

Data Processing Agreement

Last updated 7 October 2026 · GDPR Art. 28 contract.

Translations of this document are provided for convenience. In case of any difference between a translation and this English version, the English version prevails.

How this works

This DPA forms part of the Terms of service. It activates automatically when a workspace is created and personal data is uploaded into it. The customer organisation that owns the workspace is the controller; Dazr is the processor. No signature is required; if your procurement process needs a counter-signed copy, email legal@dazr.eu.

1. Definitions

Terms in this DPA carry the meaning given in Regulation (EU) 2016/679 (the GDPR). "Customer Personal Data" means personal data the controller (or its members or auditors acting under it) puts into the workspace, including any personal data inside control task content, evidence, comments, files, risks, incidents, vendor records, members and invites, public-intake submissions, and the activity log.

2. Subject matter, duration, nature and purpose

- Subject matter: processing Customer Personal Data so the controller can manage its information-security and data-protection compliance program through the Dazr Compliance platform.
- Duration: for the term of the controller's subscription, plus the post-termination grace period in the Terms.
- Nature and purpose: hosting, storage, transmission, retrieval, erasure, and the operations described in the Terms and the Privacy Policy.
- Type of personal data: identification data of workspace members and invited auditors (email, name, role); identification data of public-intake reporters and incident reporters where applicable; employer contact data and operational metadata uploaded by the controller. The controller is responsible for not uploading special-category data unless its own legal basis allows it.
- Categories of data subjects: the controller's employees, contractors, invited external auditors, and any individuals identified in compliance content that the controller chooses to upload.

3. Processor obligations

1. We process Customer Personal Data only on documented instructions from the controller. The instructions are the act of using the platform's intended functions; if we believe an instruction infringes the GDPR or another EU/Member-State data-protection law, we will inform the controller.
2. We ensure that persons authorised to process Customer Personal Data have committed themselves to confidentiality.
3. We take all measures required pursuant to Art. 32 GDPR (Security of processing). The current measures are described in section 7 below.
4. We respect the conditions in Art. 28(2) and (4) for engaging sub-processors (see section 6).
5. We assist the controller, taking into account the nature of processing and the information available to us, in fulfilling its obligation to respond to data-subject rights requests, breach notifications, DPIAs, and prior consultations with supervisory authorities (Art. 28(3)(e) and (f)).
6. At the controller's choice we delete or return all Customer Personal Data after the end of the provision of services, and delete existing copies unless EU or Member-State law requires storage.
7. We make available to the controller all information necessary to demonstrate compliance with Art. 28, and

allow for and contribute to audits, including inspections (see section 9).

4. Controller obligations

- The controller warrants it has a lawful basis under Art. 6 (and where relevant Art. 9) for the personal data it puts into the workspace.
- The controller is responsible for the accuracy of Customer Personal Data and for responding to data-subject rights requests over its workspace (we'll route any such requests we receive to the controller, and assist as required by Art. 28(3)(e)).
- The controller controls access - member roles, auditor invitations, the public-intake portal - through the platform's controls.

5. International transfers

Customer Personal Data is stored and processed on servers in the European Union. Vercel, Upstash and Namecheap are companies based in the United States; should one of them access Customer Personal Data from outside the EU, the transfer is governed by the European Commission's Standard Contractual Clauses (Decision 2021/914), module 3 (processor to processor), with the supplementary measures described in section 7. The current sub-processors and their server regions are at </legal/subprocessors>.

6. Sub-processors

1. The controller authorises us to engage sub-processors to provide the service. The current list is at </legal/subprocessors>.
2. We will inform the controller of any intended additions or replacements at least 30 days in advance by email to the workspace owner and to anyone who has asked us at privacy@dazr.eu to be told.
3. The controller may object on reasonable data-protection grounds. If we cannot accommodate the objection, the controller may terminate the affected service and receive a pro-rated refund for the unused remainder of the current billing period.
4. We impose on every sub-processor, by written contract, data-protection obligations no less protective than those in this DPA, and we remain liable to the controller for the performance of the sub-processor's obligations.

7. Security measures (Art. 32)

- Encryption. Workspace records are encrypted with AES-256-GCM by the application before they are stored, on top of the storage provider's at-rest encryption, with keys derived (HKDF-SHA-256) from a 256-bit master key that is held only as a secret of the production environment, separate from the stored data; the master key can be rotated, after which a background job re-encrypts the stored records. Uploaded files (evidence, policy and profile documents, breach-report attachments) are encrypted at rest by the storage provider, stored under random addresses that cannot be guessed and served only after an access check; SBOM files in the Cyber Resilience Act module are also encrypted by the application. All transport is HTTPS with HSTS preloaded; no plaintext fallback.
- Access control. Role-based access control inside the platform (owner / admin / member / auditor); time-boxed and revocable auditor sessions. Operational access is limited to a small support team via the support portal, which is metadata-only by design.
- Authentication. Passwordless sign-in with Google or Microsoft (OpenID Connect) or a one-time email code; auditors confirm a one-time email code. HMAC-signed session tokens with limited TTL. Rate limiting on every public endpoint, including admin login.
- Resilience and integrity. An activity log of every state-changing action, keeping the most recent 2,000 to 50,000 events depending on the plan. Backups inside the EU. Integrity of stored payloads is verified by AEAD authentication tags; tampered ciphertexts decrypt to an error and are not served.

- Network and headers. Strict Content-Security-Policy with hashed inline-script allow-list, strict X-Frame-Options, X-Content-Type-Options nosniff, and HSTS preload.
- Vulnerability management. Dependencies are pinned; we monitor advisories and patch on a schedule appropriate to severity.

8. Personal data breach

If we become aware of a personal-data breach affecting Customer Personal Data, we will notify the workspace owner without undue delay and at the latest within 72 hours of becoming aware (Art. 33(2)). The notification will describe, to the extent known: the nature of the breach, the likely consequences, the measures taken or proposed, and the contact point for more information. We will assist the controller with its own notification obligations under Art. 33 and Art. 34.

9. Audits

The controller (or a third-party auditor it has mandated) may audit our compliance with this DPA once per twelve months, on at least 30 days' written notice and during business hours, in a manner that does not unreasonably interfere with our operations and that respects the confidentiality of other customers' data. We may charge a reasonable fee for any audit beyond this allowance. Where an Art. 28(3)(h) audit obligation can be satisfied by a third-party attestation we hold, we will provide it in lieu of an on-site audit.

10. Liability

Each party's liability under this DPA is subject to the limits in the Terms of service. Nothing in those limits caps liability for damages incurred by data subjects under Art. 82 GDPR.

11. Term and termination

This DPA continues for as long as we process Customer Personal Data, and survives termination of the Terms of service to the extent and for the duration that we still hold any such data. Sections 8 (breach), 9 (audits), and 12 (return / deletion) survive termination.

12. Return and deletion

On termination of the service, the controller may export workspace data through the platform's export tools during the 30-day grace period in the Terms. After the grace period we delete Customer Personal Data; backups are aged out per our retention schedule. Records we are required to retain (e.g. invoicing under Italian commercial law) are kept only for the period of that obligation.

13. Order of precedence

If there is a conflict between this DPA and the Terms of service or the Privacy policy, this DPA prevails on data-processing matters. SCCs incorporated for any non-EU transfer prevail over both this DPA and the Terms with respect to the matters they regulate.

14. Notices

- To Dazr: privacy@dazr.eu (data protection) or security@dazr.eu (incidents).
- To the controller: the workspace owner email on file at the time of notice.