DATASHEET

Infoblox Privacy Sheet

SUMMARY

This Infoblox Privacy Sheet describes the processing of personal data (or personally identifiable information) by Infoblox solutions.

OVERVIEW OF INFOBLOX CAPABILITIES

Infoblox provides on-premise and cloud-based software products, services, and solutions ("Services") to provide DNS / DHCP/ IP Address Management (DDI) services (e.g., IP address management, advanced domain name system architecture) and network security tools (e.g., threat and malware defense).

Please see the following link for more details on Infoblox: https://www.infoblox.com/products/.

Individuals working for or on behalf of you as the customer may be asked to provide personal data (e.g., name, email address for credentialing process) ("you" or "end-user") in order to use the Services (e.g., through registering to use the customer support portal or Infoblox cloud services portal. Configurations of Infoblox's Services may also cause personal data to be exposed or sent to Infoblox; specific design configuration choices related to personal data can be reviewed with Infoblox's sales engineers. The following paragraphs describe Infoblox's processing of personal data in connection with the delivery of Services, the location and transfers of that data as part of the Services, and how that data is secured through provision of the Services in accordance with applicable privacy law and principles. If you choose to use Infoblox's Services that involve Infoblox cloud services or if you engage with Infoblox for maintenance and support services, you will need to disclose personal data to Infoblox.

Infoblox will use your personal data in a manner consistent with all domestic and international privacy regulations, this Privacy Sheet, and according to any Agreement you enter into as a condition of using the Services. The following paragraphs describe which personal data that Infoblox processes to deliver the Services, the location of that customer's personal data, and how that customer personal data is secured in accordance with applicable privacy law and principles.

PERSONAL DATA PROCESSING

The table below lists the personal data used by Infoblox to carry out the services and describes why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing
Platform Account/ Contact Information	• Administrator first and last name • Administrator email address	• Activation of services • Future notification of features/updates • Remote access support • Authentication/Authorization
User, Device and Network Usage and Event Data	• IP Addresses • MAC Addresses • Hostname/Device name/ID • Username/Group name • Device ID	• DNS query data is initially processed to direct end user to the domain being queried • DNS query data is used to conduct analytics and statistical analysis in aggregate form to track and predict threats, for internal security research, and for reporting purposes to customer • All Usage and Event Data is also processed for Infoblox threat intelligence research by threat intelligence research teams
Authentication, Activity and Configuration Logs	• Which end-users access the services • Which devices access the services • End-user IP address when accessing the services • Device ID	• Provide and maintain services • Improve user experience of the services • Improve security functionality of the services • Improve quality of the services • Log what policies were implemented and/or changed and the customer administrator who made the change
Dashboard Activity Information	• Device information: device name, IP address, MAC addresses, Hostname/ Device name/ID	• Analyze feature usage and product functionality
Support Information	• First and last name • Email address • Phone number • Job title • Time zone • Customer data uploaded through Support tickets	• Review of the support service quality • Troubleshooting • Analysis of service
Support Bundles	• NIOS configurations Internal device identifiers such as IP addresses, MAC addresses, hostnames	• A ‘snapshot’ of the running configuration of the NIOS appliance may be uploaded to Infoblox customer support in order to reproduce issues.

CROSS-BORDER TRANSFERS

Infoblox is headquartered in the United States and operates internationally. Infoblox Threat Defense and DDI products are built upon Amazon Web Services ("**AWS**") within multiple data centers in the AWS East Region of the United States and in the AWS Frankfurt Region of Germany.

AWS offers robust controls to maintain security and data protection. Physical security controls include, but are not limited to, perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems, and other electronic means. Infoblox can provide additional information about AWS security and certifications under NDA to existing customers. More details about Infoblox's security can be found in our technical and organizational measures ("**TOMs**"), which is available here.

Infoblox provides customer support via a 'follow-the-sun' methodology which involves support staff in multiple global Centers of Excellence to be involved in resolving incidents. Infoblox's customer support employees throughout the world may have access to Customer's personal data stored in the United States or Germany on AWS or otherwise provided by Customer to Infoblox during maintenance or support Services. Additionally, certain personal data may be transferred across borders to Infoblox's third party vendors ("**Sub-processors**") for purposes related to providing the Services, such as providing telephone services, sending surveys after responding to support calls, providing customer relationship management services, hosting other backend solutions for Infoblox. These Sub-processors each sign Data Processing Agreement with Infoblox which define the uses they may make of the information and the minimum security requirements for protecting our Customer data.

Infoblox relies upon EU Standard Contractual Clauses for cross-border transfers of data from the European Union to the United States and other countries that have been found to lack appropriate data privacy protections. Each Customer with EU locations should enter into our Data Processing Agreement which includes the Standard Contractual Clauses and is available here.

ACCESS CONTROL

Access by Customer

Customers can view activity logs through the platform interface. Administrators can also modify and control access to the services and other administrator information, set network policies, monitor network, and limit or approve access to users and applications.

Access by Infoblox

Access to logs is restricted to support engineers, threat research and analytics teams, as well as customer support teams when a support case is opened. Access is allowed for the purposes of troubleshooting, solving issues, and improving the effectiveness of security protections.

DATA DELETION AND DATA RETENTION

A customer may request deletion of individual personal data at any time by submitting a request through the Infoblox Support Portal. When a customer makes a request for deletion of personal data stored by Infoblox, Infoblox will purge or anonymize the requested data from its systems to the extent required by applicable law and/or contract and may retain administrative data required for legitimate business purposes. Infoblox only keeps personal data for as long as it has an ongoing legitimate business need to do so.

PERSONAL DATA SECURITY

Infoblox uses encryption to protect customers' personal data at rest and in transit. Across our catalog of products and services, we implement encryption to meet or exceed industry standards and best practices. For any personal data that is transmitted across public or untrusted networks, Infoblox implements Transport Layer Security (TLS 1.2) or IPSEC encryption to safeguard the confidentiality and integrity of customers' data.

Regardless of whether the data is encrypted, Infoblox uses multiple techniques to protect customer data, including, but not limited to: network segmentation between datastores and other components of the Infoblox platform, least privilege access to datastores based upon roles or responsibilities, and hardening of production assets to minimize attack surface.

INFORMATION SECURITY INCIDENT MANAGEMENT

Breach and Incident Notification Processes

The Infoblox security team coordinates the data incident response process and manages the Infoblox's response to data-centric incidents. The Infoblox team works in collaboration with incident response teams within Infoblox, including the Infoblox Product Security Incident Response Team ("**PSIRT**") where applicable and necessary to a particular incident.

Infoblox's security team, in collaboration with the Infoblox PSIRT team, manages the receipt, investigation, and public reporting of security vulnerabilities related to Infoblox's Services. The team works with customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Infoblox's Services.

Customers may subscribe to notifications of Infoblox security advisories within the Customer Support Portal. The subscriber's relationship with Infoblox determines the level of access. If you have questions or concerns account accessing the Support Portal, please contact Customer Support.

Certifications and Compliance with Privacy Laws

The Infoblox Information Security and Legal Teams provide risk and compliance management and consultation services to the Infoblox Business Teams to help drive security and regulatory compliance into the design of Infoblox's Services. Infoblox and its underlying processes are designed to meet Infoblox's obligations under the EU General Data Protection Regulation ("GDPR") and other privacy laws around the world.

Infoblox achieved FedRAMP moderate authorization for Infoblox Threat Defense Federal Cloud on 12/15/2022. The NIOS / Trinzic hardware appliance is Common Criteria EAL-2 Certified. Infoblox has completed SOC 2 Type II audits and is currently working on ISO 27001. To access our comprehensive compliance documentation and find answers to frequently asked questions related to security and privacy, please visit our Infoblox Trust Center.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240827v1