Schedule C — Data Processing Addendum

Version 1.0 · Effective 16 November 2026 · Last updated 16 November 2026 · Legal bundle DRIP-LEGAL-2026-11-16

ITEM	VALUE
Document	Schedule C to the DeRISK™ Intelligence Platform EULA — Data Processing Addendum ("DPA")
Version	1.0
Effective date	16 November 2026
Published at	denexus.ai/legal/dpa

This DPA forms part of the EULA, or of any MSA that incorporates it. It applies automatically when you accept the EULA; no separate signature is needed. A countersigned PDF is available on request from legal@denexus.ai. Capitalized terms not defined here have the meanings in the EULA or in applicable Data Protection Law.

1. Scope and roles

1.1 What this DPA covers. This DPA applies when DeNexus processes Customer Personal Data on your behalf in providing the Services. "Customer Personal Data" means personal data contained in Customer Data, Outputs or Processed Data. Examples include names and contact details in questionnaires, staff named in assessments, and identifiers in Active Directory exports or network data.

1.2 Roles. You are the controller of Customer Personal Data, and DeNexus is your processor. If you act as a processor for your own client, for example a broker submitting an insured's data, DeNexus is your sub-processor. You confirm that your client has authorized this.

1.3 What it does not cover. DeNexus is an independent controller for account data, usage data and Run Records, which it processes to operate, secure and improve the Services. Our privacy notice at denexus.ai/legal/privacy describes that processing.

1.4 Data Protection Law means all data protection laws that apply to the processing. This includes the EU GDPR, the UK GDPR and Data Protection Act 2018, the Swiss Federal Act on Data Protection, and US state privacy laws such as the California Consumer Privacy Act (CCPA).

2. Processing on your instructions

2.1 Your instructions. We process Customer Personal Data only on your documented instructions, unless the law requires otherwise, in which case we tell you first unless the law forbids it. Your instructions are:

- the EULA, including its retention rules by tier (EULA 7.5 to 7.7);
- your configuration and use of the Services, including the products and tier you choose;
- any further written instruction you give that is consistent with the EULA.

2.2 Purpose. We process Customer Personal Data only to provide the Services to you. We do not use it to train AI Models, sell it, or use it for any other customer (EULA 7.3 and 7.4). Building our document-reading capability uses document structure and formats only; personal data is excluded or anonymized before any such use.

2.3 Unlawful instructions. We will tell you if we believe an instruction breaches Data Protection Law. We may then suspend that processing until you confirm or change the instruction.

3. Confidentiality, security and personal data breaches

3.1 Personnel. Everyone we authorize to process Customer Personal Data is bound by confidentiality duties.

3.2 Security. We implement the technical and organizational measures in Annex II, appropriate to the risk. We may update them, but not in a way that materially lowers overall protection.

3.3 Breach notification. We will notify you without undue delay, and in any event within 48 hours (or any shorter period agreed in an MSA), after becoming aware of a personal data breach affecting Customer Personal Data. We will give you the information we have, then add to it as we learn more:

- what happened, and the categories and approximate number of data subjects and records affected;
- likely consequences;
- measures taken or proposed.

We will take reasonable steps to contain the breach. Notification is not an admission of fault.

4. Sub-processors

4.1 General authorization. You authorize us to use sub-processors of the types described in Annex III, as named in our current sub-processor list, and others added under this Section 4.

4.2 Their obligations. We impose data protection terms on each sub-processor that are at least as protective as this DPA. We remain liable for their performance.

4.3 Changes. We will give at least 30 days' notice before adding or replacing a sub-processor, by emailing your account administrator and updating the named sub-processor list. In an emergency, for example to keep the Services secure or available, notice may be shorter, and we will explain why.

4.4 Objection. You may object on reasonable data protection grounds within the notice period. We will try to find a solution. If we cannot, you may terminate the affected Services and receive a pro-rata refund of prepaid fees for them.

4.5 Named list. The current list of sub-processors, with each one's name, service and location, is available to customers on request from privacy@denexus.ai. It is DeNexus Confidential Information.

5. Assistance, information and audits

5.1 Data subject requests. If we receive a request from a data subject about Customer Personal Data, we will pass it to you and not answer it ourselves, unless the law requires. We will help you respond, taking into account the nature of the processing.

5.2 Impact assessments. We will give you reasonable information to help with data protection impact assessments and consultations with supervisory authorities.

5.3 Information. On request, we will give you the information reasonably needed to show compliance with this DPA. This includes our most recent independent security report or certification, where available, under confidentiality terms.

5.4 Audits. If that information is not enough to meet a legal or regulatory requirement, you may audit our compliance with this DPA. Audits require 30 days' written notice, take place at most once a year (unless a regulator requires more, or after a personal data breach), and are conducted during business hours by you or an independent auditor under confidentiality terms. You bear the audit's cost. Audits must not access other customers' data or compromise security.

6. Deletion and return

6.1 During the term. We delete Customer Personal Data in line with the retention rules for your tier (EULA 7.5). On Free Tiers it is deleted when each run completes. On Premium Tiers it is kept for 12 months on a rolling basis unless your Order Form says otherwise, or until you ask us to delete it.

6.2 At the end. After termination you have 30 days to export your data free of charge (EULA 7.7). We then delete Customer Personal Data, including Processed Data that contains it, and confirm deletion in writing on request. Backup copies are deleted within 35 days in the normal backup cycle.

6.3 Legal retention. If the law requires us to keep any Customer Personal Data longer, we keep only what is required, protect it under this DPA, and process it only for that purpose.

7. International transfers

7.1 Where data goes. DeNexus, Inc. is in the United States, and Customer Personal Data may be processed there. Non-US data residency is available as a priced option (EULA 9.5).

7.2 EU standard contractual clauses. For transfers from the EEA to DeNexus, the parties incorporate the standard contractual clauses in Commission Implementing Decision (EU)

2021/914 ("SCCs"), as follows:

SCC POINT	CHOICE
Module	Module 2 where you are a controller; Module 3 where you are a processor
Clause 7 (docking)	Applies
Clause 9(a) (sub-processors)	Option 2, general authorization, 30 days' notice (Section 4)
Clause 11 (redress)	Optional wording not used
Clause 13 (supervision)	The supervisory authority determined under Clause 13
Clauses 17 and 18 (law and courts)	Law and courts of Spain
Annexes I, II and III	Annexes I, II and III of this DPA

7.3 United Kingdom. For transfers from the UK, the ICO's International Data Transfer Addendum to the SCCs (version B1.0) applies. Its tables are completed with the information in this DPA, and either party may end it under its Section 19.

7.4 Switzerland. For transfers from Switzerland, the SCCs apply with these changes: references to the GDPR mean the Swiss Federal Act on Data Protection; the Swiss Federal Data Protection and Information Commissioner is the competent authority; and Swiss data subjects may sue in Switzerland.

7.5 Data Privacy Framework. DeNexus is not certified under the EU–US, UK or Swiss–US Data Privacy Framework. Transfers rely on the SCCs and the UK and Swiss provisions above.

7.6 Onward transfers. We put appropriate safeguards in place with sub-processors outside the EEA, UK or Switzerland.

8. US state privacy laws

Where the CCPA or a similar US state law applies, DeNexus acts as your service provider or processor. We will not:

- sell or share Customer Personal Data, as those terms are defined in that law;
- retain, use or disclose it for any purpose other than providing the Services, or outside our direct business relationship with you;
- combine it with personal data from other sources, except as the law permits.

We will tell you if we can no longer meet these obligations. You may then take reasonable steps to stop unauthorized use.

9. Your obligations as controller

You confirm that:

- you have a lawful basis, and have given any notices required, to submit Customer Personal Data to the Services. This includes data about your clients, insureds, applicants and their personnel;
- your instructions comply with Data Protection Law;
- you will not submit special categories of personal data, criminal-offence data, or data about children;
- you will submit only the personal data needed for your purpose, and remove it from documents where it is not needed.

10. Precedence, liability and term

10.1 Precedence. On the processing of personal data, this DPA prevails over the EULA and any MSA. The SCCs prevail over this DPA wherever they conflict.

10.2 Liability. Each party's liability under this DPA is subject to the limitations and exclusions in the EULA, or in your MSA, except where Data Protection Law or the SCCs do not allow it.

10.3 Term. This DPA applies for as long as DeNexus processes Customer Personal Data. It survives termination of the EULA until all Customer Personal Data has been deleted.

10.4 Changes. We may update this DPA under EULA Section 17, or where Data Protection Law or new standard contractual clauses require it. Updates will not lower the protection of Customer Personal Data.

Annex I — Processing details

ITEM	DETAILS
Data exporter	The Customer named at sign-up or in the Order Form; controller (or processor for its clients)
Data importer	DeNexus, Inc., 101 Federal Street, Suite 1900, Boston, MA 02110, USA; processor (or sub-processor). Contact: privacy@denexus.ai. Group establishments: DeNexus Tech. S.L., Calle Goya, 15, 28001 Madrid, España (EU); DeNexus UK Limited, 5 New Street Square, London EC4A 3TW, United Kingdom (UK)
Data subjects	Your employees and contractors; your clients, insureds and applicants, and their personnel; individuals named in documents, questionnaires or data you submit
Personal data	Names, job titles and business contact details; user and account identifiers (for example in Active Directory exports); device identifiers, hostnames and IP addresses in network data; any other personal data in documents you submit
Special categories	None. You must not submit them (Section 9)
Frequency	Continuous, for as long as you use the Services
Nature of processing	Hosting, storage, extraction and analysis by automated agents and AI Models, generation of reports, and deletion
Purpose	Providing the Services to you under the EULA

ITEM	DETAILS
Retention	Free Tiers: deleted when each run completes. Premium Tiers: 12 months on a rolling basis or as your Order Form states. Then deleted under Section 6
Sub-processors	Annex III

Annex II — Security measures

DeNexus applies the measures below. Schedule D (Security) describes them further; more detail is available under confidentiality terms.

AREA	MEASURES
Encryption	Data encrypted in transit and at rest
Segregation	Customer Data segregated by tenant; no cross-tenant access
Access control	Single sign-on support, least-privilege access for staff, access reviews, credentials kept secret
AI processing	AI Models process data in inference only and do not retain it; controls at the model boundary mask credentials and payment-card numbers, screen documents for prompt injection, and filter personal data from generated reports
Logging and monitoring	Security events logged and monitored; usage monitored for abuse
Deletion	Retention by tier and deletion under Section 6, including backups
Vulnerability management	Regular patching and vulnerability remediation
Incident response	Documented incident response, with breach notification under Section 3.3
Resilience	Backups and recovery procedures for the platform
Personnel	Confidentiality obligations, security training, and background checks where lawful
Sub-processors	Security due diligence and contractual data protection terms
Assurance	Independent audit reports available under confidentiality terms, as they become available

Annex III — Sub-processors

Types of sub-processors as of 16 November 2026. The named list is available to customers on request (Section 4.5). Changes follow Section 4.

SUB-PROCESSOR TYPE	SERVICE	LOCATION
Cloud infrastructure provider	Hosting, storage, backups and AI-model inference for the managed SaaS deployment. No AI processing takes place outside this provider's environment	United States; EU region where agreed for the engagement

No DeNexus affiliate processes Customer Personal Data: engineering, product and customer support are provided by DeNexus, Inc. from the United States. On-premise and private-cloud deployments run in the customer's own environment, with no DeNexus hosting sub-processor.

Questions about these terms: legal@denexus.ai · Current version: denexus.ai/legal