Heimdal General Data Protection Regulation (GDPR) and Privacy Whitepaper

Our commitment to Security, Compliance and Privacy

HEIMDALSECURITY.COM

About Heimdal® Security (Heimdal/ the Company)

Founded in Copenhagen in 2014, Heimdal empowers CISOs, Security Teams, and IT admins to enhance their SecOps, reduce alert fatigue, and take proactive measures through one seamless command and control platform.

Heimdal's award-winning cybersecurity solutions cover the entire IT estate, offering solutions for every challenge, from endpoint to network level, in vulnerability management, privileged access, Zero Trust implementation, ransomware prevention, and more.

Currently, Heimdal's cybersecurity solutions are deployed in over 45 countries, supported regionally by offices in 15+ countries, by 175+ highly qualified specialists. Heimdal is ISAE 3000 certified and secures more than three million endpoints for over 11,000 companies.

Heimdal provides unwavering support to its partners, focusing on consistency and scalability. The common goal is to create a sustainable ecosystem and a strategic partnership between Heimdal and its partners.

For more information, visit Heimdal.

1. Privacy and General Data Protection Regulation

At Heimdal, we are committed to respecting privacy and keeping personal data safe. Our work is in line with international privacy regulations, GDPR (General Data Protection Regulation), and customers' expectations.

We analyzed GDPR requirements and how they reflect in our Company's activities. Consequently, we implemented an organization-wide GDPR, and privacy compliance strategy intended to meet all requirements.

We're equally committed to helping our clients be GDPR compliant by implementing processes that uphold the underlying principles of GDPR. However, it is important to recognize that privacy compliance is a shared responsibility. Regulatory privacy compliance requires a combination of processes, policies, expertise, education, and training as well as appropriate internal tools.

We believe that the path to compliance requires a shared understanding and common culture around privacy.

2. GDPR Compliance Through Strategic Policy Implementation at Heimdal

At Heimdal, our dedication to data protection and privacy compliance reflects through a robust suite of policies designed to meet and exceed GDPR requirements.

These policies are integral to our security framework, ensuring that all aspects of data handling, from collection to disposal, are conducted with the utmost integrity and compliance.

a. General Data Protection Policy

Heimdal's General Data Protection Policy is the foundation of our privacy practices. It outlines our commitment to data protection and sets the standard for processing personal data within legal and ethical guidelines. This policy guides all other data protection policies and procedures, ensuring consistency and compliance across our operations.

b. Data Handling Policy

Our Data Handling Policy details the procedures for securing, processing, and managing personal data at every stage of its lifecycle. It defines the roles and responsibilities of all Heimdal employees involved in data handling, ensuring that personal data is processed in a manner that guarantees security and privacy.

c. Data Retention Policy

The Data Retention Policy at Heimdal specifies the duration for which distinct types of personal data can be retained based on their purpose and significance. This policy ensures compliance with GDPR's data minimization and storage limitation principles, stating clear guidelines for data retention and the conditions under which data must be securely disposed.

d. Data Subject Access Request Policy & Procedure

This policy provides a structured process for handling requests from data subjects who wish to access their personal data, as stipulated under GDPR. It includes templates and procedures that guide our response to these requests, ensuring timely and compliant handling of such inquiries.

e. Data Subject Rights Policy

The Data Subject Rights Policy at Heimdal outlines the procedures for upholding the rights of individuals under GDPR, including:

- the right to be informed
- the right to rectification
- the right to erasure
- the right to object

This policy ensures that data subjects can effectively exercise their rights, and it provides templates and guidance notes for Heimdal's staff on how to process and respond to rights requests appropriately.

f. Clean Desk Policy

Our Clean Desk Policy minimizes the risk of unauthorized access or data breaches by ensuring that sensitive information, whether digital or on paper, is not left unattended. This policy supports GDPR's principle of integrity and confidentiality, emphasizing the importance of a secure physical environment.

g. Data Breach Policy

Heimdal's Data Breach Policy establishes protocols for detecting, reporting, and investigating personal data breaches. It includes procedures for notifying supervisory authorities and affected individuals where necessary, in compliance with GDPR's timely breach notification requirements. This policy ensures that all breaches are handled systematically to mitigate any potential impact on the data subjects and the organization.

3. Security of processing personal data

In Heimdal, GDPR compliance is based on the control framework requirements of our ISAE 3000 Soc 2 certification. Through ISAE 3000 Soc 2 certification, Heimdal has incorporated several privacy controls into our larger security and control framework.

Heimdal demonstrates compliance with internal controls according to these standards, attested to by **an external independent auditor**. The scope of the audit includes key controls from GDPR and other privacy laws.

Heimdal's clients can see below a short description of the ISAE 3000 Soc 2 controls versus GDPR requirements:

ISAE 3000 Soc 2 control	Control activities	NIS 2 Directive Compliance
CC3.0 Risk assessment methodology	• Risk assessment	Art. 28 (General Obligations of Processors), Art 32 (Security of Processing).
CC5.3 Information security policies	• Information Security Policy • Personal Data Policy • Review of policies	Art. 28 (General Obligations of Processors), Art 32 (Security of Processing).

ISAE 3000 Soc 2 control	Control activities	NIS 2 Directive Compliance
CC7.0 System Operations & CC3.0 Risk assessment	• Roles and responsibilities • Remote workplaces • Authentications of external connections • Authentification of external suppliers on internal systems	Art. 28 (General Obligations of Processors), Art. 31 (Cooperation with the supervisory authority) Art. 33 (Notification of a personal data breach to the supervisory authority
CC.1.0 Human resource security and personal	• Before employment • During employment • GDPR awareness • Non-disclosure and confidentiality agreements • End or change of employment • Communication with authorities • Control ownership and responsibili	Art. 28(1) Specifies that a processor shall only act on the documented instructions from the controller. Art. 28(3)(b) Requires the processor to ensure that persons authorized to process the personal data have committed themselves to confidentiality.
CC3.0 Risk assessment	• Risk assessment methodology • Information security risks • Risk review and approval • Ownership of assets • Classification of assets • Classification of information	Art. 30 (Records of processing activities) Art. 32 (Security of Processing)
CC5.0 Control activities – Access management	• Policy for access management • User registration and deregistration • Management of access rights • Management of privileged access rights • Management of password requirements	Art. 28 (General Obligations of Processors), Art. 30 (Records of processing activities) Art. 32 (Security of Processing)
CC6.0 Logical and physical access controls	• Physical perimeter safeguarding • Physical access control • Data ownership • Administration of certificates and keys	Art. 28 (General Obligations of Processors),
CC7.0 System Operations	• Vulnerability checks • Threat management • Enable detailed logging • Event alerts • Critical monitoring • Logging of unsuccessful logins • Logging of privileged access	Art. 28 (General Obligations of Processors),
CC2.0 Communication and information security	• Policies and procedures for transfer of information • Track software inventory information • Information security incident management	Art. 28(3)(c) Requires contracts between controllers and processors to mandate that processors implement appropriate technical and organizational measures for data security, safeguarding against unauthorized or unlawful processing, loss, destruction, or damage.

ISAE 3000 Soc 2 control	Control activities	NIS 2 Directive Compliance
CC6.2: Acquisition, development and maintenance of systems	• System acquisition, development and maintenance of systems	Art. 25 Data protection by design and by default
CC9.0: Supplier relationships, processors and sub-processors	• Agreements with sub-processors • Approved sub-processors • Supervision of sub-processors	Art. 28 (General Obligations of Processors),
CC7.3: Information security incident management	• Information security incident management • Reporting of information and personal data security incidents • Controles and responsability	Art. 32 (Security of Processing) Art. 33 Notification of a personal data breach to the supervisory authority Art 34 (Communication of a personal data breach to the data subject)
Compliance	• Identification of applicable legislation • Data protection agreements with clients • Instruction from clients • Reasonable assistance to the clients • Deletion and return of customers data • Independent review of controls	Art. 28 (General Obligations of Processors), Art. 29 (Processing under the authority of the controller or processor) Art. 30 (Records of processing activities) Art. 32 (Security of Processing) Art. 33 Notification of a personal data breach to the supervisory authority

4. Personal data processed by our products

In adherence to the GDPR and other Privacy laws, our company commits to upholding the highest standards of privacy and data protection. Here are the general principles guiding our data processing activities:

a. Lawfulness, Fairness, and Transparency: Processing is always performed legally, fairly, and in a transparent manner in relation to the data subject.

b. Purpose Limitation: The data is collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

c. Data Minimization: Adequate, relevant, and limited data are processed in relation to the purposes for which they are processed.

d. Accuracy: All reasonable steps are taken to ensure that inaccurate personal data is promptly erased or corrected.

e. Storage Limitation: Personal data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

f. Integrity and Confidentiality: Processing is done in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

Following these principles, the specific personal data processed by our products are outlined below:

Product	Data Processed (description)
DNS Security Endpoint	Hostname, Username (associated with the Hostname), IP Address, Domains
DNS Security Network	Hostname, IP Address, Domain
Next-Gen Antivirus, XTP and MDM	Hostname, Username (associated with the Hostname), Personal Applications Executed
Ransomware Encryption Protection	Hostname, Username (associated with the Hostname), Personal Applications Executed
Privilege Elevation and Delegation Management (PEDM)	Hostname, Username (associated with the Hostname), Personal Applications Executed
Application Control	Personal Applications Executed
Email Security	Email Content, Email Attachments, Email body, Email Subject, Email Address, Source & Destination IP
Remote Desktop Control	Username, IP Address, Session Recordings (if enabled, will be stored with Heimdal).
Patch and Assets Management	Hostname, Username (associated with the Hostname), Name of installed 3rd party applications and their versions, Name of available and installed Operating System updates
Threat - hunting and Action Center (TAC)	Depending on the products that you have the data processed above
Privileged Account and Session Management (PASM)	Server name (chosen by the data controller), number of accounts (administrator users and non-administrators), usage data (number and length of sessions)
Heimdal Dashboard (XDR – Unified Security Platform)	User login details: Full name, E-mail Address, Phone number (optional)

5. Data Storage and Management at Heimdal: Aligning Product Strategies with GDPR Compliance

Heimdal's approach to data storage and management is meticulously designed to align with the General Data Protection Regulation (GDPR) requirements, ensuring that all personal data handled across our product offerings is stored securely and managed responsibly. This chapter outlines our strategic framework for data storage, detailing the specific storage practices for each product, highlighting how these practices comply with GDPR's stringent standards for data protection.

Overview of Data Storage Principles at Heimdal

At Heimdal, we adhere to the following key principles to ensure GDPR compliance in our data storage practices:

a. **Data Minimization:** We store only the data necessary to fulfill the intended processing purposes.
b. **Limitation of Purpose:** Data is collected and stored strictly for legitimate business purposes as disclosed to and consented by the users.
c. **Security of Data:** Implementing robust technical and organizational measures to protect data against unauthorized access, alteration, and destruction.
d. **Storage Limitation:** Data is retained only for as long as necessary to serve the specified purposes and in accordance with our Data Retention Policy.

Product	Storage period
DNS Security Endpoint	2 years
DNS Security Network	30 days
Next-Gen Antivirus, XTP and MDM	2 years
Ransomware Encryption Protection	90 days for endpoint; 2 years for cloud
Privilege Elevation and Delegation Management (PEDM)	2 years
Application Control	90 days
E-mail Security	none, 30 days, 90 days or 1 year
Remote Desktop Control	2 years
Patch and Assets Management	2 years
Threat - hunting and Action Center (TAC)	2 years
Privileged Account and Session Management (PASM)	2 years
Heimdal Dashboard (XDR – Unified Security Platform)	Contract period

6. Data Storage Locations and Options at Heimdal: Ensuring Flexibility and Compliance

At Heimdal, we understand the importance of data sovereignty and the diverse compliance needs of our global customer base. To accommodate this, we offer flexible data storage options across multiple regions, ensuring that our clients can select the data storage location that best meets their legal and operational requirements.

Heimdal's customers have the privilege of selecting the location where their data is stored, depending on the product they use. This choice allows businesses to meet specific data residency requirements and helps in complying with regional data protection regulations. **If a customer does not specify a preference, by default, data is stored within the European Union, thereby aligning with stringent EU data protection standards.**

Data Storage Locations for Heimdal Products

a. DNS Security Network

For our DNS Security Network product, we offer the following data storage options on Amazon Web Services (AWS), allowing customers to choose the location that best suits their regulatory and operational needs:

- **AWS Europe (Germany/Frankfurt):** Ideal for customers who require data storage within the European Union to comply with GDPR and other European data protection laws.
- **AWS UK (UK/London):** Serves customers who prefer their data to be stored in the UK, accommodating post-Brexit data sovereignty requirements.
- **AWS US (US/Virginia):** Suits customers in the United States, ensuring compliance with US data protection regulations and providing fast, reliable service to North American users.

b. All Other Heimdal Products

For all other products, Heimdal utilizes Microsoft Azure for data storage, with the following options available to meet diverse geographical and regulatory needs:

- **Azure Europe (Netherlands/Amsterdam):** This location is ideal for customers within the EU who are seeking compliance with GDPR and wish to maintain data within the European Economic Area.
- **Azure UK (UK/London):** Offers a dedicated option for UK-based customers, ensuring data sovereignty in alignment with UK data protection regulations.
- **Azure US (US/Virginia):** Provides a storage solution for U.S. customers, aligning with local compliance requirements and ensuring optimal data access speeds.

7. Conclusion

In this Whitepaper, we have outlined Heimdal's robust approach to ensuring compliance with the General Data Protection Regulation (GDPR) and maintaining the highest standards of privacy and data protection. Through our multi-layered security suite and comprehensive privacy policies, Heimdal demonstrates an unwavering commitment to safeguarding data across all operations.

Heimdal's commitment to security, compliance, and privacy is not just about adhering to regulatory requirements but is a core aspect of our operational philosophy.

Our GDPR compliance is complemented by our ISAE 3000 certification and the integration of privacy controls into our security framework, further enhanced through regular audits by an independent external auditor. This rigorous approach ensures that both Heimdal and our clients meet the stringent demands of various privacy laws and regulations effectively.

As we move forward, Heimdal will continue to innovate and adapt our strategies to meet the challenges of the digital age, ensuring that our commitment to security, privacy, and compliance remains strong.

By choosing Heimdal, organizations can trust that they are partnering with a leader dedicated not only to technological excellence but also to the ethical responsibility of protecting data.

For further details about our GDPR compliance and data protection practices, or if you have any specific inquiries, please contact our Data Protection Officer at

For further details about our GDPR compliance and data protection practices, or if you have any specific inquiries, please contact our Data Protection Officer at compliance@heimdalsecurity.com.

Confidentiality and Liability Disclaimer

This Whitepaper is intended for informational purposes only and is provided as a general resource, not as a comprehensive guide.

The contents are considered confidential and are the proprietary information of Heimdal. Unauthorized distribution or use of this document is strictly prohibited.

While every effort has been made to ensure the accuracy of the information contained herein, Heimdal assumes no responsibility for any errors or omissions. The information provided is subject to change without notice, and Heimdal does not guarantee that the measures described are appropriate for every situation.

Specific features and details are typically provided in product data sheets and through direct consultation. It is recommended that clients consult these resources, or contact Heimdal directly, to understand how our solutions may be configured to meet the specific requirements of their environment.

Heimdal®

HEIMDALSECURITY.COM