Data Processing Agreement

Anubion ApS — Azure Governance & Operations Platform

> *By completing the signup form on anubion.io and ticking the box to accept these terms, you — on behalf of the company you represent — enter into a legally binding data processing agreement with Anubion ApS. This Agreement applies alongside the Anubion Master Service Agreement or Beta Terms of Service, depending on which service you have signed up for. Please read this Agreement carefully before accepting it. If you do not accept these terms, do not sign up for the service.*

1. Introduction and Scope

This Data Processing Agreement (the "Agreement") governs all data-related obligations between Anubion ApS ("Anubion", "we", "us", "our") and the Customer ("Customer", "you", "your") in connection with the provision of the Anubion Azure governance and operations SaaS platform (the "Service").

This Agreement is incorporated into, and forms part of, the Anubion Master Service Agreement or, where applicable, the Anubion Beta Terms of Service, and governs the processing of personal data and customer data as required under Article 28 GDPR and applicable Danish law.

This Agreement covers two distinct categories of data processed by Anubion:

- Personal data (as defined under GDPR) — governed by Part A of this Agreement.
- Infrastructure metadata and security posture data (commercially sensitive but not personal data under GDPR) — governed by Part B of this Agreement.

Both parts must be read together. In the event of conflict between Part A and Part B, Part A shall prevail in respect of personal data. All liability arising under this Agreement is subject to the caps and exclusions set out in the Master Service Agreement or Beta Terms of Service (as applicable).

2. Acceptance and Formation of Agreement

By completing the signup form at anubion.io and ticking the box indicating acceptance of this Agreement, the individual completing the form represents and warrants that:

- They are authorised to enter into legally binding agreements on behalf of the Customer.
- They have read and understood this Agreement.
- The Customer is a legal entity (private company) and not a private individual or public authority.

Upon submission of the signup form with the acceptance box ticked, a binding agreement is formed between Anubion ApS and the Customer. Anubion ApS records the date, time, submitting user, Customer legal entity name and registration number, and version of this Agreement accepted for documentation purposes.

For the purposes of this Agreement, the Customer acts as data controller and Anubion ApS acts as data processor.

3. Definitions

In this Agreement, the following definitions apply across both Part A and Part B:

- "Personal Data" means any information relating to an identified or identifiable natural person, as defined in Article 4(1) GDPR.
- "Customer Data" means all Azure infrastructure metadata, security posture data, compliance findings, and related information processed by the Provider on behalf of the Customer through the Service, excluding Personal Data which is addressed separately in Part A.
- "Processing" has the meaning given in Article 4(2) GDPR and, in the context of Part B, includes any collection, storage, use, analysis, or transmission of Customer Data.
- "Service" means the Provider's Azure governance and operations SaaS platform, which connects to the Customer's Microsoft Azure environment via a service principal to process infrastructure metadata and generate governance and security insights.
- "Service Principal" means the Azure Active Directory application registration installed by the Customer into their Azure environment to grant the Provider's platform read access.
- "Security Posture Data" means the Customer's security score, compliance findings, identified misconfigurations, policy violations, and governance recommendations generated by the Service.
- "Supervisory Authority" means the competent national data protection authority, including the Danish Data Protection Agency (Datatilsynet).
- "Sub-Processor" means any third party engaged by the Provider to process Personal Data or Customer Data on the Provider's behalf.

4. Description of the Service and Data Flows

The Service operates as follows:

- The Customer installs a Service Principal into their Microsoft Azure environment, granting the Provider's platform read-only access to Azure resource metadata.
- The platform collects and processes infrastructure metadata including subscription names, resource group names, resource names, resource tags, configuration states, and identity and access management data.
- This data is processed through the Provider's proprietary algorithm, which evaluates it against Microsoft best practice frameworks and the CIS (Center for Internet Security) benchmarks.
- The results — including Security Posture Data, governance recommendations, and compliance findings — are stored and displayed to the Customer through the Provider's portal.

The Provider does not access the Customer's Azure environment directly at any time. All processing is performed within the Provider's own platform based on data collected via the Service Principal.

PART A — Personal Data Processing Agreement (GDPR)

This Part A constitutes the data processing agreement required under Article 28 GDPR. It governs the processing of personal data by the Provider as data processor on behalf of the Customer as data controller.

5. Scope of Personal Data Processed

The Service processes the following limited categories of personal data, which arise incidentally in the course of processing Azure infrastructure metadata:

- Azure Active Directory / Entra ID user display names and user principal names (email addresses).
- Service principal names and identities.
- Names of resource owners where captured in Azure resource tags or metadata.

No special categories of personal data (Article 9 GDPR) are processed. The volume of personal data processed is limited and incidental to the primary purpose of processing infrastructure metadata.

6. Purpose and Legal Basis

Personal data is processed solely for the purpose of operating the Service — specifically to identify and display resource ownership, access permissions, and identity-related security findings within the Customer's Azure environment. The Provider shall not process personal data for any other purpose.

The Customer is the data controller and is responsible for ensuring it has a valid legal basis for making personal data available to the Provider via the Service.

7. Obligations of the Provider (GDPR)

In its capacity as data processor, the Provider shall:

- Process personal data only on documented instructions from the Customer and only as necessary to provide the Service. The Provider shall immediately inform the Customer if, in the Provider's opinion, any instruction infringes the GDPR or applicable data protection law, in accordance with Article 28(3)(h) GDPR. In such cases, the Provider is entitled to suspend processing of the relevant instruction until the Customer has confirmed or modified it.
- Ensure that all personnel with access to personal data are bound by enforceable confidentiality obligations.
- Implement appropriate technical and organisational security measures in accordance with Article 32 GDPR, as further detailed in Part B, Clause 14 of this Agreement.
- Not transfer personal data outside the European Economic Area. All processing takes place exclusively within the Denmark. Should any future processing outside Denmark become necessary, the Provider shall first obtain the Customer's prior written consent and implement an appropriate transfer mechanism under Chapter V GDPR.
- Assist the Customer in fulfilling its obligations to respond to Data Subject rights requests under Chapter III GDPR, including rights of access, rectification, erasure, restriction, portability, and objection.
- Assist the Customer in ensuring compliance with Articles 32–36 GDPR, including obligations relating to security, breach notification, and data protection impact assessments.

- Notify the Customer within 72 hours of becoming aware of a personal data breach affecting Customer personal data, in accordance with Clause 16 of this Agreement.
- Delete or return all personal data within 30 days of termination of the Service, at the Customer's election, and confirm deletion in writing.
- Make available to the Customer all information necessary to demonstrate compliance with this Part A and cooperate with audits as set out in Clause 18.

8. Data Subject Rights

The Provider shall promptly forward any Data Subject rights requests received directly to the Customer and shall not respond to such requests on the Customer's behalf without prior written authorisation. The Provider shall assist the Customer in responding to such requests within the timeframes required by GDPR, taking into account the nature of the processing and the information available to the Provider.

9. Retention and Deletion of Personal Data During the Contract

Personal data shall not be retained for longer than necessary for the purpose for which it is processed. The following retention periods apply during the active term of this Agreement:

- Azure AD user display names and user principal names (email addresses): retained for the duration of the Customer's active subscription. Deleted or anonymised within 30 days of the user being removed from the Customer's Azure environment or within 30 days of termination, whichever is earlier.
- Service principal names and identities: retained for the duration of the active subscription. Deleted within 30 days of the relevant service principal being decommissioned or upon termination.
- Access logs and audit trails containing personal data: retained for a maximum of 90 days from the date of the logged event, after which they are deleted or anonymised.

The Provider shall document and maintain records of deletion activities. The Customer may request confirmation of deletion of specific categories of personal data at any time. Upon termination, the obligations in Clause 23 apply.

10. Sub-Processors (Personal Data)

The Customer grants general written authorisation for the Provider to engage sub-processors to assist in delivering the Service. The Provider shall impose data protection obligations on all sub-processors that are no less protective than those set out in this Part A. The Provider remains fully liable to the Customer for any failure by a sub-processor to fulfil its obligations.

The named sub-processors approved at the date of this Agreement are set out in Appendix A to this Agreement. The Provider shall give no less than 30 days' written notice of any intended change to sub-processors. The Customer may object to such changes on reasonable data protection grounds within 14 days of notification.

11. International Transfers of Personal Data

Personal data shall not be transferred to a country outside the European Economic Area without the Customer's prior written consent and the implementation of an appropriate transfer mechanism in accordance with Chapter V GDPR.

All personal data processed in connection with the Service is stored and processed exclusively in Denmark. No personal data is transferred to a country outside the European

Economic Area. The Provider uses Microsoft Azure as its cloud infrastructure provider, operating exclusively within EU data centres. Microsoft Azure's processing in connection with the Service is subject to Microsoft's Data Protection Addendum, available at https://www.microsoft.com/en-us/licensing/product-licensing/products. The specific processing locations are set out in Appendix A to this Agreement.

In the event that any future sub-processor requires processing outside the EEA, the Provider shall notify the Customer in advance, obtain the Customer's prior written consent, and implement an appropriate transfer mechanism under Chapter V GDPR before any such transfer takes place. Details would be documented in an updated Appendix A.

PART B — Customer Data Processing & Confidentiality

This Part B governs the processing, storage, protection, and confidentiality of Customer Data — being Azure infrastructure metadata and Security Posture Data — which is commercially sensitive but does not constitute personal data under GDPR. The obligations in this Part B are contractual in nature and governed by Danish law.

12. Data Ownership

All Customer Data processed under this Agreement — including all infrastructure metadata, Security Posture Data, compliance findings, and any insights derived specifically from the Customer's environment — is and remains the sole property of the Customer. The Provider acquires no ownership, license, or proprietary interest in Customer Data as a result of providing the Service. The Provider's proprietary rights extend only to its algorithm, platform, and general methodologies, not to the Customer's data or Customer-specific outputs.

13. Purpose Limitation

The Provider shall process Customer Data exclusively for the purpose of operating, maintaining, and technically supporting the Service and generating governance and security recommendations for display to the Customer. The Provider shall not:

- Use Customer Data to train, calibrate, or improve its algorithm or any machine learning model using Customer-specific data without the Customer's prior written consent.
- Benchmark the Customer's environment against other customers.
- Share, sell, or disclose Customer Data or derived insights to any third party.
- Use Customer Data for any commercial or analytical purpose beyond direct service delivery.

14. Security Measures

The Provider shall implement and maintain appropriate technical and organisational measures to protect both Personal Data (Part A) and Customer Data (Part B) against unauthorised access, disclosure, alteration, loss, or destruction. These measures shall include, at minimum:

Encryption:

- Data at rest: Customer data is stored in Microsoft Azure. Azure SQL Database data is encrypted at rest using Transparent Data Encryption (TDE) in line with Microsoft's platform defaults.
- Data in transit: TLS 1.2 minimum for application and database endpoints; HTTPS-only for the web application; SQL connections use encryption.
- Scope: Encryption is provided at the database and managed service layer and on underlying encrypted storage, as described in Microsoft's documentation for the services in use.

Access Controls:

- Application access: Authenticated via Microsoft Entra ID; APIs require valid authorisation. MFA for users and operators is enforced by the Customer's Entra ID policies (e.g. Conditional Access), where configured.
- Provisioning and deprovisioning: Subject to the Provider's formal identity and access management process, covering onboarding, role assignment, and offboarding.
- Privileged access: Privileged access is logged via Entra ID, Azure, and PIM as applicable and reviewed regularly.

Infrastructure and Hosting:

- Cloud provider: Microsoft Azure.
- Certifications: Microsoft Azure maintains industry certifications and attestations. Details are available via the Microsoft Trust Center and the Customer's DPA with Microsoft.
- Controls: Network and identity controls per Azure deployment; least-privilege access to Azure resources; secrets managed in Azure Key Vault; TLS 1.2+ and HTTPS-only where applicable.

Vulnerability Management:

- Penetration testing: An internal penetration test is conducted annually, covering external endpoints, authentication and authorisation flows, and critical APIs.
- Vulnerability scanning: Application dependencies are scanned automatically in the CI/CD pipeline; infrastructure is monitored continuously; static code analysis is performed on every pull request; critical and high findings are escalated immediately.
- Patching: Underlying platform components are patched by Microsoft per their standard lifecycle policy. Application dependencies and internal releases are patched per the Provider's change management process.

Business Continuity:

- Backups: Production data is backed up via Azure SQL automated backups on the General Purpose tier, with a retention period of 7 days. Backups include full, differential, and transaction log backups, managed and zone-redundantly stored by Microsoft.
- Review cadence: Security measures are reviewed and updated at least annually and following any significant change to infrastructure or processing activities.

The Provider shall review and update security measures at least annually or following any significant change to its infrastructure. Documentation of security measures shall be made available to the Customer upon written request.

15. Support Access

The Provider's personnel do not have routine or standing access to Customer Data or Personal Data. The Provider does not access the Customer's Azure environment directly — all support is conducted within the Provider's own platform only.

Where access to Customer Data within the Provider's platform is required for support or troubleshooting, the following conditions apply:

- Access shall be carried out by named Provider personnel with the minimum access necessary for the specific task.
- Access shall be time-limited and revoked immediately upon completion of the support activity.
- All support access shall be logged, including the identity of the accessing personnel, time, duration, and reason for access.
- The Customer shall be notified prior to or promptly following any support access to their data.

The Customer may request a log of support access events at any time.

16. Breach and Incident Notification

This clause applies to breaches or incidents affecting both Personal Data (Part A) and Customer Data (Part B).

In the event of a security breach, unauthorised access, or any incident that results in or is reasonably likely to result in the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of Personal Data or Customer Data, the Provider shall:

- Notify the Customer without undue delay and in any event within 72 hours of the Provider becoming aware of the incident.
- Provide in the initial notification, or as soon as practicable thereafter: the nature of the incident; the categories and approximate volume of data affected; the likely consequences; and the measures taken or proposed to address the incident and mitigate its effects.
- Keep the Customer informed of all material developments until the incident is fully resolved.
- Cooperate fully with the Customer in any investigation, regulatory notification, or remediation efforts.

For incidents involving Personal Data, the 72-hour notification period aligns with the Customer's obligations to notify the Supervisory Authority under Article 33 GDPR. The Provider shall provide sufficient information to enable the Customer to meet its regulatory notification obligations.

The Provider shall maintain an internal incident response procedure, a summary of which shall be made available to the Customer upon request.

17. Data Storage and Location

All Personal Data and Customer Data processed under this Agreement is stored and processed exclusively in Denmark. All data is hosted on Microsoft Azure infrastructure

located within the EU, primarily in Denmark East. No Personal Data or Customer Data is transferred to, processed in, or stored in any country outside the European Economic Area.

The Provider shall give no less than 30 days' written notice of any proposed change to data storage location or hosting provider.

18. Audit Rights and Supervision

The Customer has the right to supervise the Provider's compliance with both Part A and Part B of this Agreement. The Parties agree to the following supervision methodology as the default approach:

- Annual written self-declaration: The Provider shall submit an annual written statement to the Customer confirming compliance with the obligations in this Agreement, including the security measures in Clause 14, any personal data breaches in the preceding 12 months, and any material changes to sub-processors or processing locations. At the date of this Agreement, the Provider does not hold formal third-party security certifications (such as ISO 27001, SOC 2 Type II, or ISAE 3000). Compliance is therefore demonstrated through this annual self-declaration. Should the Provider obtain any such certification in the future, it will be provided to the Customer and may supplement or replace the self-declaration as evidence of compliance.
- Ad hoc audit: The Customer may, on reasonable prior written notice of no less than 10 business days, request additional documentation or conduct an inspection to verify compliance where there is specific reasonable cause to do so. Any such audit shall be conducted at the Customer's cost, during normal business hours, and subject to a confidentiality obligation.

The Provider shall cooperate fully with all supervision activities. The annual self-declaration or certification shall be provided by the Provider no later than 30 days after the anniversary of this Agreement each year.

19. Security Score and Sensitive Findings

The Provider acknowledges that the Customer's Security Posture Data represents a detailed and sensitive picture of the Customer's security vulnerabilities. In addition to the general measures in Clause 14, the Provider shall:

- Restrict internal access to Security Posture Data to personnel with a documented operational need.
- Not reference a Customer's security score or findings in any external communication, marketing, or benchmarking without the Customer's prior written consent.
- Apply the same deletion obligations to Security Posture Data as to all other Customer Data upon termination.

20. Sub-Processors and Third Parties (Customer Data)

The Provider may engage third-party sub-processors (such as cloud infrastructure providers) to assist in delivering the Service. The Provider shall impose confidentiality and security obligations on all sub-processors equivalent to those set out in this Part B. A current list shall be provided to the Customer upon written request, and no less than 30 days' notice shall be given of any changes.

21. Confidentiality

The Provider shall treat all Personal Data and Customer Data as strictly confidential and shall limit access to personnel who require it to deliver the Service. All such personnel shall be bound by enforceable confidentiality obligations. This confidentiality obligation survives termination of this Agreement for a period of five (5) years.

22. Customer Obligations

The Customer is responsible for:

- Installing and maintaining the Service Principal in its Azure environment with appropriate permissions, and revoking it upon termination of the Service.
- Ensuring that Authorised Users of the portal are aware of and comply with applicable confidentiality obligations in respect of data visible in the portal.
- Notifying the Provider promptly of any suspected unauthorised access to the Customer's portal account.
- Ensuring it has a valid legal basis for making personal data available to the Provider via the Service.

23. Return and Deletion of Data

Upon expiry or termination of the applicable Master Service Agreement or Beta Terms of Service, Anubion shall, within 30 days of the termination date and at the Customer's written election:

- Export and return all Personal Data and Customer Data in a structured, commonly used, machine-readable format; or
- Securely delete all Personal Data and Customer Data and provide written confirmation that deletion has been completed.

Deletion from backup systems shall occur within the applicable backup retention schedule. The Provider shall confirm this to the Customer in writing.

24. Liability

The Provider shall only be liable for loss or damage to Personal Data or Customer Data that is directly caused by the Provider's gross negligence, wilful misconduct, or material failure to comply with the obligations set out in this Agreement. The Provider shall not be liable for loss or damage that arises despite the Provider having properly implemented and maintained the security and operational measures required under this Agreement.

All liability under this Agreement is subject to the liability caps and exclusions set out in the applicable Master Service Agreement or Beta Terms of Service. For the avoidance of doubt, Anubion is not liable for the Customer's own failure to configure the Service Principal appropriately or to manage Authorised User access securely.

25. Insolvency and Business Continuity

In the event that the Provider becomes insolvent, enters administration, receivership, or any other form of insolvency proceedings, or ceases to carry on business, the Customer is hereby designated as a beneficiary third party with respect to all Personal Data and Customer Data held by the Provider at the time of such event.

The Provider undertakes to ensure that any insolvency practitioner, administrator, or successor entity appointed in connection with such proceedings is made aware of: (a) the Customer's ownership of Customer Data; (b) the Provider's obligations to return or delete

such data under this Agreement; and (c) the Customer's right to access and retrieve its data as a priority matter.

The Provider shall, to the extent reasonably practicable, give the Customer advance written notice if it anticipates entering insolvency proceedings, and shall take all reasonable steps to facilitate the secure return or transfer of Personal Data and Customer Data to the Customer prior to any such event.

This clause shall survive termination or expiry of this Agreement.

26. Term

This Agreement is effective from the date of Customer's acceptance and remains in force for the duration of the applicable Master Service Agreement or Beta Terms of Service. It terminates automatically upon expiry or termination of the applicable agreement, subject to survival of the confidentiality obligations set out in Clause 21, the deletion obligations set out in Clause 23, and the insolvency provisions set out in Clause 25.

27. Governing Law and Jurisdiction

This Agreement is governed by Danish law. Any disputes arising from or in connection with this Agreement shall be subject to the exclusive jurisdiction of the courts of Denmark. Where this Agreement overlaps with GDPR obligations, the applicable provisions of GDPR shall take precedence over Danish law to the extent required.

28. Order of Precedence

In the event of conflict between this Agreement and the applicable Master Service Agreement or Beta Terms of Service on matters of data protection or data handling, this Agreement shall prevail. In the event of conflict between Part A and Part B of this Agreement in respect of personal data, Part A shall prevail.

29. Record of Acceptance

This Agreement is accepted electronically via the signup form on anubion.io. No physical signature is required. By ticking the acceptance box and submitting the signup form, the Customer agrees to be bound by the terms of this Data Processing Agreement, including both Part A (GDPR), Part B (Customer Data Confidentiality), and Appendix A (Approved Sub-Processors and Processing Locations).

Upon acceptance, Anubion ApS records the following information for documentation purposes:

- Date and time of acceptance (UTC).
- Full name and email address of the submitting user.
- Customer legal entity name and registration number.
- Version of this Agreement accepted (as shown in the document footer).

A copy of this acceptance record is available to the Customer upon written request to Anubion ApS. The Customer should retain a copy of this Agreement in the version accepted at the time of signup for their own records.

Appendix A — Approved Sub-Processors and Processing Locations

This Appendix A forms part of the Data Processing Agreement between Anubion ApS and the Customer. It sets out the sub-processors approved by the Customer upon acceptance of this Agreement, together with the locations where personal data is processed. This Appendix shall be updated by Anubion in accordance with the notification obligations in Clauses 10 and 11 of this Agreement.

Section 1 — Approved sub-processors

Sub-processor	Role	Processing location	Transfer mechanism
Microsoft Azure	Cloud infrastructure, database, and storage	European Union	EU/EEA only. No third-country transfer. Microsoft DPA applies.
[Additional sub-processor]			

Section 2 — Processing locations

All personal data and Customer Data is processed and stored exclusively within Denmark. Processing takes place on Microsoft Azure infrastructure in Denmark East. No personal data is transferred to or stored in any country outside the EEA.

Section 3 — Updates to this Appendix

The Provider shall update this Appendix A when sub-processors are added or removed, giving no less than 30 days' written notice to the Customer. An updated version of this Appendix, acknowledged by both Parties in writing, shall replace the previous version and form part of the Agreement. Where the Customer does not object within 14 days of notification, the update is deemed accepted.