Data Processing Addendum (DPA)

SecForm · Version v1.0 · Last updated 17 May 2026

This Data Processing Addendum ("DPA") forms part of the SecForm Terms of Service between SecForm ("Processor") and the customer identified in the order or account ("Controller"). It governs the Processing of Personal Data by the Processor on behalf of the Controller and satisfies Article 28 GDPR. Where international transfers are necessary, the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914) are incorporated by reference (Module 3).

1. Subject matter and duration

Provision of the SecForm form-building, hosting and submission-management service for the term of the Terms of Service, plus retention periods set out in section 7.

2. Nature, purpose and categories

Nature/purpose: collection, storage, structuring, retrieval, transmission and erasure of form responses on the Controller's behalf.
Data subjects: the Controller's end users, applicants, customers, employees, or other respondents.
Personal Data: identifiers (name, email, phone), contact details, free-text answers and uploaded documents — as configured by the Controller. Special categories only where the Controller chooses to collect them and has a valid Article 9 basis.

3. Processor obligations (Article 28)

SecForm shall: (a) process Personal Data only on documented instructions from the Controller; (b) ensure personnel are bound by confidentiality; (c) implement appropriate technical and organisational measures (section 6); (d) engage sub-processors only under section 4; (e) assist the Controller with Data Subject rights, security, breach notification, DPIAs and prior consultations; (f) at the Controller's choice, return or delete all Personal Data at the end of the service; (g) make available all information necessary to demonstrate compliance and allow for audits (section 5).

4. Sub-processors

The Controller grants general authorisation for the sub-processors listed below. SecForm remains liable for their acts and omissions and will notify the Controller of any intended addition or replacement at least 30 days in advance.

Sub-processor	Purpose	Location	Transfer
Supabase (Postgres/Auth/Storage)	Primary application database, auth, encrypted file storage	Frankfurt, DE	EU/EEA
Cloudflare, Inc.	CDN, DDoS, WAF, Turnstile CAPTCHA	EU edge PoPs	SCCs for incidental US
OVHcloud SAS	Backups and DR snapshots	Gravelines / Roubaix, FR	EU/EEA
Resend / Postmark	Transactional email delivery	EU region endpoints	SCCs for incidental US
Sentry (self-hosted EU)	Error monitoring (PII scrubbed)	Frankfurt, DE	EU/EEA

5. Audits

SecForm makes available, on request, its current security documentation (architecture overview, sub-processor list, penetration-test summary, and, where applicable, ISO 27001 / SOC 2 reports). On-site audits are available with 30 days' notice, no more than once per 12 months, under NDA and reasonable scoping.

6. Security measures (Annex II)

Encryption: AES-256 at rest, TLS 1.2+ in transit, signed time-limited URLs for file downloads.
Access control: RBAC, mandatory SSO + MFA for staff, least privilege, quarterly access reviews.
Network: WAF and DDoS protection at the edge, IP allow-lists for admin endpoints, isolated production VPC.
Application: dependency scanning, secret scanning, mandatory code review, automated SAST on every merge.
Logging: centralised audit logs, anomaly detection, 24/7 on-call rotation.
Resilience: daily encrypted backups, point-in-time recovery, RTO ≤ 4h / RPO ≤ 1h.
Personnel: background checks, confidentiality agreements, annual training.
Incident response: Controller notified within 72 hours of a confirmed personal data breach affecting their data.

7. Return and deletion

On termination, SecForm will, at the Controller's choice, return or delete all Personal Data within 30 days, and delete existing copies within 90 days (including from encrypted backups as rotation completes), unless EU or Member-State law requires further storage.

8. International transfers

Personal Data is stored and processed exclusively within the EU/EEA. For any incidental transfer to a sub-processor's non-EEA parent entity, the SCCs (Module 3) apply together with supplementary measures including encryption, strict role-based access, and transfer-impact assessments.

9. Governing law

This DPA is governed by French law. The courts of Paris have exclusive jurisdiction, without prejudice to Data Subject rights under Article 79 GDPR.

Signatures

For the Processor (SecForm)	For the Controller (Customer)
Name:	Name:
Title:	Title:
Entity:	Entity:
Date:	Date:
Signature:	Signature:

Return a signed copy to **dpo@secform.fr**. A countersigned PDF will be returned within 5 business days. The live version of this DPA is published at **secform.fr/dpa**.