Arbor DDoS Products in a GDPR Compliant Environment

This document addresses questions from organizations that use Arbor DDoS (Distributed Denial of Service) products and are evaluating their GDPR compliancy obligations.

What is the GDPR?

The General Data Protection Regulation (GDPR) is a new comprehensive data protection law in the European Economic Area (EEA) that goes into effect on 25 May, 2018 and updates existing laws to strengthen the protection of personal data. It replaces the patchwork of national data protection laws currently in place with a single set of rules, directly enforceable in each EEA member state.

What does the GDPR regulate?

The GDPR regulates the "processing" — which includes the collection, storage, transfer or use — of personal data about EEA individuals. Any organization that processes personal data of EEA individuals, including tracking their online activities, is within the scope of the law, regardless of whether the organization has a physical presence in the EEA. Importantly, under the GDPR, the concept of "personal data" is very broad and covers any information relating to an identified or identifiable individual (also called a "data subject").

Under the regulation: '**Personal data**' is defined as any information relating to an identified or **identifiable natural person** (the '**data subject**').

A '**controller**' is defined as the natural or legal person which determines the purposes and means of the processing of personal data.

A '**processor**' is defined as the natural or legal person which processes personal data on behalf of the controller.

The GDPR requires controllers and processors to implement appropriate technical and organisational measures to **ensure a level of security appropriate to the risk**, taking into account the state of the art, the costs of implementation, as well as the likelihood and severity of risk to the rights and freedoms of natural persons.

The regulation grants data subjects some specific rights, amongst which are right of access (that is, for example, to receive a copy of their personal data); right to rectification of inaccurate personal data; right to erasure of personal data; right to data portability; and the right to object to processing of personal data.

Is the use of Arbor DDoS products permitted?

Yes. Under the GDPR, only lawful processing of data is permitted. Article 6 of the GDPR identifies the conditions under which processing is deemed lawful, which includes "processing [that] is necessary for the purposes of the legitimate interests pursued by the controller." Recital 49 of the GDPR explicitly refers to processing of data "to the extent strictly necessary and proportionate for the purposes of ensuring network and information security" as a legitimate interest pursued by a controller.

Arbor DDoS products, which include Arbor SP, Arbor TMS, and Arbor APS, are on-premise devices that are designed for the purpose of network and information security, DDoS detection, analytics, mitigation, and traffic analytics. As such, the use of Arbor products falls within the scope of processing necessary for the purposes of a legitimate interest pursued by the user of such products. With Arbor SP, customers are able to visualize and explore large amounts of network traffic statistics with varying levels of granularity depending on the age of data or the system's configuration. With Arbor TMS and Arbor APS, customers can mitigate DDoS attacks and other network threats by instructing the device to apply specific "countermeasures" to network traffic in transit, and can visualize samples of the traffic itself in order to build more accurate protection policies. The data collected and processed by Arbor DDoS products enables the customer, the controller, to visualize network traffic and mitigate DDoS attacks to protect and secure their network.

Is the data collected by Arbor DDoS products permitted under the GDPR?

Yes. Arbor SP collects flow telemetry records, which include source and destination address, number of bytes and packets and timestamps of IP traffic flows, as well as other information related to network infrastructure. Arbor TMS and Arbor APS can collect full IP packets for the purpose of analysis of DDoS attacks.

While "online identifiers" such as internet protocol (IP) addresses are referenced in the GDPR as an example of personal data that is subject to the regulation, the GDPR also sets forth the principles that some personal data is more sensitive than others and that certain types of processing presents a lesser risk to the rights and freedoms of individuals than others. While flow telemetry records and IP packets fall under the scope of personal data due to how broadly the term is defined under the GDPR, when the Arbor DDoS products are used for the purpose of network and information security, the level of risk presented by such processing is low. Controllers and processors using Arbor DDoS products can also take advantage of the security features made available by the Arbor DDoS products to further minimize risk associated with processing of this type of data.

Do Arbor DDoS products support GDPR compliancy?

Yes. Controllers and processors have the responsibility to implement proportionate security measures to provide a level of security appropriate to the risk to data privacy. In the case of the data processed by Arbor DDoS products, such risk is very low.

Arbor DDoS products include security features that can be configured by the customer and are designed to provide a level of security appropriate to the risk associated with the data being processed.

These features also support the principles of privacy by design and default:

- All Arbor DDoS products provide a built-in firewall to restrict access to authorized IP addresses only, which limits accessibility of data.
- All Arbor DDoS products provide authentication of users by means of a local database or by means of external TACACS/RADIUS systems, thus enabling, for example, two-factor authentication mechanisms. Local password security policies can be enforced as well.
- All Arbor DDoS products provide granular authorization mechanisms enabling system administrators to restrict access to specific product features, e.g., command line, raw flow telemetry records, or IP packets, to authorized users only.
- All Arbor DDoS products provide accounting of user actions, either locally or by means of external TACACS/RADIUS systems.

Arbor DDoS products provide other built-in capabilities which are designed to further reduce risk:

- Arbor TMS and Arbor APS can be configured to limit the amount of IP packets that can be captured per interactive capture.
- Arbor SP can be configured to limit the amount of raw flow telemetry records that are stored and set their maximum age before automatic deletion.

Is there such a thing as “GDPR compliant” products?

No. The GDPR imposes obligations on the controllers and processors of data, but it does not impose express obligations on products in and of themselves. Data controllers and processors comply with the provisions of the GDPR by implementing technical and organizational measures designed to ensure security appropriate to the level of risk associated with the type of data and type of processing they are undertaking. Arbor DDoS products include features that a data processor or data controller can implement as part of a comprehensive security plan.

Must Arbor DDoS products include pseudonymisation features?

No. The GDPR does not mandate specific security features, but rather recommends that appropriate security measures are implemented taking into account the state of the art, the costs of implementation, and the likelihood and severity of risk to the rights and freedoms of natural persons.

While data encryption, anonymization, and pseudonymisation can be useful security measures, role-based access controls also constitute appropriate security measures given the purpose of the Arbor DDoS products.

Can Arbor DDoS products help me comply with my obligations as a controller or processor?

Yes. Arbor DDoS products can help controllers and processors establish appropriate measures for the secure processing of data. The products incorporate data protection by design and default principles, such as Role Based Access Control[1] and implementation of the principle of least privilege[2].

All control plane communications between Arbor appliances, as well as administrative connections, are encrypted via secure protocols SSH and HTTPS.

All Arbor DDoS products provide a **built-in firewall** to restrict access to authorized IP addresses only.

> See: How to configure in Arbor DDoS products: `ip access commands`.

All Arbor DDoS products provide **authentication** of users by means of a local database or by means of external TACACS/RADIUS systems, thus enabling, for example, two-factor authentication mechanisms. Local password security policies can be enforced as well.

> See: How to configure in Arbor DDoS products: `service aaa local|radius|tacacs` commands.

Arbor SP enables **advanced password requirements** for locally authenticated users in order to enforce policies for stronger passwords.

> See: How to configure in Arbor SP: `service aaa password` and `service aaa local advanced harden_passwords` commands.

> See: How to configure in Arbor APS: `service aaa max_login_failures` and `password_length commands.`

All Arbor DDoS products provide granular **authorization** mechanisms enabling system administrators to restrict access to specific product features (such as the command line, raw flow telemetry records, or IP packets) to authorized users only.

> See: How to configure in Arbor DDoS products: `service aaa groups commands` (in Arbor SP's GUI, also `Administration > Accounts/Accounting > Capability Groups` and `> Account Groups)`

All Arbor DDoS products provide **accounting** of user actions, either locally or by means of external TACACS/RADIUS systems.

> See: How to configure in Arbor DDoS products: `service aaa local|radius|tacacs accounting` commands (also `Administration > Accounts/Accounting > TACACS+/RADIUS Accounting` in Arbor SP graphical user interface).

Arbor TMS and APS can be configured to limit the amount of IP packets that can be captured per interactive capture.

[1] csrc.nist.gov/Projects/Role-Based-Access-Control/faqs

[2] www.us-cert.gov/bsi/articles/knowledge/principles/least-privilege

Arbor SP can be configured to limit the amount of raw flow telemetry records that are stored and their maximum age before automatic deletion.

> See: How to configure in Arbor SP: service sp device edit <device_name> raw_flows commands.

Arbor APS provides a way to limit the age of data stored in the system.

> See: How to configure in Arbor APS's GUI: `Administration > General > Data Retention`.

Arbor APS and Arbor SP data sharing services are disabled by default, and provide examples of the type of data shared if enabled. To view the current status of data sharing services within each solution, access:

> `Administration > ATLAS Intelligence Feed in Arbor APS's GUI`, and `Administration > ATLAS > ATLAS Visibility in Arbor SP's GUI.`

Please refer to the Arbor DDoS product documentation and to your account team for additional details on these features.

With regard to the data processed by Arbor DDoS products, must I maintain, acquire or process additional information to be compliant with "data subject rights" provisions?

No. Article 11 of the GDPR states that if the purpose of the data processing does not require the identification of a data subject, then the controller isn't obligated to maintain, acquire or process additional information just to be compliant with the data subject rights provisions. Article 11 also states that if the controller is not in a position to identify the data subject, the data subject rights sections (which includes the right to be forgotten, right of access, right of portability, and right of rectification) do not apply. Recital (57) also provides guidance by stating that, "If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation."

The primary use of Arbor DDoS products is the monitoring and filtering of traffic — not the monitoring of individuals. In addition, the information that may be included in a packet capture file and stored in the Arbor DDoS products is not captured and stored in a manner that enables the product user to identify the information of a given data subject that may be contained inside the packet.

Can I still provide Arbor employees with remote access to my Arbor DDoS product for remote fault diagnosis?

Yes. Customers may provide Arbor employees with remote access to their deployed Arbor DDoS products for the purpose of fault diagnosis and technical maintenance services. Providing such access amounts to the utilization of Arbor as a processor or subprocessor. Arbor is committed to compliance with the GDPR and has implemented technical and organizational measures designed to ensure security appropriate to the level of risk associated with its processing activities.

What are the measures that Arbor has taken to be compliant with GDPR?

The measures taken by Arbor to comply with the GDPR include:

- The protection of personal data through reasonable security safeguards designed to prevent loss or unauthorized access, destruction, use, modification, or disclosure.
- Implementing robust security measures on its infrastructure (both on premise and in the cloud) such as antivirus, firewalls, scheduled vulnerability scanning, penetration testing and security code peer reviews.
- Infrastructure (both on premise and in the cloud) that is hardened against DDoS attacks and monitored 24x7x365.
- Encryption of all traffic communications on its cloud, in addition to anonymizing, pseudonymizing, or obfuscating data where technically appropriate.
- An internal process for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures designed to ensure the security of personal data processing.

As a company with offices in the United States, Arbor is aware of the need to have an export mechanism in place with customers who may provide it with data originating from the EEA. The GDPR recognizes the European Commission's Decision of 5 February 2010 on standard contractual clauses for the transfer of Personal Data to Processors established in third countries, under the Directive 95/46/EC ("Model Clauses") as an acceptable means for organizations to legalize transfers of personal data outside the EEA. To enter into data protection terms that include the Model Clauses with Arbor, visit: Arbor Data Privacy Addendum.

Disclaimer

Information provided in this document, including any comments, opinions, recommendations, answers, analysis, references, referrals or legally related content or information (collectively "Information") is intended for general informational purposes only and not to provide legal advice, and should be used only as a starting point for addressing your legal issues. The Information presented may not reflect the most current legal developments. You should always contact your legal or compliance team for advice on specific legal issues, including how the GDPR is being implemented in your region or jurisdiction.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us