CROPILOT

Data Processing Agreement

Version: 2026-09-review-v1

REVIEW DRAFT - NOT OPEN FOR ACCEPTANCE

Document SHA-256: 3b73e7509a4f2c81fd0f40afff6d56521318b00c42a7c5a5cf3ac32057e48e18

1. Parties and scope

This Data Processing Agreement (DPA) supplements the CroPilot service agreement between CROPILOT AS, organisation number 937 028 245, Elisenbergveien 17, 0265 Oslo, Norway (Processor), and the legal entity identified in the acceptance record (Customer). The Customer acts as controller, or as a processor authorised by its controller to appoint CroPilot as a subprocessor. The Customer remains responsible for that authority.

The DPA applies when CroPilot processes personal data on the Customer's behalf to provide the enabled website observation, analytics, recommendation, review and testing services. It does not itself activate those services, authorise visitor tracking, publish a change, approve model spending or change subscription terms. For Customer Personal Data, this DPA prevails over inconsistent service terms. GDPR means Regulation (EU) 2016/679 as applicable in the EEA.

2. Documented instructions and confidentiality

CroPilot will process Customer Personal Data only on documented instructions, including this DPA, its completed schedules, the service configuration and authorised requests. Transfers are subject to section 6. If law requires other processing, CroPilot will notify the Customer before processing unless the law prohibits that notice. CroPilot will promptly inform the Customer if an instruction appears to infringe applicable data-protection law and suspend the affected instruction pending clarification.

Access is limited to people who need it to provide the service and are bound by confidentiality obligations. Customer Personal Data must not be used for unrelated advertising, sale, cross-customer model training or another independent purpose under this DPA. Separately enabled providers and purposes must be disclosed and authorised in the schedules.

3. Customer responsibilities

The Customer determines the purposes and lawful basis for its processing, supplies accurate instructions, gives required notices, obtains any necessary consent, and ensures that it has rights to the submitted content and connected websites. It must configure collection to avoid unnecessary personal data and must not intentionally submit special-category data, criminal-offence data, passwords, payment-card details or children's data without a separately agreed, lawful scope.

The Customer chooses authorised representatives and reviews access. Agencies must have their clients' documented authority. Accepting this DPA is not consent from website visitors.

4. Security and personal-data breaches

CroPilot will implement appropriate technical and organisational measures under GDPR Article 32, considering the risks, including access control, tenant isolation, protected transport, restricted operational access, data minimisation, recovery procedures and security monitoring. The applicable measures and implementation limits are specified in Schedule B; this is not a certification or an availability guarantee.

CroPilot will notify the Customer without undue delay after becoming aware of a personal-data breach affecting Customer Personal Data. Available information will include the nature and likely consequences, affected data and people where known, mitigation and a contact point. Information may be supplied in phases. CroPilot will assist the Customer with its notification obligations; the Customer determines notifications to authorities and individuals.

5. Subprocessors

The Customer gives general written authorisation only for the subprocessors and processing described in the completed Schedule C. Before adding or replacing a subprocessor, CroPilot will notify the Customer through its designated account contact at least 30 days in advance and allow an objection on reasonable data-protection grounds. The parties will seek a workable alternative; if none is possible, the Customer may end the affected processing before the change takes effect.

CroPilot will impose equivalent data-protection obligations on each subprocessor and remains responsible to the Customer for their performance. A vendor shown as a candidate or awaiting confirmation is not authorised by this review draft.

6. International transfers

CroPilot will not transfer Customer Personal Data outside the EEA, including through remote access, without the Customer’s documented instructions and a valid Chapter V mechanism. Schedule C must identify locations and the applicable mechanism, such as a relevant adequacy decision or correctly executed Standard Contractual Clauses with the necessary assessment and supplementary measures.

This DPA does not itself execute Standard Contractual Clauses or certify that a provider arrangement has been checked. The applicable transfer arrangements must be completed before the affected processing begins.

7. Assistance, rights and audit

Taking account of the nature of processing and information available, CroPilot will assist the Customer with requests to access, correct, erase, restrict, export or object to processing, and with security, breach, impact-assessment and prior-consultation obligations under Articles 32–36. Requests received directly from an individual will be referred to the Customer unless law requires otherwise.

CroPilot will make information needed to demonstrate compliance with Article 28 available and allow and contribute to audits and inspections by the Customer or its mandated auditor. Reasonable arrangements may

protect other customers' confidentiality and service security but must not remove these rights. Any separately chargeable assistance must be agreed in advance.

8. Duration, return and deletion

This DPA lasts while CroPilot processes Customer Personal Data for the Customer. On termination, at the Customer's choice, CroPilot will return the personal data in an agreed commonly used format or delete it, and delete remaining copies, unless applicable law requires storage. The completed Schedule A must specify the operational return, active-system deletion and backup-expiry periods before acceptance is enabled.

Data awaiting deletion in protected backups remains subject to confidentiality and restricted processing; if restored, the deletion instruction must be reapplied. Any legally required retention must be identified and limited to that purpose. The Customer may request confirmation of completion.

Schedule A — Processing details

Subject and purpose: providing the Customer's enabled website optimization service, including permitted page observation, visitor measurement, supported recommendations, customer review, and separately authorised tests. No independent advertising or unrelated model training is included.

Nature: collection, transmission, organisation, storage, analysis, generation of proposals, retrieval, authorised disclosure, export and deletion as needed for the enabled services.

Data subjects: visitors to connected websites; Customer personnel and authorised users; where a commerce connection is enabled, customers represented in permitted order/conversion records.

Data categories: pseudonymous visitor/session and assignment identifiers; page URLs, interactions, device/browser metadata and timestamps; permitted page text/images and screenshots; configured conversion events and limited order references/amounts where enabled; authorised account/contact information. Data may still be personal even when direct identifiers are removed.

Duration and deletion schedule: REVIEW REQUIRED. Confirm the actual collection retention, active-system deletion, export delivery and backup-expiry periods for the enabled service. The review draft makes no unsupported promise of automatic deletion within a fixed number of days.

Schedule B — Technical and organisational measures

Application controls: authenticated team membership and role checks; separation of tenants; restrictions on support impersonation; documented decisions for collection and changes; bounded network collection and target validation; explicit enabled capability scope; data minimisation and secret-safe outputs.

Operational measures to confirm before publication: infrastructure locations, access-review practice, encryption-at-rest coverage, backup/restore availability, incident contacts and escalation, deletion operation and security review cadence. A control implemented in code is not proof that every deployment has been configured or independently audited.

Schedule C — Subprocessors and transfer arrangements

REVIEW REQUIRED. The final schedule must list each contracted processing entity, service, data categories, processing and remote-access locations, transfer mechanism and notification contact. The public subprocessor inventory is a review aid; it is not a substitute for the completed contractual schedule.

Current implementation inventory includes Render for application/database infrastructure and Google Gemini for enabled generation. Support, diagnostics, analytics and billing integrations must be classified by actual use and role before inclusion. No draft list grants new access or activates an integration.

Electronic acceptance and records

Acceptance requires an authenticated workspace owner who confirms authority to bind the named Customer. The record identifies the Customer, representative, workspace, accepted version and document digest, UTC timestamp and exact agreement text. It can be downloaded together with the accepted text. A later edit to the published agreement does not rewrite an earlier acceptance.

This review version is not open for binding acceptance. Publication requires the operator identity, schedules and operational commitments to be confirmed. Contact privacy@cropilot.ai for privacy or processing questions.