Privacy Policy

Borg Security AS

Effective date	20/04/2026
Last updated	20/04/2026
Contact	privacy@borgresearch.io
Website	https://odin.borghq.io

This Privacy Policy explains how Borg Security AS ("Borg," "we," "us," or "our") collects, uses, stores, and discloses personal data in connection with our services, including the Odin platform, asset discovery tools, AI-enabled penetration testing services, related reporting, support, and associated websites or portals (collectively, the "Services").

Borg provides autonomous and AI-enabled offensive security services and acts as a data processor on behalf of customers when providing the core Services and/or as an independent data controller for its own legitimate business purposes, such as account management, billing, security, fraud prevention, service integrity, analytics, cookies, troubleshooting, marketing communications, and legal compliance.

1. Who we are

Borg Security AS

Kjopmannsgata 59, Trondheim, 7011, Norway

Privacy contact: privacy@borgresearch.io

Website: https://odin.borghq.io

2. Scope of this Privacy Policy

- This Privacy Policy primarily applies to personal data processed by Borg as an independent data controller when we manage customer accounts, billing, support, cookies, analytics, marketing, and security, maintain our platform and websites, and otherwise process personal data as an independent controller for our own legitimate business purposes.
- Where Borg acts as a data processor when operating and providing the Services, the processing is governed by the applicable data processing agreement (DPA), and the customer acts as data controller. This Privacy Policy does not replace any data processing agreement between Borg and its customers. Where Borg processes personal data on behalf of a customer, the relevant customer remains responsible for the lawfulness of that processing and for responding to certain privacy requests where required by law.

3. Governing audience and jurisdictions

This Privacy Policy is intended primarily for customers, users, and website visitors in Norway and the European Economic Area (EEA).

- Borg is headquartered in Norway and seeks to structure its privacy practices in line with the GDPR, the Norwegian Personal Data Act, and related EEA privacy standards. If non-EEA laws apply to a particular customer relationship, that may be addressed separately in contract.

4. Roles of the parties

When Borg acts as a processor (which is the default for the core Services): Borg processes personal data on behalf of customers in order to provide the Services, including offensive security testing, asset discovery, vulnerability discovery and validation, analysis of systems, repositories and configurations, and the generation of findings, reports, and related outputs.

When Borg acts as an independent controller: Borg may also process personal data as an independent controller where necessary for its own legitimate business purposes, including account administration, billing, platform and service security, abuse prevention, fraud detection, service integrity, troubleshooting, analytics, marketing communications, audit, and legal compliance.

5. Personal data we process

- Account, contact, and business information, such as names, business email addresses, user identifiers, workspace details, and billing or administrative information.
- Customer environment and service data on behalf of the customer, including personal data contained in customer systems, repositories, databases, applications, cloud environments, logs, metadata, IP addresses, technical identifiers, configurations, findings, screenshots, evidence, and support records.
- Authorization and operational records, including verification events, integration authorizations, workspace settings, selections and exclusions, credentials, launch actions, pause or stop requests, and written instructions.
- Support, communications, website, and marketing data, including support requests, communications with Borg, web analytics, cookie identifiers, and subscription preferences.
- Sensitive or regulated data may be incidentally processed on behalf of the customer if it is present in customer systems or environments made available to the Services, even though the Services are not intended for special categories of personal data unless expressly agreed.

6. Sources of personal data

- We collect personal data directly from customers, authorized users, website visitors, and other individuals interacting with us.
- We also collect personal data through customer-configured integrations, repositories, cloud environments, APIs, connected systems, website cookies and analytics tools, billing systems, support channels, and the operation of the Services.

7. How we use personal data

The purposes of processing depend on Borg's role as either a data processor or an independent controller, and include the following:

- To provide the Services (as a data processor on behalf of the customer), including authentication, account administration, asset discovery, security testing, findings management, reporting, support, and professional services.

- To operate and secure our business (as an independent data controller), including maintaining service integrity, detecting and preventing abuse or fraud, enforcing our agreements, troubleshooting, maintaining audit trails, logs, and technical records, and complying with legal obligations.
- To improve and analyze our Services (primarily as an independent data controller, and where possible using aggregated or de-identified data), including service analytics, benchmarking, troubleshooting, support, and product improvement using de-identified or aggregated data where appropriate.
- To communicate with you about service updates, security notices, and operational issues (as a data processor on behalf of the customer), and to send product announcements, and marketing communications (as an independent data controller) in accordance with applicable law and your communication preferences.

8. AI-enabled and automated processing

- Our Services include AI-enabled, automated, and agentic security functionality. Processing may occur through systems that analyze customer environments, repositories, and other data sources with limited or no human review.
- This means personal data may be analyzed by automated systems without necessarily being extracted or made available to Borg personnel in an intelligible form. The Services are designed to support activities such as analysis, vulnerability discovery, validation, and report generation using automated systems.

9. Human access restrictions

- Borg limits human access to personal data and customer content.
- In connection with AI Services, Borg personnel will not access or review the substantive contents of a customer's internal files, repositories, databases, applications, environments, or other information residing within customer systems without the customer's prior explicit consent, except where required by applicable law.
- This does not prevent Borg personnel from accessing credentials, logs, metadata, findings, operational telemetry, audit records, screenshots, or other technical records where reasonably necessary to operate, support, secure, audit, troubleshoot, or improve the Services.

10. Cookies and analytics

- Our websites and portals may use cookies and similar technologies for security, session management, authentication, preference storage, analytics, and product improvement.
- Where required by applicable law, we will request consent before placing non-essential cookies or similar technologies on your device.
- You can usually control cookies through your browser settings and, where offered, through our cookie consent tools. Disabling some cookies may affect website or platform functionality.

11. Marketing communications

- We may send marketing or product-related communications to business contacts where permitted by applicable law.
- You can opt out of non-essential marketing communications at any time by using the unsubscribe mechanism in the message or by contacting privacy@borgresearch.io.
- We may still send service-related, transactional, security, or administrative communications where necessary.

12. Legal bases for processing

- Where Borg acts as an independent controller, we process personal data on one or more of the following legal bases, as applicable: performance of a contract, compliance with legal obligations, legitimate interests, and consent where required by law.
- Where Borg acts as a processor on behalf of a customer, the customer is responsible for determining and documenting the appropriate legal basis for the processing.

13. Disclosure of personal data to third parties and affiliates

- Where Borg acts as an independent controller we may disclose personal data to affiliates, and service providers (acting as processors), including infrastructure and hosting providers, analytics providers and payment processors. We may also disclose personal data to professional advisers, auditors, regulators, courts, law enforcement, and others where necessary to protect rights, security, service integrity, or legal compliance.
- Such third parties act as independent controllers or processors to Borg, depending on the nature of the relationship.

14. Subprocessors

- Where Borg acts as a data processor, we engage subprocessors to process personal data on behalf of the customer in connection with the delivery of the Services. Such subprocessors may include hosting and infrastructure providers, analytics providers, storage providers, payment processors, model and AI service providers, and other vendors supporting delivery of the Services.
- All subprocessors are engaged in accordance with the applicable Data Processing Agreement (DPA).
- An up-to-date list of authorized subprocessors is available at: https://odin.borghq.io/legal/subprocessors

15. International transfers

- Borg may transfer personal data to affiliates, subprocessors, or service providers in countries outside the EU/EEA where necessary to provide the Services. Where Borg acts as a data processor, international transfers are carried out on behalf of the customer and in accordance with the applicable DPA and the customer's instructions.
- Where required by applicable law, Borg uses an appropriate transfer mechanism for such transfers, such as Standard Contractual Clauses or another valid mechanism under applicable data protection law.

16. Security

- Borg maintains a written information security program designed to protect the confidentiality, integrity, and availability of customer content and personal data.
- Our security measures include encryption of customer content at rest and in transit using industry-standard cryptographic protocols, role-based access controls, least-privilege access, multi-factor authentication, strict access limitations, regular vulnerability assessments and penetration testing, and a documented incident response plan.

17. Incident response

- If Borg becomes aware of a personal data breach affecting personal data within Borg's systems or under Borg's control, Borg will notify the relevant customer without undue delay, as required by applicable law and the applicable agreement.
- Where Borg acts as a processor, the relevant customer remains responsible for notifications to supervisory authorities and data subjects unless applicable law requires otherwise.

18. Data retention

- Where Borg acts as a data processor, retention of personal data is governed by the applicable Data Processing Agreement (DPA) and the instructions of the customer.
- Where Borg acts as an independent data controller, we retain personal data for as long as necessary for the purposes described in this Privacy Policy, including for account administration, billing and legal compliance, and as reasonably necessary for security, audit, fraud prevention, dispute handling, and defense of claims.
- Borg may retain logs, audit records, security telemetry, incident records, and similar technical records where reasonably necessary for those purposes, even if such records contain or reflect personal data.
- Personal data retained in backup systems may be kept until deleted or overwritten in the ordinary course of backup retention practices, provided it remains protected.

19. Data subject rights

- Depending on your location and the applicable law, you may have rights to request access, correction, deletion, restriction, objection, portability, and to lodge a complaint with a supervisory authority.
- If Borg processes your personal data on behalf of a customer, that customer acts as the data controller and is responsible for handling your request. If you contact us to exercise your rights in relation to personal data processed on behalf of a customer, we will, where appropriate, redirect your request to the relevant customer or inform you how to contact them.
- To exercise your rights in relation to personal data processed by Borg as an independent data controller, or to otherwise contact us regarding privacy matters, email privacy@borgresearch.io.

20. California privacy notice

- To the extent the California Consumer Privacy Act (CCPA) applies, Borg processes relevant personal information on behalf of customers for the business purposes set out in the applicable agreements and does not sell or share personal information within the meaning of the CCPA.

21. Children

- Our Services are intended for business and enterprise use and are not directed to children.

22. Changes to this Privacy Policy

- We may update this Privacy Policy from time to time. Where required by law, we will provide notice of material changes by appropriate means, such as email, in-product notification, or by posting an updated version on our website with a revised effective date.

23. Contact us

Borg Security AS

Kjopmannsgata 59, Trondheim, 7011, Norway

- privacy@borgresearch.io
- https://odin.borghq.io