS113630704
Contact for data protection	Maksim Zhuk, owner, support@vernesoft.com
Activities relevant to the transfer	Provision of the Services.
Role	Processor (Module Two), or sub-processor where Customer is a processor (Module Three)
Signature and date	As in Section 15.

B. Description of processing

Categories of data subjects

- End users of Customer's applications who register or sign in through the Services, including through Telegram.
- Recipients of authentication emails and other notices that the Services send on Customer's behalf.
- Members of Customer's team: the account holder and any colleagues invited to Customer's projects, whose actions in the dashboard and through API keys are recorded in the audit log.
- Any individuals whose personal data Customer includes in webhook or job payloads.

Categories of personal data

- Identity data: email address, preferred language, membership and role in Customer's organizations, and any additional attributes or metadata Customer configures.
- Credentials: password hashes, one-time codes, recovery codes, second-factor secrets, and identifiers received from sign-in providers.
- Telegram sign-in data, where enabled: Telegram user ID, username, first name and profile photo URL.
- Session and security data: session identifiers, IP addresses, user agents, and timestamps of authentication events.
- Activity records: for each calendar month, the identifiers of the end users who signed in, used to count monthly active users; and the warnings sent and deletions made under Customer's automatic-deletion rules.

- Audit log: for each significant action, the identifier of the person who did it (an end user, a member of Customer's team, a member of Verne's staff acting on Customer's account, or the API key used), the kind of action, what it was done to, the time, and the IP address and user agent of the request. The actions are an end user's sign-in and password change; a change of an end user's role in an organization; and, for Customer's team, creating and revoking API keys, changing project settings, members and roles, sign-in provider and security settings, webhook endpoints, the automatic-deletion rules, and the log's own retention setting. The log holds no email address, name or password. The address of the request is the one that reached the Services: where Customer's backend drives a sign-in for its user, it is the backend's.
- Email data: recipient address and content of verification, recovery and sign-in emails, and of the notices sent under Customer's automatic-deletion rules.
- Payloads: the content of webhooks and scheduled jobs submitted by Customer, and of the events about Customer's end users (such as registrations and sign-ins) that the Services deliver to Customer's webhook endpoints. Verne does not inspect the content Customer submits.

Special categories of data

None intended. Customer shall not submit special categories of personal data in identity attributes, metadata or payloads.

Frequency of transfer

Continuous.

Nature of processing

Hosting and storage; authentication and session management; sending authentication emails and notices; delivering webhooks, including events about end users; executing scheduled HTTP requests; counting monthly active end users; deleting end-user accounts under rules Customer sets; keeping an audit log of significant actions for Customer.

Purpose

Providing the Services to Customer under the Terms.

Retention

Scheduled and delayed job execution history, and finished delayed jobs, are deleted once older than the window of Customer's plan, checked hourly: 7 days on the Free plan, 90 on Pro, and 180 on Advanced and on a contract plan. Job definitions themselves, and any job still pending or running, are kept until Customer deletes them or the Services end.

Webhook messages and their delivery attempts are deleted once they are 180 days old, checked daily. Message payload content expires earlier, no later than 90 days after sending.

Audit log entries are deleted once older than the window of Customer's plan: 7 days on the Free plan, 30 on Pro, 90 on Advanced, and on a contract plan the period agreed in the contract, or 90 days if it states none. Customer may shorten the window in the dashboard and may not lengthen it beyond its plan. The deletion runs hourly; an entry past the window is no longer shown from the moment it passes. Entries are never edited, and Customer cannot delete one earlier.

Otherwise, for the term of the Services, then deleted as set out in Section 9.

Transfers to sub-processors

As set out in Annex III, for the same nature and purpose, for the term of the Services.

C. Competent supervisory authority

(a) Where Customer is established in an EU Member State: the supervisory authority of that Member State.

(b) Where Customer is not established in an EU Member State but has appointed a representative under Article 27(1) GDPR: the supervisory authority of the Member State in which the representative is established.

(c) Where Customer is not established in an EU Member State and is not required to appoint a representative: the supervisory authority named here: _____.

Annex II — Technical and organisational measures

The measures below are those in place on 2026-11-05.

Hosting. The platform runs on servers in an OVHcloud data centre in France.

Encryption in transit. The websites and the API are served over TLS, with certificates issued by Let's Encrypt and managed by the reverse proxy. Plain HTTP requests are redirected to HTTPS, and browsers are instructed to use HTTPS only (HSTS).

Network exposure. Web and API traffic reaches the platform only through a single reverse proxy; apart from it, only the ports of Verne's own mail server are open to the internet. Databases, the cache and the internal services are reachable only from internal container networks; their ports are not published.

Attack filtering and rate limiting. Requests to the websites and the API are rate-limited at the edge and filtered by CrowdSec, which blocks addresses associated with attacks (Annex III, Part C).

Customer isolation. Each end-user identity is bound to the Customer that owns it, and API access is authorised with Customer-specific keys that enforce this binding.

Credential storage. API keys are generated from 32 random bytes and stored only as SHA-256 hashes. Passwords set through the Services are stored by the identity service (Ory Kratos) as bcrypt hashes with a cost factor of 12; password hashes that Customer imports from another system are stored in the form in which they were imported. Telegram bot tokens are encrypted with AES-256-GCM.

Second factor. Customer's end users, and members of Customer's team in the dashboard, can protect their sign-in with a one-time-code app (TOTP) and recovery codes.

Logging. The identity service is configured not to write sensitive values to logs.

Access log retention. Reverse-proxy access logs, which include end-user IP addresses, are rotated daily and kept for no longer than 14 days.

Email relay. Emails to end users leave Verne's mail server through Scaleway Transactional Email (Annex III), which accepts them only over an encrypted connection. As Scaleway states for that service, message content is encrypted and is deleted as soon as sending ends: when the recipient's server accepts the message, at the first permanent failure, or after 36 hours of failed attempts. A message classified as spam is deleted after 72 hours, a message held for a blocked domain after 15 days, and encrypted backups of message content after 7 days. Sending metadata and logs (sender and recipient addresses, subject, status, and the time and result of each delivery attempt) are kept for as long as Verne's sending domain is active with the service, and Verne can ask Scaleway to delete particular records.

Access control. Servers are administered by Verne's operator over SSH with key authentication. Deployments are made by a CI pipeline with its own key, and a key used for automated monitoring can run only a fixed list of commands. The administrative panel is served on a separate host and requires an administrator identity, which is kept apart from customer accounts.

Change management. An automated test suite must pass before any change is deployed; deployment is performed by a CI pipeline.

Monitoring. Automated external health checks run every 3 hours, a watchdog on the server runs every 3 minutes, and service status is published on a public status page.

Audit log. Significant actions of Customer's team and of its end users are recorded in a log that cannot be changed through the Services: the database refuses any update, and any delete other than the scheduled removal of entries past the retention window and the deletion of Customer's account. An action taken in the dashboard or with an API key is recorded in the same database transaction as the action, so neither is saved without the other. A sign-in and a password change happen inside the identity service, so they are recorded when it reports them to the gateway; one it does not report is not recorded, and a failed sign-in is not reported. The log holds identifiers and no email address. Customer reads it in the dashboard (project owners and admins) and through the API; the gateway, not the caller, states who and from where.

Automatic deletion. Job history, webhook messages and audit-log entries are deleted automatically after the periods set out in Annex I.B.

Data subject rights. API endpoints allow Customer to retrieve, update and delete end-user identities and revoke their sessions.

Backups. The three databases that hold Customer Personal Data (accounts and configuration, end-user identities and credentials, webhook configuration) are dumped once a day and encrypted on the server with a public key before they leave it; the private key is held only by Verne's operator and is not on the server. The encrypted copies are stored in OVHcloud Object Storage in France (Paris region, a different site from the servers), where the storage provider also encrypts them at rest. Each copy is locked against deletion and overwriting for 30 days and is then deleted, no later than 35 days after it was made. The server's own access to that storage cannot delete or overwrite copies, so a compromise of the server does not let an attacker erase the backups. Email content, support mailboxes, usage analytics and operational telemetry are not backed up. Backup freshness is monitored automatically, and restoring from a backup has been tested.

Annex III — Sub-processors and other recipients

As of 2026-11-05.

Part A — Sub-processors engaged by Verne

Sub-processor	Purpose	Location of processing	Transfer safeguard
OVH SAS (OVHcloud), 2 rue Kellermann, 59100 Roubaix, France	Hosting of the platform and storage of encrypted backups	France: servers in a French data centre; encrypted backups in OVHcloud Object Storage, Paris region	Not needed (inside the EEA)
Scaleway SAS (Scaleway Transactional Email), 8 rue de la Ville-l'Évêque, 75008 Paris, France	Relaying the authentication emails, and the notices under Customer's automatic-deletion rules, that the Services send to Customer's end users	France (Paris region). Scaleway states that it stores and processes this data in France and does not replicate, cache or back it up outside the EU. It deletes the content once the recipient's mail server accepts the email (after 36 hours of failed attempts at the latest), but keeps sender and recipient addresses, subject and delivery status for as long as Verne's sending domain is active, and says it plans to shorten that in 2027	Not needed (inside the EEA). Scaleway's data processing agreement applies

Part B — Sign-in providers enabled by Customer

These providers are used only if Customer enables them, and they act under their own relationship with the end user.

Provider	Used for	Location stated by the provider
Telegram Messenger Inc.	Sign-in with Telegram through Customer's own bot	For users who registered from the EEA or the UK: data centres in the Netherlands
Other sign-in providers configured by Customer, for example Google or GitHub	Sign-in with that provider	As stated by each provider

Part C — Other recipients acting as controllers

These recipients are not engaged to process Customer Personal Data on Verne's behalf. They receive the limited data shown, for the purpose shown, and decide for themselves how they use it, under their own privacy policies.

Recipient	Data received	Purpose	Location
CrowdSec SAS, 20 rue Maurice Arnoux, 92120 Montrouge, France	IP addresses that trigger Verne's attack detection	Network security: blocking addresses known for attacks	France. Per its documentation, kept up to three months