Data Processing Agreement

Anubion ApS — Azure Governance & Operations Platform

> *By completing the sign-up form on anubion.io and ticking the box to accept these terms, you enter into a legally binding data processing agreement with Anubion ApS. This Agreement applies alongside the Anubion Trial Terms of Service or, where applicable, the Anubion Master Service Agreement. Please read this Agreement carefully before signing up.*

1. Introduction and Scope

This Data Processing Agreement (the "Agreement") governs all data-related obligations between Anubion ApS ("Anubion") and the Customer in connection with the provision of the Anubion Azure governance and operations SaaS platform (the "Service"), whether during a free trial period or a paid subscription.

For the Customer acts as data controller and Anubion acts as data processor. This Agreement is required under Article 28 GDPR and forms part of the Anubion Trial Terms of Service or Master Service Agreement, as applicable.

This Agreement covers two categories of data: Personal data under GDPR (Part A) and infrastructure metadata and security posture data (Part B). In case of conflict, Part A prevails for personal data.

2. Acceptance

By completing sign-up on anubion.io and ticking the acceptance box, the Customer accepts this Agreement. The accepting individual warrants they have authority to bind the Customer. Anubion records the date, time, user details, Customer entity name and registration number, and version accepted.

Part A — Personal Data (GDPR)

3. Definitions

"Personal Data", "Data Controller", "Data Processor", "Processing", "Data Subject", and "Supervisory Authority" have the meanings given in Regulation (EU) 2016/679 (GDPR). "Sub-Processor" means any third party engaged by Anubion to process Personal Data on behalf of the Customer.

4. Scope of Personal Data Processed

Anubion processes two categories of personal data on behalf of the Customer:

- Login data: Name and email address of users who access the Service, collected directly at account creation or via Entra ID SSO.

Sensitivity: Confidential with personal data.

- Azure identity data: Usernames and Azure role assignments visible in the Customer's Azure environment, accessed via read-only service principal. This data is displayed in the platform but is not persistently stored by Anubion.

No sensitive personal data, CPR numbers, or special category data under Article 9 GDPR is processed.

5. Purpose and Legal Basis

Personal data is processed solely for the purpose of providing the Service — specifically, authenticating users, managing platform access, and displaying Azure identity and role information as part of the governance assessment. The legal basis for processing is the performance of this Agreement (Article 6(1)(b) GDPR).

6. Obligations of Anubion

Anubion shall:

- Process Personal Data only on documented instructions from the Customer as set out in this Agreement and any applicable data processing instructions.
- Immediately inform the Customer if, in Anubion's opinion, any instruction infringes GDPR or applicable data protection law. Anubion may suspend processing of that instruction pending clarification.
- Ensure that personnel authorised to process Personal Data are bound by confidentiality obligations.
- Implement appropriate technical and organisational security measures in accordance with Clause 13.
- Not transfer Personal Data outside the European Economic Area. All processing takes place exclusively within the EU. Should any future processing outside the EEA become necessary, Anubion shall first obtain the Customer's prior written consent and implement an appropriate transfer mechanism under Chapter V GDPR.
- Assist the Customer in responding to Data Subject requests under Articles 15-22 GDPR by providing relevant information within 5 business days of request.
- Assist the Customer with security obligations under Article 32, breach notification under Articles 33-34, and data protection impact assessments under Article 35.
- At the Customer's choice, delete or return all Personal Data upon termination and provide written confirmation of deletion.
- Make available all information necessary to demonstrate compliance with this Agreement and cooperate with audits and inspections in accordance with Clause 17.

7. Data Subject Rights

The Customer is responsible for responding to Data Subject requests. Where a Data Subject contacts Anubion directly, Anubion will forward the request to the Customer within 3 business days without responding itself.

8. Retention and Deletion of Personal Data During the Contract

During the active service period: login user data is retained for the duration of the active user account and deleted within 30 days of user removal. Azure identity data displayed in the platform is not persistently stored and requires no deletion routine.

Sensitivity: Confidential with personal data.

Upon trial expiry without conversion: all personal data is retained for 30 days following the Trial End Date to allow retrieval, then permanently and securely deleted. Written confirmation is provided within 7 days of deletion.

Upon termination of a paid subscription: all personal data is deleted within 30 days of the termination date. Written confirmation is provided within 7 days of deletion.

Access log data containing personal data is deleted after 90 days from the logged event.

9. Sub-Processors

The Customer provides general authorisation for Anubion to engage the sub-processors listed in Appendix A. Anubion shall inform the Customer of any intended changes to sub-processors with at least 30 days' notice. The Customer may object in writing within that period. If no objection is received, the change is deemed accepted. Anubion remains fully liable for sub-processor compliance.

10. International Transfers

All Personal Data is stored and processed exclusively within the European Union. No Personal Data is transferred to any country outside the EEA. Microsoft Azure infrastructure operates in EU regions only in connection with this Service. Should any future transfer outside the EEA become necessary, Anubion shall first notify the Customer, obtain prior written consent, and implement an appropriate transfer mechanism.

11. Illegal Instructions

If the Customer instructs Anubion to process Personal Data in a manner that Anubion reasonably believes would infringe GDPR or applicable data protection law, Anubion shall immediately notify the Customer in writing. Anubion may suspend the relevant processing pending written confirmation or modification of the instruction.

12. Purpose Limitation

Anubion processes Personal Data exclusively for the purposes set out in this Agreement. Anubion does not use Customer Personal Data for its own commercial purposes, for training AI or machine learning models, for marketing, or for any purpose other than providing the Service.

13. Security Measures

Anubion implements the following technical and organisational security measures:

- Encryption at rest: Azure SQL Transparent Data Encryption (TDE).
- Encryption in transit: TLS 1.2 minimum, HTTPS only.
- Access control: Role-based access via Microsoft Entra ID. Internal access to Customer data limited to named personnel with documented need.
- Multi-factor authentication: Enforced via Microsoft Entra ID.
- Privileged access: Logged via Azure PIM. All privileged access is time-limited and requires justification.
- Vulnerability management: Automated scanning in CI/CD pipeline on each deployment.
- Penetration testing: Conducted annually by an independent third party.

Sensitivity: Confidential with personal data.

- Backup: Azure SQL automated backups with 7-day retention and zone-redundant storage.
- Secrets management: Azure Key Vault.

Anubion does not hold ISO 27001, SOC 2 Type II, or ISAE 3000 certification at the date of this Agreement. Compliance is demonstrated through an annual written self-declaration covering security measures, incidents, and changes. Should Anubion obtain any such certification in future, it will be provided to the Customer.

14. Breach Notification

Anubion shall notify the Customer without undue delay and no later than 24 hours after becoming aware of a Personal Data breach. The notification shall include: a description of the breach, categories and approximate number of data subjects and records affected, likely consequences, and measures taken or proposed to address the breach.

15. Data Storage and Location

All Personal Data and Customer data is stored and processed exclusively within the European Union on Microsoft Azure infrastructure in West Europe (Netherlands) and/or North Europe (Ireland). No data is transferred to or stored in any country outside the EEA.

16. Supervision of Sub-Processors

Anubion shall ensure that sub-processors are bound by data protection obligations equivalent to those in this Agreement. Microsoft Azure, as the sole sub-processor, holds ISO 27001, SOC 2, and ISAE 3000 certifications. Annual compliance reports are available via the Microsoft Trust Center and shall be forwarded to the Customer upon request.

17. Audit Rights and Supervision

The Customer may request compliance documentation or conduct an audit with no less than 10 business days' prior written notice and reasonable cause. Anubion shall submit an annual written self-declaration within 30 days of each anniversary of this Agreement, confirming compliance with all obligations, any personal data breaches in the preceding 12 months, and any material changes to sub-processors or processing locations.

18. Insolvency

The Customer is designated as a beneficiary third party in any insolvency proceedings involving Anubion. In the event of insolvency, Anubion shall notify any appointed administrator of the Customer's ownership of and right to retrieve its data. The Customer's right to retrieve or have its data deleted survives insolvency. This clause survives termination of this Agreement.

19. Term

This Agreement is effective from the date of Customer's acceptance and remains in force for the duration of the applicable Trial Terms of Service or Master Service Agreement. It terminates automatically upon expiry or termination of the applicable agreement, subject to survival of confidentiality, deletion, and insolvency obligations.

Sensitivity: Confidential with personal data.

20. Order of Precedence

In the event of conflict between this Agreement and the applicable Trial Terms or Master Service Agreement on matters of data protection, this Agreement prevails. In the event of conflict between Part A and Part B for personal data, Part A prevails.

21. Record of Acceptance

This Agreement is accepted electronically via the sign-up form on anubion.io. No physical signature is required. The Customer should retain a copy of this Agreement in the version accepted at sign-up.

Part B — Customer Infrastructure Data

22. Scope

Part B governs the handling of infrastructure metadata, security posture data, and Azure configuration data that does not constitute Personal Data under GDPR. This includes Azure resource names, subscription structures, configuration states, security scores, and governance findings.

23. Data Ownership

All Customer infrastructure data belongs exclusively to the Customer. Anubion claims no ownership or licence rights in Customer data beyond what is necessary to provide the Service.

24. Confidentiality

Anubion treats all Customer infrastructure data as strictly confidential. Anubion shall not disclose Customer data to any third party except sub-processors engaged to provide the Service, and only to the extent necessary for that purpose.

25. Return and Deletion

Upon trial expiry without conversion, all Customer infrastructure data is retained for 30 days following the Trial End Date, then permanently deleted. Upon termination of a paid subscription, data is deleted within 30 days of the termination date. Written confirmation is provided in both cases.

26. Governing Law

This Agreement is governed by Danish law. Any disputes shall be subject to the exclusive jurisdiction of the courts of Copenhagen, Denmark.

Appendix A — Approved Sub-Processors and Processing Locations

Sensitivity: Confidential with personal data.

The following sub-processors are approved by the Customer upon acceptance of this Agreement:

Sub-processor	Role	Processing location	Transfer mechanism
Microsoft Azure (Microsoft Danmark ApS, CVR 31564895)	Cloud infrastructure, database hosting, and platform operations	EU only — West Europe (Netherlands) and/or North Europe (Ireland)	EU/EEA only. No third-country transfer. Microsoft DPA applies.

Section 2 — All Personal Data and Customer infrastructure data is processed and stored exclusively within the European Union. No data is transferred to or stored outside the EEA.

Sensitivity: Confidential with personal data.