General GDPR Policies

Q: Is Infoblox compliant with GDPR?
A: Yes, Infoblox complies with applicable law including, without limitation, GDPR. Infoblox currently complies with GDPR through use of standard contractual clauses. Infoblox includes a customer Data Processing Addendum (DPA) as part of its terms and conditions available at https://www.infoblox.com/company/legal/data-processing-addendum. Infoblox will gladly enter into a fully executed DPA and model clauses for the transfer of personal data outside of the EU with customers as needed and upon request that is substantially similar to Infoblox’s standard DPA. All such requests to enter into a fully executed DPA should be directed to your Infoblox account representative.

Q: Does Infoblox have the necessary agreements with its subprocessors to comply with GDPR?
A: Yes, Infoblox has executed DPAs and standard contractual clauses (as necessary) with select subprocessors as required under GDPR. Infoblox’s list of subprocessors is available to customers upon request by contacting the Infoblox account team executive.

Q: Will Infoblox join the EU-US Privacy Shield Framework?
A: Infoblox plans to join the EU-US Privacy Shield Framework. Infoblox has engaged a third-party specialist to become Privacy Shield certified and anticipates becoming Privacy Shield certified within the year.

Q: What is the process for customers to view or request to remove any data associated with an individual (i.e., “the right to be forgotten”)?
A: Infoblox complies with applicable law and its contractual obligations, including, without limitation, requirements around data retention. Infoblox customers are organizations rather than individuals, but Infoblox may process personal data relating to individuals as part of conducting business or providing services. If a customer organization uses an Infoblox service, then the process will be specific to that service. Please review our Privacy Policy at https://www.infoblox.com/company/legal/privacy-policy/ for information on our practices. An individual belonging to a customer organization may access, correct, amend or request deletion of their personal data by logging into their account for Infoblox sites or solutions or at http://info.infoblox.com/manage-profile.html. Individuals may also request access to their personal data and to have their personal data corrected, blocked or deleted by sending an email to privacy@infoblox.com. In accordance with GDPR and contractual requirements, Infoblox will share requests for data deletion received from data subjects with the respective customer (i.e., controller).

Q: What is Infoblox’s privacy policy, and how can I ask Infoblox about data privacy questions?
A: Infoblox’s privacy policy (https://www.infoblox.com/company/legal/privacy-policy/) provides general information on our privacy practices. All data privacy-related inquiries should be directed to privacy@infoblox.com.
Q: Where is the data being processed and stored?

A: Depending on the products purchased by the customer, data may be processed and stored in the customer data center or in a cloud environment or a hybrid solution. Details about processing and storage of personal data are handled during contract negotiations with the customer. The customer agreement will specify the nature, scope, purpose, and duration of personal data that the parties anticipate will be involved in the services. The details about processing and storage will be based on the geographic scope of the project and the product or solution being procured or implemented by the customer.

Q: How do Infoblox customers get notified in case there is a data breach that impacts customer data?

A: Infoblox will notify customers of a data breach in accordance with applicable law and contractual obligations. Infoblox will notify impacted individuals via email to the registered users within Infoblox systems such as Infoblox Cloud and Infoblox Support Portal and/or in accordance with applicable law and contractual obligations.

GDPR and Infoblox Products

Q. What is Infoblox’s GDPR compliance strategy for on-premises products such as NIOS™?

A: The NIOS appliance is a highly secure platform which does not need to be specifically modified in order to become GDPR compliant. When upgrades or changes to NIOS operating system are developed, careful review is given to desired changes to ensure that the handling of personal data is not impacted. Customers who install the on-premises NIOS / Grid platform maintain the majority of their data within their own data centers. When obtaining customer support, personal data may be captured as part of troubleshooting, as referenced on page 4, below.

Q. What tools does Infoblox provide to secure NIOS data?

A: Since the personal data processed as part of the products and services is owned and processed by the customer in an on-premise implementation, the customer may elect to use various state-of-the-art mechanisms and tools provided by Infoblox as part of the implementation to secure the data collected by NIOS. The NIOS / Grid appliance is Common Criteria certified and may be operated in a mode which meets strict FIPS 140-2 encryption standards, providing additional data security.

Q. What tools / methodologies are available for a NIOS customer to comply with GDPR related requests such as “right to access personal data” or “right to be forgotten”?

A:

1. **Request for personal data access** – End-users’ request for access to personal data stored by NIOS can be fulfilled by performing a global search.

2. **Requests for deletion of personal data** – Historical data can be deleted using the tools available in Splunk Add-on to delete appropriate indexes. Another solution is to create relevant dashboards within Infoblox Reporting and Analytics, which can further be used to initiate deletion of user data.

3. **Requests related to stop collecting data** – The need for collecting personal data can be minimized by modifying the type of data collected by NIOS. As an example, usernames associated with IP addresses need not be stored in NIOS data sets. Such personal data can be stored outside of NIOS, for instance NIOS can be integrated into a SIEM which may contain the personal data.
Q. Will there be any data integrity issues in NIOS if data is deleted to fulfill a GDPR related request?

A: There should not be any data integrity issues in NIOS if the data is deleted from the GUI, APIs, or Splunk user interface.

Q. What DNS/DHCP/IP Address Management (DDI) related data received by Infoblox may be subject to GDPR regulations?

A. Depending on the products and services purchased by the customer, personal data may be transferred from a customer to Infoblox making the products and services subject to GDPR. The customer is the controller of such personal data and decides what personal data is collected and processed through engaging Infoblox to provide the products and services. Infoblox collects and processes personal data only as necessary to provide the products and perform the services for which the customer has engaged Infoblox. Personal data is retained in accordance with applicable law and contractual requirements agreed to by Infoblox and the customer.

Q. Are Infoblox’s cloud services (such as BloxOne™ Threat Defense (B1TD), formerly known as ActiveTrust Cloud) subject to GDPR?

A. This depends on if the data is subject to GDPR. This is a fact-specific inquiry. Infoblox stores data only as necessary to provide the services. Due to the nature of the services that Infoblox provides (including DDI infrastructure and security services), there may be a transfer of personal data across borders. For specific information on what personal data is processed for your particular solution, please contact your Infoblox account executive.

Q. What policies and procedures does Infoblox have for personal data that it processes or stores?

A. Infoblox has policies and procedures in place to ensure compliance with GDPR. Infoblox will support of its Customer’s GDPR compliance in accordance with contractual obligations and applicable law. Infoblox is in process for FedRAMP certification which includes third-party audit of all policies, procedures, security practices and technical controls related to the cloud platform. An overview of Infoblox’s cloud security posture is available to prospective customers upon request. Infoblox follows current research and industry trends that relate to cloud computing security to enable us to improve the security of Infoblox cloud services.

GDPR and Infoblox Support

Q. How do Infoblox Support Services implicate GDPR?

A. For the purposes of providing support services, Infoblox requires customers to create an account on the Infoblox support portal site and provide contact information for personnel authorized to contact Infoblox for support requests. If EU data is implicated, the agreement with the customer or Infoblox’s terms and conditions available at https://www.infoblox.com/company/legal/data-processing-addendum govern the transfer of personal data.

In providing support services, Infoblox may access personal data provided by customer to Infoblox in order to troubleshoot support issues that are contained in logs or datasets. Personal data submitted by a customer in connection with a support service will only be used by Infoblox for purposes of providing support to the customer. Through a customer’s account, the customer will have the ability to update the customer’s contact information. For any personal data that Infoblox may maintain in its records which cannot be accessed by a customer directly, the customer may submit a request to update or delete personal data as applicable, and Infoblox will process such requests in accordance with applicable law.