nGenius Products in a GDPR Compliant Environment

This document addresses questions from organizations that use nGenius® Smart Data Core™ platform and application 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 nGenius products permitted?

Yes. Under the GDPR, only 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." The determination of whether certain processing does or does not fall under the scope of "legitimate use" is based on analyzing whether the interests of the controller in conducting the processing of personal data does or does not outweigh the rights and freedoms of the individuals whose personal data is processed.

The nGenius product suite consists of Smart Data Core platform products and application products. The Smart Data Core platform products consist of the nGenius Infinistream solution for on-premise environments, and vSCOUT and vSTREAM for virtual environments. The Smart Data Core application products are nGeniusONE, nGenius Business Analytics, nGenius Subscriber Intelligence and nGenius Session Analyzer. nGenius products are designed for real time contextual analysis of service, network and application performance that provides customers full visibility into their networks and applications, thus allowing them to run at their optimum performance without disruption. The need to ensure the health and availability of the network and diverse application environments, as well as to identify server issues, security breaches, and other significant service delivery problems are vital objectives of enterprises today. While personal data may be captured and stored by customers using the nGenius products, such information is incidental to the purpose of such capture and storage and furthermore can be limited in terms of access, type and scope by using certain product features.

Is the data collected by nGenius products permitted under the GDPR?

Yes. The nGenius products collect and analyze packets on a network (IP packets), which include data such as 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 connected to a Wireless Service Provider's network, the nGenius products also collect information such as MSISDN, IMSI and other information for analyzing network performance. While information contained in IP packets falls under the scope of personal data due to how broadly the term is defined under the GDPR, the GDPR also sets forth the principles that some types of personal data is less sensitive than others and certain types of processing presents a lesser risk to the rights and freedoms of individuals than others. When the nGenius products are configured to optimize existing security features and are used for the purpose of network and application analysis, the level of risk presented by such processing is low. For example, information such as MSISDNs, which may be considered more sensitive than other data types, can be masked and access severely restricted to specific authorized users. To learn more about security features available on the nGenius products, please visit my.netscout.com/mcp/security or contact your NETSCOUT account team for additional details.

Do nGenius products support GDPR compliancy?

Yes. Under the GDPR, controllers and processors have the responsibility to implement proportionate security measures to provide a level of security appropriate to the risk to data privacy. The nGenius 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], and include security features that can be configured by the customer that are designed to provide a level of security appropriate to the risk associated with the data being processed, including:

- All nGenius products provide authentication of users and accounting of user actions by means of a local database or by means of external TACACS/RADIUS systems. Local password security policies can be enforced as well.
- All nGenius 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 nGenius platform hardware is shipped with robust hardened hardware and Operating Systems. The products also have built in access control features to prevent unauthorized access to packets.
- All nGenius applications are designed to limit access to certain monitors that display data and/or mask sensitive data based on user privileges.
- All control plane communications between nGenius products, as well as administrative connections, are encrypted via secure protocols SSH and HTTPS
- nGenius applications enable advanced password requirements for locally authenticated users in order to enforce policies for stronger passwords.
- nGenius applications provide a way to limit the age of data stored in the system.
- nGenius products provide other built-in capabilities which are designed to further reduce risk such as:
  - Ability to limit the number of bytes in an IP packet that can be captured so that only header information is captured.
  - Ability to aggregate packet data into metadata by communities rather than individuals, thus minimizing identification of personal data accessible by users with limited privileges.
- NETSCOUT's patented Adaptive Session Trace (AST) technology uses a proprietary dynamic slicing technology that reduces the data captured in packets before storing them, so that only information required for network monitoring is captured. Administrators can override this default functionality in order to capture more information in network packets.

For details on how to optimize the security features of your existing nGenius solution investment, visit my.netscout.com/mcp/security or contact your NETSCOUT account team for additional information.

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

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

Can I share traffic data such as CAP and PCAP files with NETSCOUT under GDPR provisions?

Yes. Under the GDPR, controllers may share personal data with processors with whom they have a contract which sets forth the subject-matter and duration of processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. In the scope of contracted services, such as maintenance, professional, or managed services, customers may provide traffic data such as CAP and PCAP files to NETSCOUT for the purpose of enabling NETSCOUT to resolve and/or optimize performance of NETSCOUT solutions, or for the purpose of enabling NETSCOUT to perform service assurance services on behalf of the customer. Providing such data to NETSCOUT in the context of these types of services amounts to utilizing NETSCOUT as a processor or subprocessor. NETSCOUT 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.

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

Do nGenius products include pseudonymisation features?

Yes, where appropriate. 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. Where appropriate, for example in the case of MSISDN numbers, the nGenius products can be configured to apply masking measures designed to ensure that users with limited privileges are not presented with sensitive data. 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 nGenius products.

With regard to the data processed by nGenius 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 is not 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 nGenius products is for the monitoring and analysis of traffic to ensure high levels of availability and performance of applications running on the user’s network — not the monitoring of individuals.

Can I still provide NETSCOUT employees with remote access to my nGenius product for remote fault diagnosis?

Yes. Customers may provide NETSCOUT employees with remote access to their deployed nGenius products for the purpose of fault diagnosis and technical maintenance services. Providing such access amounts to the utilization of NETSCOUT as a processor or subprocessor. NETSCOUT 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 NETSCOUT has taken to be compliant with GDPR?

The measures taken by NETSCOUT 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, NETSCOUT 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 NETSCOUT, visit: NETSCOUT 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