Data Processing Addendum

Scan Open Source Solutions S.L. (SCANOSS and Earnie) · Version 2.0 · Last updated 11 November 2026

This Data Processing Addendum ("**DPA**") forms part of the Terms of Service or other written agreement (the "**Terms**") between:

1. **Scan Open Source Solutions S.L.** ("**SCANOSS**"), a company registered in Spain with tax ID (NIF) B05462742 and registered office at Paseo de la Castellana 81, 15th floor, 28046 Madrid, Spain; and
2. the customer that has entered into the Terms with SCANOSS (the "**Customer**"),

each a "**Party**" and together the "**Parties**".

This DPA applies where, and only to the extent that, SCANOSS Processes Customer Personal Data on behalf of the Customer in providing the Services, including the SCANOSS platform and Earnie. It replaces any earlier data processing addendum between the Parties concerning the Services.

1. Definitions and interpretation

1.1 In this DPA:

- "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with a Party, where "control" means the power to direct the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.
- "**Customer Personal Data**" means Personal Data that SCANOSS Processes on behalf of the Customer under the Terms, as described in Annex 1.
- "**Data Protection Laws**" means all laws on data protection and privacy that apply to the Processing of Customer Personal Data, including: (a) Regulation (EU) 2016/679 (the "**GDPR**"); (b) Spanish Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights ("**LOPDGDD**"); (c) the GDPR as it forms part of UK law (the "**UK GDPR**") and the UK Data Protection Act 2018; (d) the Swiss Federal Act on Data Protection; and (e) any laws that amend, replace or supplement them.
- "**Data Privacy Framework**" means the EU-US Data Privacy Framework, together with the UK Extension and the Swiss-US Data Privacy Framework where applicable.
- "**Effective Date**" means the date on which the Customer accepts the Terms or, if later, the date on which the Customer accepts or signs this DPA.
- "**Restricted Transfer**" means a transfer of Customer Personal Data to a country outside the European Economic Area, the United Kingdom or Switzerland (as applicable) that is not subject to an adequacy decision or regulation under Data Protection Laws.
- "**SCCs**" means the standard contractual clauses approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as amended or replaced from time to time.
- "**Services**" means the products and services SCANOSS provides to the Customer under the Terms, including the SCANOSS platform and Earnie, and related support.
- "**Sub-processor**" means any third party engaged by SCANOSS to Process Customer Personal Data.

- "**UK Addendum**" means the International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018, as amended or replaced from time to time.

1.2 "Controller", "Processor", "Data Subject", "Personal Data", "Personal Data Breach", "Process" (and "Processing") and "Supervisory Authority" have the meanings given in the GDPR.

1.3 Capitalised terms not defined in this DPA have the meanings given in the Terms. Headings are for convenience only. "Including" means "including without limitation".

2. Scope, roles and duration

2.1 **Roles.** For Customer Personal Data, the Customer is the Controller (or a Processor acting for its own Controllers) and SCANOSS is the Processor (or Sub-processor, as applicable). Where the Customer acts as a Processor, it confirms that its Controller has authorised the instructions given and the appointment of SCANOSS.

2.2 **SCANOSS as Controller.** This DPA does not apply to Personal Data that SCANOSS Processes as an independent Controller, such as account administration, billing, sales and marketing contacts, and service analytics. SCANOSS's Privacy Policy, published at https://scanoss.com/privacy-policy/ and https://earnie.dev/privacy-policy, governs that Processing.

2.3 **Customer Affiliates.** Where Customer Affiliates use the Services, the Customer enters into this DPA on their behalf. The Customer is solely responsible for communicating with its Affiliates and any other relevant Controllers about this DPA, and remains the single point of contact for SCANOSS.

2.4 **Details of Processing.** Annex 1 sets out the subject matter, nature, purpose and duration of the Processing, and the types of Personal Data and categories of Data Subjects, as required by Article 28(3) GDPR.

2.5 **Duration.** This DPA takes effect on the Effective Date and continues for as long as SCANOSS Processes Customer Personal Data, even after the Terms end.

3. Customer obligations and instructions

3.1 **Compliance.** The Customer will comply with Data Protection Laws in its use of the Services. It is solely responsible for the lawfulness of the Customer Personal Data, including having a lawful basis and giving any notices required for its collection and transfer to SCANOSS.

3.2 **Instructions.** The Terms, this DPA and the Customer's configuration and use of the Services are the Customer's complete documented instructions to SCANOSS. Additional instructions must be in writing, consistent with the Terms, and agreed by SCANOSS. Any instruction requiring changes to the Services or extra cost will be handled through an agreed change process.

3.3 **Special categories.** The Customer will not submit to the Services any special categories of Personal Data under Article 9 GDPR, or Personal Data relating to criminal convictions and offences under Article 10 GDPR, unless agreed in writing.

4. SCANOSS obligations

4.1 **Processing on instructions.** SCANOSS will Process Customer Personal Data only on the Customer's documented instructions under section 3.2, including for transfers to third countries,

unless Union or Member State law requires otherwise. In that case SCANOSS will inform the Customer of the legal requirement before Processing, unless that law prohibits it.

4.2 **Infringing instructions.** SCANOSS will promptly inform the Customer if, in its opinion, an instruction infringes Data Protection Laws. SCANOSS may suspend the affected Processing until the instruction is confirmed or changed.

4.3 **No other use.** SCANOSS will not sell Customer Personal Data or use it for its own purposes, including marketing or advertising, or for training machine-learning models, except as needed to provide, secure and maintain the Services.

4.4 **Confidentiality.** SCANOSS will ensure that everyone authorised to Process Customer Personal Data is bound by a contractual or statutory duty of confidentiality, and has access only as needed to provide the Services.

4.5 **Security.** SCANOSS will implement and maintain appropriate technical and organisational measures under Article 32 GDPR, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing, and the risks to Data Subjects. These include at least the measures in Annex 2. SCANOSS may update those measures, provided the overall level of protection is not reduced.

4.6 **Disclosure requests.** If a public authority requests access to Customer Personal Data, SCANOSS will, unless legally prohibited: (a) redirect the authority to the Customer; (b) notify the Customer promptly, and where possible before disclosure; and (c) challenge requests it reasonably considers unlawful. SCANOSS will disclose only the minimum data legally required.

5. Sub-processors

5.1 **General authorisation.** The Customer gives SCANOSS general written authorisation to engage Sub-processors, including those listed in Annex 3.

5.2 **Conditions.** SCANOSS will: (a) impose on each Sub-processor, by written contract, data protection obligations that offer at least the same level of protection as this DPA; (b) carry out appropriate due diligence on each Sub-processor’s security and privacy practices; and (c) remain fully liable to the Customer for each Sub-processor’s performance of its obligations.

5.3 **Changes.** SCANOSS will notify the Customer at least 30 days before adding or replacing a Sub-processor, by email to the Customer’s account contact and by updating Annex 3 on its websites. The notice will state the Sub-processor’s name, location and processing activities.

5.4 **Objection.** The Customer may object on reasonable data protection grounds by writing to SCANOSS within 30 days of the notice. The Parties will then work together in good faith for up to 30 days to find a commercially reasonable alternative. If none is found, the Customer may terminate the affected Services on written notice, without penalty, and receive a pro-rata refund of any prepaid fees for the unused period.

6. Data subject rights and assistance

6.1 **Requests.** If SCANOSS receives a request from a Data Subject about Customer Personal Data, it will, where legally permitted, promptly forward it to the Customer and will not respond except to confirm that it has been passed on.

6.2 **Assistance with rights.** Taking into account the nature of the Processing, SCANOSS will assist the Customer by appropriate technical and organisational measures, as far as possible, to respond to requests to exercise Data Subject rights under Chapter III GDPR.

6.3 **Other assistance.** Taking into account the nature of the Processing and the information available to it, SCANOSS will provide reasonable assistance to the Customer with its obligations under Articles 32 to 36 GDPR, including data protection impact assessments and prior consultations with Supervisory Authorities.

6.4 **Regulator contact.** SCANOSS will, where legally permitted, promptly notify the Customer of any communication from a Supervisory Authority about Customer Personal Data.

6.5 **Costs.** Assistance under this section beyond what the Services' standard functionality provides may be charged at SCANOSS's then-current professional services rates, as agreed in advance.

7. Personal data breaches

7.1 **Notification.** SCANOSS will notify the Customer without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data.

7.2 **Content.** The notice will include, as far as then known: the nature of the breach, including the categories and approximate numbers of Data Subjects and records concerned; the likely consequences; the measures taken or proposed to address it and mitigate its effects; and a contact point for more information. SCANOSS will provide further information in phases as it becomes available.

7.3 **Response.** SCANOSS will promptly take reasonable steps to contain, investigate and remediate the breach, and will cooperate with the Customer so it can meet its own notification obligations to Supervisory Authorities and Data Subjects.

7.4 **No admission.** Notification of a breach is not an acknowledgement of fault or liability by SCANOSS.

8. International transfers

8.1 **Location.** SCANOSS Processes Customer Personal Data primarily in the European Economic Area. SCANOSS and its Sub-processors will make Restricted Transfers only in compliance with Chapter V GDPR and this section. In Earnie SaaS deployments, the Customer can choose the region of the knowledge base.

8.2 **Transfer mechanisms.** For each Restricted Transfer, SCANOSS will rely on one of the following, in this order: (a) an adequacy decision covering the recipient, including the Data Privacy Framework where the recipient is certified; or (b) the SCCs, together with any supplementary measures needed following a transfer impact assessment.

8.3 **SCCs between the Parties.** If a Restricted Transfer from the Customer to SCANOSS occurs and no other mechanism applies, the SCCs are incorporated into this DPA as follows: Module Two (Controller to Processor) or Module Three (Processor to Processor), as applicable; the optional docking clause in Clause 7 applies; Option 2 (general authorisation) applies in Clause 9, with the notice period in section 5.3; the optional wording in Clause 11 does not apply; Clauses 17 and 18 are governed by and subject to the courts of Spain; and Annexes I to III are completed by Annexes 1 to 3 of this DPA.

8.4 **UK and Swiss transfers.** For Restricted Transfers subject to the UK GDPR, the SCCs apply as amended by the UK Addendum, whose Tables 1 to 3 are completed by this DPA and whose Table 4 allows either Party to end the UK Addendum as set out in its Section 19. For transfers subject to Swiss law, the SCCs apply with references to the GDPR read as references to the Swiss Federal Act

on Data Protection and the competent authority being the Swiss Federal Data Protection and Information Commissioner.

8.5 **Change of mechanism.** If a transfer mechanism is invalidated or no longer applies, SCANOSS will promptly notify the Customer and will either implement an alternative lawful mechanism or, if that is not possible, suspend the affected transfer. If no alternative is available within a reasonable time, either Party may terminate the affected Services under section 5.4.

8.6 **Precedence.** If the SCCs conflict with this DPA or the Terms, the SCCs prevail.

9. Return and deletion

9.1 **On termination.** When the Terms end, SCANOSS will stop Processing Customer Personal Data, except as needed to carry out this section.

9.2 **Return or deletion.** At the Customer's choice, SCANOSS will return Customer Personal Data in a commonly used format, or delete it, within 30 days after termination. If the Customer makes no choice within that period, SCANOSS will delete it. Copies in backups will be deleted in line with SCANOSS's backup rotation, within 90 days.

9.3 **Legal retention.** SCANOSS may keep Customer Personal Data where Union or Member State law requires it, only for as long and to the extent required. Retained data remains subject to this DPA and the confidentiality obligations in the Terms, and will not be actively Processed.

9.4 **Certification.** On request, SCANOSS will confirm deletion in writing.

10. Audits and information

10.1 **Information.** SCANOSS will make available to the Customer all information reasonably necessary to demonstrate compliance with Article 28 GDPR and this DPA. This includes, on request and under confidentiality, its most recent third-party certifications or audit reports and completed security questionnaires.

10.2 **Audits.** If that information is not enough to demonstrate compliance, or a Supervisory Authority requires it, the Customer (or an independent auditor bound by confidentiality and not a SCANOSS competitor) may audit SCANOSS's relevant Processing. Audits are limited to once in any 12-month period, except after a Personal Data Breach or at a Supervisory Authority's request.

10.3 **Conduct.** The Customer will give at least 30 days' written notice and an audit plan. Audits will take place during business hours, without unreasonably disrupting SCANOSS's operations, and will not extend to other customers' data or SCANOSS's privileged or commercially sensitive information.

10.4 **Costs.** Each Party bears its own audit costs. SCANOSS may charge reasonable fees for time spent on audits beyond two business days per year. Audit rights of Sub-processors are exercised through SCANOSS's own audits and the reports SCANOSS obtains from them.

11. Liability, precedence and general terms

11.1 **Liability.** Each Party's liability arising out of or in connection with this DPA, whether in contract, tort or otherwise, is subject to the limitations and exclusions of liability in the Terms. Nothing in this DPA limits either Party's liability to Data Subjects under Article 82 GDPR, or any liability that cannot be limited by law.

11.2 **Precedence.** If this DPA conflicts with the Terms regarding the Processing of Customer Personal Data, this DPA prevails, except that the SCCs prevail under section 8.6.

11.3 **Changes.** SCANOSS may update this DPA to reflect changes in Data Protection Laws, Supervisory Authority guidance or the Services, provided the update does not materially reduce the protection given to Customer Personal Data. SCANOSS will give at least 30 days' notice of material changes.

11.4 **Severability.** If any provision of this DPA is held invalid or unenforceable, the rest of this DPA remains in effect, and the provision will be amended to the minimum extent needed to make it valid while preserving the Parties' intent.

11.5 **Governing law and jurisdiction.** This DPA is governed by the law that governs the Terms, unless Data Protection Laws or the SCCs require otherwise.

11.6 **Privacy contact.** Questions about this DPA, and requests to exercise Data Subject rights, can be sent to SCANOSS's privacy contact:

- Name: Julian Coccia
- Email: support@scanoss.com
- Post: Privacy, Scan Open Source Solutions S.L., Paseo de la Castellana 81, 15th floor, 28046 Madrid, Spain

Data Subjects may also lodge a complaint with the Spanish Data Protection Agency (Agencia Española de Protección de Datos, www.aepd.es) or their local Supervisory Authority.

Annex 1: Description of processing

Item	Details
Subject matter	Provision of the Services under the Terms: the SCANOSS platform (software composition analysis, open source and licence identification, software bill of materials (SBOM) generation), Earnie (software governance, including open source detection and snippet matching, AI model detection, cryptography detection, and SBOM, AIBOM and CBOM generation), and related support.
Duration	The term of the Terms, plus the return and deletion period in section 9.
Nature of Processing	Receiving, storing, analysing, comparing, transmitting and deleting data submitted by the Customer through the Services, APIs and support channels. The Services identify code by fingerprints (hashes), and SCANOSS never receives the Customer's source code. Earnie runs on the Customer's own infrastructure: in SaaS deployments only fingerprints are sent to the SCANOSS-hosted knowledge base, and in on-premise or air-gapped deployments SCANOSS receives no Customer data.
Purpose	To provide, secure, maintain and support the Services for the Customer.
Categories of Data Subjects	The Customer's authorised users (employees and contractors); the Customer's support contacts.
Types of Personal Data	User account details (name, business email, username, user ID); authentication and API key metadata; IP addresses and usage logs; support ticket content and correspondence.
Special categories	None. The Customer will not submit special categories of data (section 3.3).
Frequency of transfer	Continuous, for as long as the Customer uses the Services.
Retention	Customer Personal Data is kept for the term of the Terms and deleted under section 9. SCANOSS does not receive or store Customer source code.
Sub-processor Processing	As set out in Annex 3.
Competent Supervisory Authority	Agencia Española de Protección de Datos (AEPD), Spain.

Parties for the SCCs

- **Data exporter:** the Customer, as identified in the Terms. Role: Controller (or Processor). Contact: as given in the Customer's account.
- **Data importer:** Scan Open Source Solutions S.L., Paseo de la Castellana 81, 15th floor, 28046 Madrid, Spain. Role: Processor (or Sub-processor). Contact: Julian Coccia, privacy contact, support@scanoss.com.

Annex 2: Technical and organisational measures

SCANOSS maintains at least the following measures.

Area	Measures
Governance	Information security policy approved by management and reviewed regularly; designated privacy contact; ISO/IEC 27001 certification and SOC 2 Type II attestation, covering all Services, including Earnie.
Data minimisation	The Services identify code by fingerprints (hashes), and SCANOSS never receives the Customer's source code; collection is limited to the data needed for the Services.
Encryption	Data encrypted in transit and at rest using industry-standard methods; encryption keys managed securely.
Access control	Single-tenant Earnie deployments, isolated per Customer; role-based, least-privilege access; mandatory multi-factor authentication; access reviewed whenever roles or systems change, and revoked on leaving.
Confidentiality of staff	Confidentiality obligations in employment and contractor agreements; security and privacy training for staff.
Availability and resilience	Hosting with redundancy; regular backups, encrypted and tested; business continuity and disaster recovery plans.
Logging and monitoring	Logging of access and administrative actions on production systems; monitoring and alerting for security events.
Secure development	Code review before deployment; dependency and vulnerability scanning (including SCANOSS's own tools); separate development, test and production environments.
Vulnerability management	Regular patching; regular external penetration testing; remediation of findings according to severity.

Area	Measures
Incident response	Documented incident response procedure covering detection, escalation, containment, notification (section 7) and post-incident review.
Sub-processor management	Security and privacy due diligence before onboarding; written data protection terms; periodic review.
Testing and evaluation	Regular review of the effectiveness of these measures, with updates where risks change.

Annex 3: Authorised sub-processors

The Customer authorises the following Sub-processors, which apply to all Services, including Earnie.

Sub-processor	Purpose	Personal Data	Location	Transfer mechanism
OVH SAS	Server hosting for the Services, including the knowledge base and APIs that receive code fingerprints	Account and usage data, IP addresses	EU	Not applicable (EEA)
Hetzner Online GmbH	Server hosting for the Services, including the knowledge base and APIs that receive code fingerprints	Account and usage data, IP addresses	EU	Not applicable (EEA)
Microsoft Ireland Operations Limited (Microsoft 365)	Email and support communication, including support@scanoss.com	Customer contact details and correspondence	EU	Microsoft’s data protection terms, including the SCCs; Data Privacy Framework for any access by Microsoft Corporation
Pipedrive OÜ	Customer relationship management for account and support administration	Customer contact details, communication history	EU	Not applicable (EEA)