Arbor Cloud and Managed Services in a GDPR Compliant Environment

This document addresses questions from organizations that use Arbor Networks Cloud and/or Managed Services offerings and are evaluating 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 purpose 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.

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 products and service include features that a data processor or data controller can implement as part of a comprehensive security plan.

What is the role of Arbor Cloud and Arbor Managed Services under the GDPR?

Under the GDPR, lawful processing of personal 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 personal 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 Cloud is an on-demand cloud-based traffic scrubbing service that defends against volumetric Distributed Denial of Service (DDoS) attacks that are too large to be mitigated by on-premise network applications. The processing performed in connection with Arbor Cloud includes the routing of network traffic to an Arbor-hosted environment, filtering out malicious traffic, and routing valid traffic to customer-owned/controlled devices. The purpose of such processing is strictly to detect and mitigate the full spectrum of DDoS attacks in order to provide network and information security and, as such, falls under the scope of lawful personal data processing under GDPR.

Arbor Managed Services is a solution that allows customers to optimize their Arbor DDoS product investment by using the services of Arbor professionals with expertise in the field of network and information security to administer and operate the solution on the customer's behalf. The type of processing performed by Arbor professionals is strictly for the purpose of monitoring the customer's network and information security and, as such, falls under the scope of lawful processing of personal data under the GDPR.

In connection with Arbor Cloud services and its Managed Service offering, Arbor requires customers to provide contact information such as email, phone number, and user name. This information is used for service and account administration (e.g., account set up, customer inquiries) and is treated by Arbor in accordance with GDPR requirements for information processed by a controller. To the extent Arbor professionals have access to personal data in connection with the Arbor Cloud or Managed Services offering, such access is based on the purchase of the service by the customer and any processing of such personal data by Arbor is in the capacity of a processor.

Is the data collected by Arbor solutions permitted under the GDPR?

Yes. Lawful processing of personal data is permitted under the GDPR. Under Recital 49 of the GDPR, the processing of personal data "to the extent strictly necessary and proportionate for the purposes of ensuring network and information security" is identified 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 and 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.

Arbor SP collects flow telemetry records, which include source and destination address, number of bytes and packets, timestamps of IP traffic flows, and other information related to network infrastructure. Arbor TMS and Arbor APS can collect full IP packets for the purpose of analyzing 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 regulation, when 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 their security features to further minimize risk associated with processing this type of data. For the security features available in Arbor DDoS products, please refer to the "Arbor DDoS Products in a GDPR Compliant Environment" document.

Can I use Arbor's Managed Services and Arbor Cloud and comply with the GDPR?

Yes. The GDPR does not prevent customers from using third parties to process information on their behalf. Rather, GDPR imposes obligations regarding security and transparency with respect to such processing. The processing for which customers use Arbor Managed Services and Arbor Cloud falls under the scope of "legitimate interest of the controller" and therefore is deemed a lawful purpose. To the extent Arbor professionals process personal data in connection with a customer's purchase of Arbor Managed Services or Arbor Cloud, Arbor understands its obligations as a processor and has implemented both technical and organization measures designed to ensure security appropriate to the level of risk associated with the processing of flow telemetry data. Please refer to the "What are the measures that Arbor has taken to be compliant with GDPR?" FAQ below for more details.

What are Arbor's obligations under the GDPR?

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 the risk to the rights and freedoms of natural persons. Controllers have the additional obligations of complying with data subject rights provisions and implementing privacy by design and default policies and procedures. Processors have obligations to assist controllers. Arbor is both a controller and a processor with respect to personal data it receives. Arbor is a controller for personal data it requests as part of its registration process or in connection with service administration. This information is typically user name, email, phone, company and potentially device identification information. With respect to personal data that Arbor receives from customers within the scope of services being provided, Arbor is a processor. Whether acting as a controller or a processor, Arbor understands its obligations under GDPR and has implemented appropriate technical and organizational measures designed to provide a level of security appropriate to the type of personal data collected and processed.

Can I use Arbor Managed Services or Arbor Cloud if my company is located in the EEA?

Yes. 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 Directive 95/46/EC ("Model Clauses"), as an acceptable means for organizations to legally transfer personal data outside the EEA. 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 personal data originating from the EEA. Arbor makes available data protection terms that include the Model Clauses to all EEA customers. Please visit: Arbor Data Privacy Addendum to download and countersign the Arbor Model Clauses.

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

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

- Protecting 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 thecloud) such as antivirus, firewalls, scheduled vulnerability scanning, penetration testing and security code peer reviews.
- Hardening infrastructure (both on premise and in the cloud) against DDoS attacks and monitoring it 24x7x365.
- Encrypting all traffic communications on its cloud, in addition to anonymizing, pseudonymizing, or obfuscating personal data where technically possible.
- Regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures of internal processes designed to ensure the security of personal data processing.

For the security features available in Arbor DDoS products, please refer to the "Arbor DDoS Products in a GDPR Compliant Environment" document.

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

SECFAQ_003_EN-1801 05/2018