DATA PROCESSING AGREEMENT

Data Processing Agreement ("**DPA**") forming part of the Agreement between Borg Security AS ("**Borg**") and the Customer governing Borg's Processing of Personal Data on behalf of the Customer in connection with the Services.

1. DEFINITIONS

1.1 Definitions used in this Agreement shall be construed in the same way as in the Prevailing Data Protection Legislation. In addition to definitions elsewhere in this Agreement, the following definitions shall apply:

Data Processing Agreement/DPA	means this Data Processing Agreement on the Processing of Personal Data on behalf of the Customer.
Master Service Agreement	Master Service Agreement means the Agreement as defined in the Master Service Agreement governing the provision of the Services between Borg Security AS and the Customer, including these general terms, any applicable Ordering Document, Service Appendices, this DPA, and the Documentation.
Prevailing Data Protection Legislation	means the GDPR, the Norwegian Personal Data Act, the UK GDPR to the extent applicable, and any other privacy or data protection laws applicable to Borg's Processing of Customer Personal Data under the Agreement.
GDPR	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such Data, and repealing Directive 95/46/EC.
Personal Data	means any information relating to an identified or identifiable natural person, as defined in the Prevailing Data Protection Legislation, including Personal Data contained in Customer Data.
Services	means the services provided by Borg Security AS as described in the Master Service Agreement, including the Odin platform, the AI penetration testing agent Mjolnir, asset discovery tools (Huginn and Muninn), and related support or embedded research services, as applicable.
Process/Processing	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, including Processing carried out by Automated Processing Systems.
Sub-processor	means a third party engaged by Borg to Process Personal Data on behalf of the Customer in connection with the Services.
Customer Data	means any data, content, code, systems, environments, repositories, logs, findings, inputs, credentials, configurations, or other information made available by or on behalf of the Customer to Borg in connection with the Services, including data accessed through integrations or testing activities, and including Customer Content as defined in the Master Service Agreement.
Customer Personal Data	means any Personal Data forming part of Customer Data and processed by Borg on behalf of the Customer in connection with the Services.
Restricted Transfer	means a transfer of Customer Personal Data to a country or recipient that requires an approved transfer mechanism under Applicable Data Protection Law.
Automated Processing Systems	means Borg's automated systems, including artificial intelligence models, AI agents, and related tools (including Mjolnir), used to perform analysis, testing, and Processing of Customer Data, including Processing carried out without human intervention or review, as further described in Annex A (A.2(ii)).

All other non-defined terms, including but not limited to "Controller", "Processor" and "Personal Data Breach", shall have the same meaning as in the Prevailing Data Protection Legislation.

2. BACKGROUND AND PURPOSE

2.1 This DPA sets out the rights and obligations of the Data Controller ("**Customer**") and the Data Processor ("**Borg**") with respect to Borg's Processing of Personal Data on behalf of the Customer in connection with the Services. This DPA has been designed to ensure the Parties' compliance with Article 28(3) of the GDPR. Borg does not represent or warrant compliance with data protection laws of jurisdictions outside the EU/EEA, except to the extent such compliance is explicitly required under applicable EU or Norwegian law.

2.2 The Parties acknowledge that the Services involve automated and potentially extensive analysis of Customer systems and environments, including access to Personal Data by Automated Processing Systems without human review. Such Processing may occur in accordance with the categories described in Annex A, including Processing performed solely by Automated Processing Systems without access to Personal Data in an intelligible form.

2.3 This DPA, including its Annexes, forms part of the Agreement as described in the Master Service Agreement. The Annexes set out further details of the Processing and use of Sub-Processors:

- Annex A contains a reference link to detailed information on the processing of Personal Data, including the purpose and nature of the processing, type of Personal Data, categories of data subjects and duration of the processing.
- Annex B contains a reference to the list of autorised Sub-processors maintained by Borg.

2.4 In the event of a conflict between this DPA and the other parts of the Agreement, this DPA shall prevail with respect to the Processing of Personal Data.

2.5 Borg reserves the right to update and amend this DPA, including its Annexes, from time to time. The applicable version will be made available on Borg's website. Where changes materially affect the Processing of Personal Data or the Customer's rights and obligations under this DPA, Borg shall notify the Customer by reasonable means (including email or in-product notification) at least thirty (30) days prior to such changes taking effect. Updates to Sub-Processors shall be notified in accordance with Section 7.4.

2.6 Borg may process Personal Data as an independent data controller where such processing is necessary for its own legitimate business purposes, including security, abuse prevention, fraud detection, service integrity, billing, legal compliance, and operation of its business. Such processing shall be outside the scope of this DPA.

3. THE RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

3.1 The Customer is solely responsible for ensuring that the Processing of Personal Data under the Agreement, including any instructions to Borg and its use of the Services, complies with all Prevailing Data Protection Legislation binding on the Customer. The Customer is further solely responsible for identifying and complying with any privacy or data protection laws outside Norway and the EEA that may apply to the Customer, its business, its users, its systems, or its environments, except to the extent Borg has expressly agreed in writing to comply with such laws in connection with the Services.

3.2 The Customer shall determine the purposes and means of the Processing and is responsible for ensuring that the Processing is lawful, including that a valid legal basis exists in accordance with applicable data protection law, cf. GDPR Article 24. The Customer is also solely responsible for determining whether any non-Norwegian or non-EEA privacy or data protection requirements apply to the Customer's use of the Services or to the Personal Data made available through the Services.

3.3 The Customer is responsible for determining whether the Services are appropriate for the Personal Data made available, taking into account the nature of the Services, including automated Processing and potential access to systems, environments, and data across multiple locations and jurisdictions.

3.4 The Customer acknowledges that the Services may involve access to Personal Data across multiple systems, environments, and jurisdictions, including through automated systems without human review, and represents and warrants that it has all necessary rights, permissions, and legal bases to disclose such Personal Data to Borg and to authorize the Processing under this DPA.

4. THE RIGHTS AND OBLIGATIONS OF THE DATA PROCESSOR

4.1 **Instructions.** Borg is subject to the Customer´s authority regarding the processing of Personal Data and shall only process Personal Data based on documented instructions from the Customer. Customer acknowledges that its configuration of the Services, including asset selection, integrations, and test execution, constitutes documented instructions to Borg. Subsequent instructions may also be given by the Customer throughout the duration of the processing of Personal Data. These instructions shall always be documented. If Borg means that an instruction from the Customer is in breach of the Prevailing Data Protection Legislation or any other legislation, Borg shall immediately notify the Customer about this. To the extent that additional requirements apply under non-EEA data protection laws, the Customer shall provide documented instructions to Borg, and Borg shall only be obliged to implement such requirements to the extent they are technically feasible, proportionate, and agreed in writing between the Parties.

4.2 **Confidentiality.** Borg shall ensure that access to Personal Data is limited to authorized personnel and Automated Processing Systems strictly as necessary to provide the Services. The Parties acknowledge that Borg's Automated Processing Systems may access and analyze Personal Data as part of the Services without such data being reviewed by Borg personnel. Processing carried out solely by Automated Processing Systems may occur without Personal Data being made available to Borg personnel in an intelligible form, as described in Annex A.

4.3 **Security measures.** Borg confirms that it will take appropriate technical and organizational measures to ensure that all processing of Personal Data under this DPA meets the requirements of the Prevailing Data Protection Legislation, including compliance with all the requirements of GDPR article 32. Borg will implement technical and organizational measures which can be disclosed on Customer's reasonable request (as may be amended from time to time). Processing performed by Automated Processing Systems shall be subject to the same security requirements as Processing performed by personnel.

4.4 **Audit.** Borg shall make available to the Customer information reasonably necessary to demonstrate compliance with this DPA. Audits shall be subject to reasonable prior notice, confidentiality obligations, and may be satisfied through provision of audit reports, certifications, or other documentation. On-site audits shall only be permitted where required by applicable law and subject to agreement between the Parties.

4.5 **Assistance according to GDPR articles 32-36.** Borg is obliged to provide the Customer with access to relevant data security documentation, and shall, to the extent reasonably possible, assist the Customer with fulfilling its own responsibility in accordance with the Prevailing Data Protection Legislation. Borg shall have no obligation to access, retrieve, or otherwise make available Personal Data where such access would require actions outside the scope of the Services, beyond the Customer's documented instructions, or would require disproportionate effort. This limitation applies in particular to Processing performed solely by Automated Processing Systems where Personal Data is not available to Borg in an intelligible form.

4.6 **Assistance with inquiries.** Borg shall, to the extent reasonably possible, assist the Customer in fulfilling its obligations towards data subjects under the Prevailing Data Protection Legislation, including by providing relevant information on the Processing and supporting responses to requests from data subject regarding their rights after GDPR chapter III. Such assistance shall take into account the nature of the Services and Borg's actual level of access to Personal Data. Where Processing is carried out by automated systems without human access, including Processing described in Annex A (A.2(ii)) where Personal Data is not available in an intelligible form to Borg, Borg shall provide available technical information, but shall have no obligation to access or retrieve Personal Data beyond the scope of the Services or the Customer's documented instructions. Borg shall promptly forward any data subject requests it receives to the Customer.

4.7 **Other type of assistance.** Borg shall, to the extent reasonably possible and taking into account the nature of the Services and Borg's actual level of access to Personal Data, provide reasonable assistance to the Customer in relation to its compliance obligations under the Prevailing Data Protection Legislation, to the extent not already covered by Sections 4.5–4.6.

4.8 **Compensation for assistance.** Borg shall be entitled to reasonable compensation for assistance provided under Sections 4.5–4.7 and Section 5, and any other assistance requested by the Customer under this DPA or applicable law, unless otherwise expressly agreed. Such compensation shall be based on time spent in accordance with Borg's then-current rates, or as otherwise agreed between the Parties.

4.9 **Disclosure.** Borg may transfer Personal Data to authorized Sub-processors and Affiliates in accordance with Annex B. Any international transfers shall be carried out in accordance with Section 6 and Chapter V of the GDPR. Borg shall not disclose Personal Data to third parties except on documented instructions from the Customer or as required by applicable law.

4.10 **Data Access.** The Customer acknowledges that, in order to provide the Services, Borg may access, analyze, and otherwise Process Personal Data contained in Customer systems, environments, repositories, and data sources, including through automated systems and, where necessary, with broad system-level access. Access by Borg personnel to Personal Data in intelligible form shall be limited to what is necessary for (i) support, troubleshooting, security, abuse prevention, audit, legal compliance, or defense of claims, (ii) human-led Professional Services expressly requested by the Customer, or (iii) situations where the Customer has given explicit consent. Processing performed solely by Automated Processing Systems may occur without Personal Data being extracted, stored, or otherwise made available to Borg in an intelligible form, and without access by Borg personnel. Borg shall not combine Customer Personal Data with personal data from other customers except as necessary to provide the Services or as permitted by applicable law.

4.11 **CCPA**. This Section 4.11 applies only to the extent that Personal Data includes personal information subject to the CCPA and supplements the other provisions of this DPA. Borg processes such Personal Data on behalf of the Customer for the business purposes set out in the Master Service Agreement. Borg shall not retain, use, or disclose such Personal Data for any purpose other than to perform the Services or as otherwise permitted by applicable law, including outside the direct business relationship between the parties. Borg shall not sell or share Personal Data within the meaning of the CCPA.

5. SECURITY AND BREACH

5.1 Borg shall implement and maintain appropriate technical and organizational measures in accordance with the Prevailing Data Protection Legislation, taking into account the nature of the Services, including automated and system-level Processing, the sensitivity of the Personal Data, and the risks to data subjects. Borg shall perform and maintain relevant risk assessments as part of its security framework. Borg shall be able to document such measures.

5.2 Borg shall notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data within Borg's systems or under Borg's control. Such notification shall include relevant information required under GDPR Article 33(3), to the extent available. For the avoidance of doubt, Processing carried out by Borg in accordance with this DPA shall not be considered unauthorized access or a Personal Data Breach. The Customer is responsible for ensuring that the scope of this DPA and the Services covers the categories of Personal Data made available to Borg. This includes ensuring that Personal Data processed through Automated Processing Systems as described in Annex A is within scope and lawfully disclosed.

5.3 The Customer is responsible for notifying the relevant supervisory authority. Borg shall not notify any supervisory authority without the Customer's prior instructions, unless required by applicable law. Borg shall, to the extent reasonably possible, assist the Customer in meeting its notification obligations, taking into account the nature of the Services and Borg's actual level of access to Personal Data

5.4 Borg shall maintain records of Personal Data Breaches and security incidents, including relevant facts, effects, and remedial actions.

5.5 Borg shall, without undue delay, take appropriate measures to mitigate and remediate Personal Data Breaches or security non-conformities for which Borg or its Sub-Processors are responsible. Such measures shall be documented. To the extent required under the DPA, such remediation shall be carried out at no additional cost to the Customer.

6. TRANSFER OF PERSONAL DATA OUTSIDE EU/EEA

6.1 Borg may transfer Personal Data to Sub-processors or Affiliates in third countries as necessary to provide the Services, including to infrastructure, analytics, and AI service providers. The Customer acknowledges and instructs such transfers as part of its use of the Services. All such transfers shall be carried out in accordance with Chapter V of the GDPR and based on a valid transfer mechanism.

6.2 Where Borg is required under applicable EU or Norwegian law to transfer Personal Data to Sub-processors in a third country or international organization, Borg shall inform the Customer of such legal requirement prior to the transfer, unless such notification is prohibited by law.

6.3 The sections in this DPA are not to be confused with the standard contractual clauses as mentioned in GDPR article 46 (2), and this DPA does not by itself ensure compliance with obligations related to international transfers in accordance with Chapter V of the GDPR. Where required, the parties shall enter into or rely on applicable Standard Contractual Clauses and related transfer mechanisms to legitimize Restricted Transfers.

7. SUBPROCESSORS

7.1 The Customer acknowledges and agrees that Borg has a general authorisation to engage Sub-Processors to support the provision of the Services. Borg maintains an up-to-date list of Sub-processors at the location referenced in Annex B, which may be updated from time to time.

7.2 Borg shall ensure that any engagement of a Sub-Processor complies with the requirements of GDPR Article 28(2) and (4), including by entering into a written agreement imposing data protection obligations no less protective than those set out in this DPA

7.3 At least ten (10) days before enabling any new Sub-Processors, Borg shall notify the Customer of the intended changes and add the new Sub-Processor to the list referenced in Annex B. The Customer may object to such an engagement by informing Borg within this ten (10) day period, provided such objection is in writing and based on reasonable grounds relating to data protection. If the Customer does not object to the changes in writing within the ten (10) day period, the Customer shall be deemed to have accepted the changes.

7.4 Borg shall, upon reasonable written request, make available information reasonably necessary to demonstrate that its Sub-Processors are bound by written obligations materially no less protective than those set out in this DPA. Borg shall not be required to disclose full copies of Sub-Processing agreements except to the extent required by applicable law, and may redact such information to protect trade secrets, security information, and confidential information of Borg or third parties. Borg shall remain responsible for the performance of its Sub-processors to the extent required under the Prevailing Data Protection Legislation. The Customer may require Borg to suspend the use of a Sub-Processor where the Customer has documented and reasonably substantiated that the Sub-Processor is in material breach of its contractual obligations or the Prevailing Data Protection Legislation.

7.5 Upon termination of this DPA, Borg shall ensure that the Sub-Processors fulfill, in the same manner as Borg, the obligation to delete or properly destroy Personal Data in accordance with Section 8.1. This obligation shall not apply to Personal Data retained in backup systems, provided that such data is securely isolated, protected in accordance with this DPA, and deleted or overwritten in the ordinary course of Borg's or the Sub-Processor's backup retention policies.

8. ERASURE AND RETURN OF DATA

8.1 Upon termination or expiration of the Service Agreement, Borg shall, at the Customer's choice and unless otherwise required by applicable EU or Norwegian law, delete or return Personal Data processed on behalf of the Customer and under Borg's control. Borg shall, upon request, confirm that such deletion or return has been completed.

8.2 The foregoing obligation applies to Personal Data stored or otherwise retained by Borg as part of the Services. Borg shall not be required to delete or return Personal Data that remains solely within the Customer's own systems, environments, or data sources.

8.3 Borg may retain Personal Data where required by applicable law or as necessary for legitimate purposes such as, but not limited to, security, audit, fraud prevention, dispute handling, or compliance obligations, provided that such data is retained only to the extent and for the duration necessary and remains protected in accordance with this DPA. Borg may also retain de-identified or aggregated data that does not identify the Customer or any data subject. For clarity, logs, audit records, security telemetry, incident records, and similar technical records generated by Borg in connection with the Services may be retained for the purposes described in Section 8.3 even where they contain or may reflect Customer Personal Data, provided such retention is limited to what is reasonably necessary for those purposes.

8.4 Personal Data retained in backup systems shall be exempt from the deletion obligations above, provided that such data is securely isolated, protected in accordance with this DPA, and deleted or overwritten in the ordinary course of Borg's, or its Sub-processors, backup retention policies.

9. LIABILITY

9.1 Each Party shall be liable for damages resulting from its breach of the Prevailing Data Protection Legislation or this DPA, subject to the exclusions and limitations of liability set out in the Master Service Agreement. The Customer shall remain solely responsible for the lawfulness of the Processing, including the legal basis and instructions provided to Borg, and Borg shall not be liable for Processing carried out in accordance with the Customer's documented instructions. This includes Processing performed through Automated Processing Systems in accordance with the Services and Annex A.

9.2 Each Party shall be liable to data subjects for damage caused by Processing in accordance with GDPR Article 82. Where both Parties are responsible, liability shall be apportioned in accordance with Article 82(5).

10. TERM AND TERMINATION

10.1 This DPA shall apply for as long as Borg Processes, including through Automated Processing Systems, Personal Data on behalf of the Customer under the Master Service Agreement.

10.2 This DPA shall automatically terminate upon termination of the Master Service Agreement, provided that all Personal Data has been deleted or returned in accordance with Section 8, unless continued Processing is required under applicable law.

11. GOVERNING LAW AND JURISDICTION

11.1 This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions set out in the Master Service Agreement.

ANNEX A – DESCRIPTION OF THE PROCESSING

A.1 Purpose of the processing

The Data Processor will process personal data on behalf of the Data Controller in order to provide the Services in accordance with the Master Service Agreement, including offensive security testing, vulnerability discovery, asset discovery, analysis, and reporting.

A.2 Nature of the processing

Processing is carried out through the Customer's use of the Services, including automated systems and AI-based agents, and may include analysis of systems, repositories, environments, configurations, and behavior, as well as vulnerability discovery, validation, and generation of findings and reports.

Processing may occur through:

(i) Processing involving access by Borg personnel, which may include access to Personal Data in an intelligible form where necessary to provide the Services; and

(ii) Processing performed solely by automated systems and AI-based agents, which may involve transient or in-environment access to Personal Data within the Customer's systems or environments, without such data being extracted or made available to Borg in an intelligible form and may include incidental access to Personal Data.

A.3 Types of personal data

Depending on the Data Controller's use of the Services, Processing may include any categories of Personal Data present in the Data Controller's systems, environments, or data sources made available to the Services, whether actively provided or incidentally encountered.

For the purposes of Section A.2 i), Processing involving access by Borg personnel may include Personal Data that is stored, generated, or otherwise made available through the Services, including, but not limited to;

- name and contact information
- user identifiers and account data
- Personal Data contained in findings, reports, screenshots, and other testing evidence
- limited logs, metadata, and system-generated data to the extent surfaced in the Services, and
- support-related data

For the purposes of Section A.2 ii), Processing performed solely by automated systems and AI-based agents may include Personal Data contained within the Data Controller's systems, environments, repositories, or live instances, including, but not limited to;

- Personal Data contained in source code, repositories, databases, or applications
- logs, metadata, and system-generated data
- IP addresses and other technical identifiers
- authentication data (e.g. tokens, credentials), and
- traffic, configurations, and other operational data

Processing is not intended to include special categories of Personal Data (GDPR Article 9) or data relating to criminal convictions (GDPR Article 10). However, such data may be incidentally processed where present in the Data Controller's systems or environments.

The Data Controller is solely responsible for determining the categories of Personal Data made available to the Services and for ensuring a valid legal basis and appropriate safeguards for such Processing.

A.4 Categories of data subjects

Data subjects may include the Data Controller's employees, contractors, end users, customers, and other individuals whose Personal Data is processed within the Data Controller's systems.

A.5 Duration of the processing

The Data Processor will process personal data on behalf of the Data Controller for as long as the Data Controller uses the Data Processor's Services and for as long as this DPA remains in force, unless longer retention is required by applicable law.

ANNEX B - AUTHORISED SUBPROCESSORS

Upon commencement of this DPA, the Customer authorizes Borg to engage the Sub-Processors listed at http://odin.borghq.io/legal/subprocessors for the processing described therein.