SiteForge Privacy Notice

Version 1.2 | Effective on publication

This notice explains how SiteForge uses personal information, who receives it, how long it is kept and how to exercise your rights. It also explains when a customer controls project information. Acknowledging this notice is not blanket consent.

Who we are and how to contact us

SiteForge Construction Software Ltd, trading as SiteForge, provides construction project software for UK businesses. We are registered in England and Wales, company number 17313591, at 4 Marsa Way, Bridgwater, England, TA6 5JN. Contact support@siteforge.uk.com or 01278 588266 for privacy questions, rights requests or complaints. Security concerns can be reported to security@siteforge.uk.com.

SiteForge and customer roles

SiteForge decides how it uses minimum identity, authority/acceptance records, its billing/project-fee verification, proportionate fraud/security records and business/support correspondence. For project content that a customer asks us to host/process, that customer normally controls the purposes and SiteForge acts as processor, or subprocessor where the customer is an authorised processor. The customer's additional project-controller privacy obligations are separate from SiteForge delivering its own User Terms and Privacy Notice. Ask the business responsible for your project about its purposes; we help route requests and handle our own controller records separately.

What information we use and where it comes from

We receive information when you register, are invited, acknowledge/agree documents, pay, provide project-value evidence, contact us or use the service. This can include names, business email/contact details, identity/authority and verification records, accepted document versions/times, memberships/permissions, payment references/status, support messages and relevant service/security events. Businesses/authorised users can provide invitations and project information. Required project-value evidence normally takes the form of a valid tender return/acceptance document and can include business contacts or signatures; provide only what is needed. Project material may include named people in files/photos/comments. Card details are entered through Stripe-hosted services; SiteForge does not receive the full card number/CVC through that checkout.

For planned relevant business telephone calls, we may collect a business contact name, role, company, telephone number and source from company websites or other legitimate business sources, alongside screening and call outcomes. We will explain the source when appropriate and provide privacy information no later than the applicable Article14 deadline, normally within one month and at the first communication if earlier. We do not use signup addresses for unsolicited marketing emails and do not treat an enquiry as consent to a campaign.

Why we use information and our lawful bases

We use necessary information to create/secure accounts, enforce authorised access, record agreement/notice versions, supply the service, verify project-value charges, answer enquiries and administer billing. Contractual necessity applies where the individual is our contracting party, such as a sole trader. For corporate contacts/invited users and proportionate fee verification/fraud/security work, appropriate legitimate interests support running a secure business service and administering the relationship. Customers determine lawful bases for their instructed project processing; SiteForge follows lawful instructions for that work. We do not treat acceptance of User Terms or acknowledgement of this notice as blanket consent.

Specific company accounting/tax and applicable data-protection duties use legal obligation. Legitimate interests support proportionate security, fraud investigation and necessary legal claims. Planned

relevant B2B phone calls follow our legitimate-interests assessment, TPS/CTPS checks and objections; you may object to direct marketing at any time. We do not use these purposes for unrelated profiling, advertising to young users or customer-content model training. Project-value concerns are reviewed by a person and the Account Holder is contacted to seek resolution before evidence-related restriction/termination, as stated in the SaaS agreement. Any genuinely optional use needing consent is explained and requested separately, with a way to withdraw.

When homepage measurement is enabled, we count visits to understand how much use our public site is getting. To estimate how many visits come from different connections each day, our server uses the IP address received with the request to create a code that changes daily. We do not store raw IP addresses for this measurement, use cookies for it, or link the counts to user accounts.

The codes expire from the live counter at the end of each UK calendar day. We keep daily totals for 30 days. Short-lived codes may remain in protected recovery records until those records are replaced or expire.

Our legitimate interest is measuring use of our public website. You can object to this use using the contact details in this notice.

Project sharing photographs and drawings AI

Project information is shared with the people the customer authorises through account/project membership, roles and module permissions. A photo described as Public in the project is for the permitted project audience; it is not a statement that it is published on the internet. Protected photos have narrower access. Ask your project administrator if you are unsure who can see your upload, and avoid uploading unrelated personal or sensitive information.

Generated photo previews remove GPS, but original files remain unchanged and can contain GPS/device/capture information. People authorised to preview/download originals or receive archives may see it. Markup layers are private to their creator; deliberately exported/shared copies follow destination permissions. Do not share original metadata you lack authority to share. SiteForge does not collect live device location through this photo-upload feature. The point-of-upload/original-access information explains these differences.

When drawings AI is enabled and authorised, drawing content goes to the OpenAI API for extraction/matching suggestions, with human checking and a manual review route. We do not make fully automated decisions with legal or similarly significant effects about people through this drawing review. Customer content is not authorised for unrelated model training. Requests use store=false and temporary provider files are deleted with retry cleanup; this does not mean every operational provider record has zero retention. Provider processing and international safeguards are described in the customer DPA/provider information.

Invited users aged 16 and 17

Customers must have an adult authorised representative. Invited business users may be aged 16 or over. If you are 16 or 17: use SiteForge only for your authorised work role, check the project audience before sharing, and ask for help if you are unsure. Your name, comments, uploads and relevant work activity can be visible to authorised project users. Original photos can contain location information. You can contact us about your information without having to ask a parent to do so. We do not ask for a date of birth simply to create an account, and a parent or employer does not automatically receive all your private account information. We assess proportionate safeguards for this use.

Service providers and international access

DigitalOcean hosts the service/database/files/backups; Laravel Forge manages servers; Resend delivers transactional/authentication/project messages; Google Workspace handles business mail and relevant support; OpenAI assists enabled drawing review. Laravel Nightwatch receives redacted technical diagnostics, potentially including internal actor IDs. Netdata handles host/resource monitoring, not platform user-account activity. Stripe provides payments, Xero invoicing and Monzo banking. SecondRing (Hallmark Logic UK Ltd) provides basic phone service without

voicemail/recording/transcription. 121prodata is selected for planned TPS/CTPS screening. WhatsApp is optional external general support only: do not send project files. Customer-authorised project recipients have their own roles. We may disclose necessary information where legally required; no unrelated marketing rights arise merely from uploading content.

Live application/database/files are in London, UK; protected project-file backup is Amsterdam, Netherlands. Nightwatch's EU production environment is recorded, but provider support/control-plane processing can still be international. Workspace is non-regional; Resend sends from Ireland with US storage; OpenAI is a Global service. Other authorised support/onward routes may involve the EEA, United States and locations in the relevant provider information. Applicable safeguards include UK adequacy routes (including eligible UK Extension recipients) or appropriate UK Addendum/SCC arrangements with the required assessment. Ask support for relevant current provider/transfer details or a copy of available safeguards, with necessary confidential information protected. UK-only customers do not imply UK-only processing.

How long we keep information

When a subscription lapses there are 14 calendar days of grace access. Within that period, authorised project information can be downloaded as archives once each project is marked Completed in Project Settings. From 30 calendar days after verified lapse, including grace, eligible account data/files may be permanently deleted manually after checks. This is not automatic deletion or a fixed completion deadline. An authorised customer can request closure through support; final deletion is irreversible and is not followed by an account-restore service. Binned files normally expire after 30 days unless purged earlier; ready generated archive downloads normally expire after 28 days. These are not source-project lifetimes. Customer/controller instructions and individual rights are handled separately from the subscription clock.

Financial records are normally kept for at least six years after the relevant financial year. Ordinary periods are support/enquiries 12 months after resolution; routine security logs normally up to 90 days; minimal rights/complaint/breach decision records reviewed three years after closure; unresponsive prospects reviewed after 12 months; agreement evidence reviewed six years after termination. We keep only minimal suppression records needed to respect objections and limited longer records for legal duties/justified holds. Project-value evidence is kept only as needed for verification and related issues under the relevant cleanup rules; necessary billing/decision records are separate. Nightwatch publishes a 90-day default for redacted diagnostics; a shorter applicable plan period may apply. Provider message logs such as Resend normally have their own shorter retention.

After account deletion or user removal, we may retain limited agreement evidence, including the contracting business name, accepting person's name and email, authority confirmations, document versions and acceptance dates. We restrict its use to necessary contract, legal-claims and accountability purposes. We normally review agreement evidence six years after the relevant relationship ends and delete it when no longer needed, unless justified continued retention applies.

Protected host/database recovery history is normally seven days; twice-daily project-file backup history retains changed/deleted files for 30 days. Older copies remain out of ordinary use and applicable deletions/restrictions are reapplied before recovered infrastructure reopens. Diagnostic IDs are not presumed anonymous or immediately selectively erased from all provider history.

Your choices rights and complaints

You may request access, correction, erasure, restriction or portability where applicable, object to relevant processing (including direct marketing at any time), or withdraw consent you gave for a distinct optional purpose. Contact support by email, phone or writing; no paid adviser or special form is needed. We may verify identity/authority and normally respond within one calendar month, subject to lawful extensions/adjustments. We can retrieve relevant personal information manually and provide it securely, protecting other people's information; a project archive is not the only way to answer a rights request. Removing a user disables login and anonymises profiles, while project/history records can remain; particular erasure requests are assessed separately with the relevant controller. Rights/incident deadlines are not the SaaS service-breach cure period.

For a privacy complaint, contact support@siteforge.uk.com, 01278 588266 or our registered office with what happened and how to reach you. We start considering it on receipt, acknowledge within 30 days, investigate, keep you informed and explain the outcome without undue delay. You may complain to the Information Commissioner's Office at ico.org.uk. We do not require a special form or paid adviser. For customer-controlled project data we help identify/contact that customer and still address our own processing. The 30-day acknowledgement limit does not mean we wait 30 days to begin investigating.

Browser storage and changes

We use necessary browser/session storage for authentication, security, preferences and service functions. The separate Cookies and Browser Storage Notice explains actual storage and optional choices, including click-to-load YouTube and mobile view memory. We do not use advertising or browser-based analytics. The limited server-side homepage measurement described above uses no browser storage. We publish updated privacy information when purposes, providers or relevant practices change and draw significant changes to affected users' attention where appropriate. A required onboarding acknowledgement records which notice was supplied/read; it is not marketing consent. Provide required account/contact/authority and project-value information to use the relevant signup/payment/project functions; if it is not supplied we may be unable to provide those functions. You can decline optional provider/consent choices without that becoming consent to all processing.