

Data Protection Considerations for NETSCOUT Arbor Cloud and Managed Services

This document addresses questions from organizations that use Arbor Cloud and/or Managed Services offerings and are evaluating data protection obligations.

What Are Data Protection Obligations?

Data protection laws, for example the EU General Data Protection Regulation (GDPR) and the US California Consumer Protection Act (CCPA), regulate the “processing” — which includes the collection, storage, transfer, or use — of personal data (data privacy related terms used in this document should generally be assumed to have definitions like those in the GDPR¹). Any organization that processes personal data of individuals is likely subject to one or more data protection laws, even if the organization has no physical presence in the country or state which has enacted the law.

Data protection laws generally require, to varying degrees, that controllers and processors implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, 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. This document addresses questions regarding how the use of Arbor Cloud and Managed Services is compatible with those requirements.

Do Arbor Products Process Personal Data?

Yes. Arbor products collect network flow records (metadata about network traffic flows traversing a network device such as a router, switch, or host, and which are not individual packets) which include, for example, source and destination address, number of bytes and packets and timestamps of IP traffic flows, as well as other information related to network infrastructure. When performing Distributed Denial of Service (DDoS) attack mitigation, Arbor products collect and process individual packets that travel through the network (IP packets). Some of the information contained in network flow records and IP packets falls under the scope of personal data due to how broadly the term can be defined.

¹ E.g., Personal data, data subject, controller, and processor.

What is the Role of Arbor Cloud and Arbor Managed Services and is it “Legitimate Use”?

Arbor Cloud is an on-demand cloud-based traffic scrubbing service that defends against volumetric Distributed Denial of Service (DDoS) attacks which 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 networks and devices. The purpose of such processing is strictly to detect and mitigate DDoS attacks in order to provide network and information security. This is a vital objective for today's enterprises and service providers, and qualifies as legitimate use under data protection laws.

Arbor Managed Services (AMS) provides access to Arbor professionals with expertise in the field of network and information security who administer and operate Arbor products on the customer's behalf. AMS enables customers to optimize their Arbor DDoS product investment. The type of processing performed as part of AMS 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.

Do Data Protection Laws Prohibit the Use of Arbor Managed Services or Arbor Cloud?

No. Data protection laws do not prevent customers from using third parties to process information on their behalf. Rather, these laws impose obligations regarding security and transparency with respect to such processing. The processing for which customers use Arbor Managed Services and Arbor Cloud generally falls under the scope of being a legitimate interest of the data 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, NETSCOUT® understands its obligations as a processor and has implemented both technical and organizational measures designed to ensure security appropriate to the level of risk associated with providing these services. Refer to the FAQ below, “What Measures Has NETSCOUT Taken To Be Compliant With Data Protection Laws,” for more details.

What Measures Has NETSCOUT Taken To Be Compliant With Data Protection Laws?

The measures taken by NETSCOUT to comply with different data protection laws include:

- The protection of personal data through reasonable security safeguards designed to prevent loss or unauthorized access, destruction, use, modification, or disclosure.
- Implementation of robust security measures on its infrastructure (both on premise and in the cloud) such as antivirus applications, 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.

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 data protection laws are implemented in your region or jurisdiction.



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