

Is Your Organization Ready for GDPR?

GDPR Checklist for Enterprise

Arbor Enterprise Network Security Solutions Can Help

The General Data Protection Regulation (GDPR) calls for unprecedented changes in the way organizations collect, process and protect the personal data of EU citizens. The GDPR requirements are not limited to organizations physically located in the EU. In fact the regulations highlight requirements for protecting the flow of personal data across borders. And for the first time, the GDPR explicitly applies to any business collecting or processing personal data, whether directly, or indirectly as a third-party.

For security operations GDPR Recital 49 defines the appropriateness of processing personal data within security solutions for the purposes of “ensuring network and information security.” It goes further: “This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.” Arbor solutions help ensure your networks are available and protected against advanced attacks targeting personal data. The checklist below can help you assess your preparedness for GDPR.

GDPR Section 2: Security of personal data, Article 32: Security of processing

For the security professional, Article 32 goes to the “heart of GDPR” — the requirements called for in the protection of personal data.

Article 32 calls for:

- “The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;” (Article 32: 1(b))
- “The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;” (Article 32: 1(c))
- “A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.” (Article 32: 1(d))

Check for these vulnerabilities in your network security posture:	Arbor DDoS Protection Solution provides:
<ul style="list-style-type: none"> ✓ Relying exclusively on stateful devices x(load balancers, firewalls, IPSs) which are vulnerable to state exhaustion DDoS attacks 	An intelligently automated, layered, fully managed combination of on-premise and in-cloud DDoS attack protection
<ul style="list-style-type: none"> ✓ Cannot protect your connection to the Internet from saturation due to volumetric DDoS attacks 	Automatic countermeasures to stop all types of DDoS attacks (volumetric, TCP state exhaustion, “lo and slow” application layer) and other advanced threats — both inbound and outbound
<ul style="list-style-type: none"> ✓ Inability of many cloud service providers to detect stealthy “low and slow” application layer and multi-vector DDoS attacks that crash servers 	Arbor Cloud Signaling™ that intelligently and automatically connects local DDoS protection with Arbor Cloud DDoS Protection Services for volumetric mitigation
<ul style="list-style-type: none"> ✓ Inefficient and no-automated DDoS mitigation due to time lost communicating and coordinating with cloud service providers during attacks 	Multiple Tbps of global in-cloud mitigation; SOC staffed 24/7 with industry leading DDoS protection experts
<ul style="list-style-type: none"> ✓ Outdated DDoS protection because you can't easily update your threat intelligence and DDoS policies 	<ul style="list-style-type: none"> • A wide range of mitigation platforms and capacities: from 2U appliances (1 Gbps-160 Gbps) to virtual software (sub 1Gbps) to multiple Tbps of global Arbor Cloud • Unified DDoS attack protection for hybrid cloud environments (i.e. combination of on-premise and Amazon Web Services) • In-box SSL decryption capabilities to identify threats hidden in encrypted traffic • ATLAS Intelligence Feed (AIF): continuously updated DDoS protection with the latest global threat intelligence from Arbor's Security Engineering & Response Team (ASERT)



GDPR Section 2: Security of personal data, Article 33. Notification of a personal data breach to the supervisory authority

GDPR notification requires:

- In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority... (Article 33: 1).
- The degree of compliance can affect the level of financial penalties. The Supervisory Authority takes "...into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;" (Article 83: 2 (d)) and "the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;" (Article 83: 2 (h)).

Check for these vulnerabilities in your network security posture:	Arbor Spectrum provides:
✓ Relying on perimeter protection to detect and block data breaches from complex/stealthy advanced threats	Provides streamlined security workflows to detect and investigate network-wide threat activity faster than traditional solutions
✓ Inability to detect a data breach in real-time. Limitations on analyzing massive amounts of log data; sidetracked by "false positives"	Real-time visualization of Indicators of Compromise (IoC) of trends in new indicators and network activity
✓ No visibility into the full extent of a data breach	Identification of cyber threats for all impacted hosts and network connections to gain visibility into the full extent of a data breach
✓ Difficult to correlate past activity with current breach	Workflow for investigation of past breach activity from full packet-level network archive
✓ Lack of global threat context to help prioritize security resources to respond to breaches	Detection based on ATLAS Intelligence Feed's Internet threat visibility and high fidelity attack campaign indicators applied to your internal network activity

GDPR Section 1: General obligations, Article 25. Data protection by design and by default

"By design and by default" attempts to enforce security planning from the ground up, in the planning of your security systems and procedures. You are required to:

- "...implement appropriate technical and organisational measures ...which are designed to implement data-protection principles ...in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects." (Article 25: 1).

Check for these vulnerabilities in your network security posture:	By design, Arbor solutions provide:
✓ Reliance on manual and event-specific security processes against DDoS and advanced attacks	Automation of policies and processes such that, by default, data protection against DDoS and advanced threats, is built in, e.g., <ul style="list-style-type: none"> • Automatic detection and mitigation of attacks • Key incident response and security operations workflows • Integrated on-premise and cloud DDoS protection
✓ Lack of global threat context to help prioritize security resources to respond to breaches	Embedded, continuously updated ATLAS global threat intelligence for the context you need for a proactive security posture against DDoS and advanced threats
✓ Reactive rather than a proactive tools for what threats might come next	



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