Privacy policy

Version 2026-09-01.1 · Effective date 1 September 2026

CorVpoint STUDIO · Courtepin, Switzerland · corvpoint.ch

Controller

The controller for the processing described in this policy is:

CorVpoint STUDIO
Sylvain Sébastian Amiet
Le Centre 29
1784 Courtepin
Switzerland

Email: info@corvpoint.ch

Scope and roles

This policy applies to the public website corvpoint.ch, to contact and project requests, to the customer portal where it is used, and to CorVpoint's own business administration.

CorVpoint is the controller for website, prospect, customer and own business data. If CorVpoint acts in a project as a processor for the customer's personal data, this occurs only under a separate agreement, typically a data processing agreement. This website policy does not replace such a contract.

Applicable data-protection law

Swiss data-protection law applies, in particular the Federal Act on Data Protection (FADP, SR 235.1) and the Data Protection Ordinance (DPO, SR 235.11).

The EU General Data Protection Regulation may apply in addition where CorVpoint offers services to persons in the EEA or monitors their behaviour on the website (Art. 3 GDPR). The website is available in German, French, Italian and English and accepts project requests from abroad. For such cases this policy also states GDPR bases and rights, without claiming that every data-protection law worldwide applies automatically.

Data categories and sources

In particular the following are processed:

- master and contact data, such as name, company, address, email, telephone number, where provided
- communication and project data from forms, briefings, attachments, emails and portal messages
- account data for login, roles, password reset and sessions
- offer, contract, invoice and payment metadata, including status, timestamps, document versions, hashes or snapshots and provider references
- technical usage and security data, such as IP address, user agent, referrer, time, requested resource and internal review notes
- where IP mapping is configured, coarse location at country, region or city level

Sources are your submissions, technical website logs, payment confirmations of the payment provider and internal administrative records. CorVpoint does not buy address lists and does not operate marketing profiling.

Hosting and technical delivery

The website is operated on own infrastructure in a rented server environment. When the site is accessed, technically necessary connection data arise in order to deliver pages, detect errors and prevent abuse.

There is no lasting storage of every individual page view as a marketing profile.

Security and access logs

For stability, abuse prevention and traceability, server, access, error and audit logs may contain IP address, user agent, referrer, time and internally set security markers.

Optional mapping of an IP address to coarse geodata occurs only if it is configured server-side. Visitor logs are retained under a capacity-driven policy. Blocked or particularly high-risk entries may be kept longer where this is required for security.

Contact, project briefing and uploads

If you use the contact form, the project briefing or an upload, CorVpoint processes the data you enter, attachments, locale, page context, a technical captcha check and sender IP and browser metadata for request handling and abuse prevention.

Submission is voluntary. Without certain data a request cannot be processed fully. Please send only data that are needed for the matter. Particularly sensitive data should not be sent unsolicited.

Customer account, login and portal

A customer account processes username or email, password hash, role, activation status and session data. A password reset stores time-limited token hashes, typically for one hour.

The session cookie is httpOnly, sameSite=lax and lasts seven days. Portal messages and project status remain bound to the account.

Offers, contracts, invoices and payments

For offers, digital acceptances, invoices, deposits, milestones and project-start gates, contract and invoice data, status, timestamps, IP and browser metadata on online acceptance, document versions, hashes or snapshots, provider IDs and internal review notes are processed.

CorVpoint does not store card, TWINT or bank data. Payments may be made through Stripe Checkout. Payment status is derived only from server-side verified provider messages, webhooks, administration evidence or documented manual checks. Return pages after a payment serve only user guidance.

Email and SMTP

System and request messages are sent by SMTP. Depending on configuration this may be a mail host of the server provider. Content, recipients and technical delivery logs of the relevant message are processed for communication and traceability.

Open email channels can have security gaps. Particularly confidential documents should be sent only through the expressly provided channel.

Free online checks

The voluntary tools under Projects, Free checks, process data only for their purpose:

- In the internet speed test, measurements are calculated in the browser. For rate limits, IP address, time and data volume may be processed briefly on the server. No lasting personal measurement result is created.
- In the website security check, the entered public URL is queried once on the server. Domain, individual results and full response headers are not stored lastingly and are not taken into marketing profiles.

Neither tool requires an account.

News and social links

Published news items may appear in the sitemap. A newsletter subscription is not currently set up.

Social-media icons in the footer are linked only if an address is set. After leaving the website the rules of the respective service apply. No social plugins, tracking pixels or advertising networks are loaded from this website.

AI and assistance tools

The public website currently runs no visitor chatbot and no automatic publication of AI-generated page content.

In projects CorVpoint may use AI or automation tools for analysis, structuring or text, code and data assistance where this is useful and agreed. Confidential customer data are not handed to external models in an uncontrolled way. Special secrecy or sector requirements must be stated in advance.

Cookies and similar technologies

No analytics, advertising or social trackers and no third-party marketing cookies are currently used. A consent banner is therefore not provided. Continuing to browse is not treated as consent.

Technically necessary first-party mechanisms are:

- corvpoint_session: sign-in for administration or the customer portal, httpOnly, 7 days
- corvpoint_preferred_locale: language choice, cookie and localStorage, 1 year
- corvpoint_admin_locale: administration language, 1 year, admin only
- cp_template_preview: signed preview cookie for templates, 8 hours, admin only
- contact captcha: short-lived HMAC in the form, 15 minutes

These accesses serve operation, security, language or an expressly started admin preview. If non-necessary trackers are introduced later, they will not be loaded before consent.

Browser storage

In addition to cookies the website uses localStorage for the public theme choice (corvpoint-theme) and separately for the admin appearance. sessionStorage may remember the return language after an admin logout.

Demo layers may use their own localStorage or sessionStorage keys. They are not the productive customer processing. IndexedDB and Cache Storage are not currently used as data processing for the public website.

Recipients and service providers

Personal data are not sold. Disclosure occurs only as far as necessary to:

- hosting and infrastructure providers
- email or SMTP service
- payment providers, currently Stripe Checkout, where a payment is started
- optionally an IP information service, only if enabled server-side
- authorities or courts where legally required

Stripe may process data in Switzerland, the EEA or further states. Stripe's terms apply in addition. CorVpoint receives payment status and provider references, not complete card data.

Countries and data transfers

Operation and primary storage take place in the Swiss server environment insofar as the infrastructure used reflects this.

Transfers to the EEA may be based on adequacy or on contractual bases. Transfers to the USA, in particular in connection with Stripe, occur only where that service is used and only under the transfer rules then applicable to the service. Standard contractual clauses or a Swiss addendum are mentioned here only where they are actually used for the concrete service. No blanket statement is made about all possible future tools.

Retention

Separate logics apply:

- statutory retention for business books, contracts and invoices under Swiss obligation and tax law, typically ten years where applicable
- requests, briefings and uploads: as long as needed for handling, offer, contract or evidence; no automatic deletion period in the running system, deletion via administration possible
- password-reset tokens: one hour
- session: seven days
- captcha: fifteen minutes
- visitor logs: capacity-driven, at least 24 hours unless security-relevant
- temporary upload fragments: two hours

After the purpose ends, data are deleted, anonymised or restricted in processing unless a statutory or evidence-related basis continues.

Security

CorVpoint takes appropriate technical and organisational measures, including access controls, session protection, server-side form and upload checks, rate limits and logging of security-relevant events.

Absolute security of electronic communication is not warranted.

Data-security breaches

In the event of a data-security breach CorVpoint assesses whether a notification to the FDPIC and information of affected persons is required under the FADP, in particular where there is a likely high risk to personality or fundamental rights.

Where the GDPR applies, its notification periods apply in addition. No outcome is promised.

Rights of data subjects

Under Swiss law you may in particular request access, rectification, erasure or restriction, object where provided, and withdraw consent with effect for the future.

Where the GDPR applies, the rights in Articles 12 to 22 GDPR are added, including data portability where applicable. Suitable evidence may be requested to verify identity. Please send requests to info@corvpoint.ch.

Complaint

You may lodge a complaint with the Federal Data Protection and Information Commissioner (FDPIC) where that authority is competent.

Persons in the EEA may additionally contact the supervisory authority of their place of residence, work or alleged infringement. No specific foreign authority is designated here as competent, because this depends on the individual case.

No automated individual decisions

CorVpoint does not take automated individual decisions with legal or similarly significant effect on this website. Commerce gates and security checks support handling but do not replace a human decision on a contract or a refusal.

Minors and particularly sensitive data

The offering is not directed at children. Particularly sensitive personal data should not be sent unsolicited through forms. If they are nevertheless provided, processing is limited to what is indispensable for the request.

Changes

This policy may be adapted when law, technology or processes change. The version published on the website with the stated version and effective date applies.