

Gigamon Helps Organizations Address the GDPR

The European Union's (EU) **General Data Protection Regulation** (GDPR) provides incentives to companies around the world to secure and take control of their data and networks. Starting on May 25, 2018, the regulation's substantial penalties apply to organizations that violate its provisions for handling and protecting EU resident's data — even those based elsewhere.

If you do business online, you're almost certainly affected. Fortunately, you have a great resource to help you understand the new regulatory environment: Gigamon. Under the GDPR framework, network visibility and data control will become more important than ever. Let's take a closer look.

The GDPR: A Big Deal for Everyone

The GDPR is a complex regulation, but its overall purpose is to provide individuals with more control over the personal data that companies retain and quick notification if that data has been compromised. It applies to anyone doing business with citizens of the European Union — and in today's distributed world, that's just about everyone. Among other things, the GDPR mandates:

- That EU citizens have the right to access data about them retained by companies and the right to request that this data be deleted.
- That organizations only store and process data about EU citizens to the minimum extent required to achieve their legitimate goals.
- That regulators be informed within 72 hours if there is a data breach affecting EU citizens.

For a deeper dive, check out www.gigamon.com/GDPR

Gigamon and GDPR Compliance

Here are some ways Gigamon solutions can help you comply:

- Gigamon packet slicing and data masking tools prevent the widespread sharing of personal data that can leave you vulnerable.
- Gigamon gives you visibility into data and applications, both within your own networks and on private or hybrid clouds. That visibility is crucial for detecting and preventing the kinds of breaches that need to be reported to regulators.
- As you beef up your security to meet the GDPR's requirements, Gigamon can bring order to your sprawling security toolsets, allowing your tools to conserve resources by focusing only on the most relevant network packets. For instance, a data loss protection tool doesn't need to analyze streaming video traffic and Gigamon will prune out those packets.

10 ways GigaSECURE helps address key GDPR requirements:

1. Provides full data access of network traffic in any environment – cloud, on-premises or virtual – to improve threat detection and mitigation.
2. Enables tool deployment into private and public cloud environments for elastic scaling of risk-analysis capabilities.
3. Connects multiple, different tools to the same traffic streams, without affecting reliability or performance.
4. Connects slower tools – both inline and out-of-band – to faster networks.
5. Decrypts and re-encrypts SSL/TLS traffic to decrease the processing load on security tools.
6. Enables quick and easy deployment of tools, such as anti-malware and intrusion prevention system (IPS) devices, at both the network edge and core – a critical capability in a data-risk-centric network.
7. Enables all current tools – not only at the edge, but also at the core – to see all data.⁵
8. Enables deployment of information-risk centric technologies, and is not solely focused on external threats. For example, User Behavioural Analytics (UBA) tools can seek to identify and distinguish legitimate user activity from an intruder misusing a stolen credential or a blackmailed employee initiating an insider threat.
9. Facilitates building a data-risk-centric InfoSec infrastructure with tools like Data Loss Prevention (DLP), File Access Monitoring (FAM) and Database Access Monitoring (DAM).
10. Enables the use of Document Management Systems and well-structured storage to help ensure knowledge of where data lives and how it is used.

For more information, please visit www.gigamon.com/GDPR