Preparing Your Network for GDPR: Answers to Key Questions

FAQ

INTRODUCTION

Work is underway at enterprises in Europe and beyond to prepare for the European Commission's General Data Protection Regulation (GDPR), going into effect next year on May 25, 2018. GDPR will impact all organizations that either conduct business in the European Union (EU), offer goods or services to residents of the EU, or monitor the online behavior of EU residents. That means nearly every global enterprise. The regulation affirms the duty of organizations to protect the personal data of EU citizens and give them more control over how that data is handled. One big change is that firms that process personal data are now responsible for protecting privacy, just as firms that collect and use the data.

GDPR is a multi-faceted regulation that affects IT infrastructure, processes, and people. No single vendor or solution provides the entire answer. But it is clear that strengthening network security and preventing data loss are key to compliance, and those are issues Ixia knows something about. This document provides a summary of information on GDPR for those making decisions about network and application security and performance monitoring, in a question-and-answer format.

ixia
A Keysight Business

Q: AT A HIGH-LEVEL, WHAT IS THE GENERAL DATA PROTECTION REGULATION (GDPR)?

A: GDPR, derived from the data protection reform first proposed in 2012 and adopted by European Union (EU) member nations on 24 May 2016, mandates new rules and practices for strengthening data protection and maintaining data privacy for individuals living within the EU. The regulation places equal responsibility for data security on both "data controllers" that collect and use personal data, and "data processors" that manipulate data on behalf of the controllers.

Q: WHAT IS "PERSONAL DATA," ACCORDING TO GDPR?

A: Personal data is any information related to a natural person or "data subject" that can be used to directly or indirectly identify the person. This includes anything ranging from a person's name, photo, email address, or static Internet Protocol (IP) address, to bank account information, posts on social network sites, or medical information.

Q: WHAT IS A "DATA CONTROLLER" AND A "DATA PROCESSOR," ACCORDING TO GDPR?

A: Data controllers are entities or persons that decide on the conditions, purposes, and means in which personal data is processed. Examples are doctors, politicians, government agencies, and social networking sites. Data processors are entities or persons that process data under the direction of a data controller, but do not make decisions on the conditions, purposes, and means of data collection. Examples are payroll processing companies, data storage providers, or hosting providers.

Q: WHICH PARTS OF GDPR REGULATION ARE MOST RELEVANT TO NETWORK ADMINISTRATORS AND SECURITY MANAGERS?

A: GDPR regulation consists of 99 articles that require legal assistance to decipher completely. However, certain articles are specifically relevant to protecting the security of personal data and violations are associated with severe fines.[1]

- **Article 25 Data Protection by Design**: limits amount of data managed and access to it
- **Article 32, Security of Processing**: governs the implementation of data security measures (such as encryption) and verification of their operation
- **Article 33, Breach Notification to Regulators**: requires notification to regulators within 72 hours of becoming aware of most breaches
- **Article 34, Breach Notification to Individuals**: requires notification to individuals affected by any breach that could result in high risk to personal rights or freedoms, unless data was protected in a way that made it unintelligible
- **Article 35, Data Protection Impact Assessment**: requires organizations to analyze the risk of certain processing activities
- **Article 44, General Principal for Transfers**: prevents unauthorized data transfers outside member states

[1] Imperva: "Get Going with your GDPR Plan," 23 March 2017 ".

Q: WHO IS IMPACTED BY THE GDPR?

A: GDPR directly affects organizations that conduct business in the EU, offer goods or services to residents of the EU, or monitor the behavior of EU residents. For companies operating globally, GDPR will be relevant, regardless of where the company is based. The situation is similar to US data protection laws, where a company based in any country doing business with customers in California must comply with California's data protection laws.

Q: DOES "BREXIT" EXEMPT ENTITIES CONTROLLING OR PROCESSING DATA IN THE UK?

A: If a UK company processes data related to individuals in other EU countries, it will still need to comply with GDPR irrespective of Brexit. However, even if a company's business is limited to only the UK, the UK Government has indicated it will implement an equivalent or alternative legal mechanism to GDPR. At the current time, GDPR provides the best baseline for how such a future requirement would be structured.[2]

Q: ARE DATA PROCESSORS, WHO ONLY ACT FOR THE BENEFIT OF CONTROLLERS, ALSO SUBJECT TO GDPR LEGAL SANCTIONS?

A: Yes, this is a significant change from the previous policies of the European Commission. For the first time, GDPR places specific obligations on data processors to comply with the core principles and mandates of data protection and individual data privacy.

Q: WHY HAS GDPR BEEN ADOPTED IN THE EU?

A: First put forward in 2012, data protection reforms were intended to modernize data handling for the digital age and to:

- Address concerns European citizens have about giving out personal data online, by giving them more control to restrict or eliminate access
- Enable better cooperation between law enforcement authorities
- Ensure fast action when breaches do occur to help people protect themselves
- Boost economic growth and encourage the flow of data between member nations through the application and enforcement of consistent rules

Q: WHAT ARE THE EXPECTED BENEFITS OF GDPR TO INDIVIDUAL CITIZENS?

A: GDPR acknowledges the fundamental right of all EU citizens to data protection. New rules strengthen existing rights and give individuals more control over their data. Most notably these rights include:

- Easier access to your own data
- Right to data portability (transfer between service providers)
- "Right to be forgotten" when you no longer want your data to be processed, provided there is no legitimate reason for retaining it
- Right to know if your data has been hacked

[2] http://www.eugdpr.org/gdpr-faqs.html

Q: WHAT ARE THE EXPECTED BENEFITS OF GDPR FOR BUSINESS AND COMMERCE?

A: Another key goal of GDPR is to stimulate economic growth by cutting the costs and red tape associated with data handling in the multi-state European market, particularly for opportunities associated with big data. These benefits include:

- One set of rules to make it simpler and cheaper to do business in the EU, hopefully making it easier for small and medium enterprises to break into new markets
- Risk-based approach to rules to avoid burdensome one-size-fits-all obligations
- Encouragement for security being designed into new products

Q: WHEN DOES GDPR GO INTO EFFECT? WHEN WILL ENFORCEMENT OF NON-COMPLIANCE BEGIN?

A: The GDPR regulation was approved by the EU Parliament on 14 April 2016 and gave countries up to 2 years to implement and begin enforcing the new requirements.[3] Some countries, such as the Netherlands, have already made the transition and approved changes to their data protection laws. Enforcement officially begins on 25 MAY 2018, but each country has some discretion over how to regulate its region.

Q: WHAT IS THE ROLE OF "SUPERVISORY AUTHORITIES (SAs)," ACCORDING TO GDPR?

A: SAs referred to in the GDPR will monitor the application of GDPR rules to protect individual rights with respect to the processing and transfer of personal data within the EU. Existing national data protection authorities may assume the role. SAs are expected to act with complete independence and stay free from external influence. They must co-operate with each other and the European Commission.

Q: WHAT ARE THE COSTS ASSOCIATED WITH NON-COMPLIANCE?

A: For many years, data protection authorities in EU member states advocated for stiffer, more consistent penalties, particularly where data crosses national boundaries and is not protected with the same standards as the state in which it originated. Moving forward, Article 83 establishes a two-tier system of fines with an extensive list of specific offences that qualify for maximum fines. While national regulators will have some discretion over the specific fines levied, it is probably safe to say the maximum fine will be more severe than under the current regulations.[4] Currently, for example, the UK Information Commissioner's Office can only implement up to a 500,000 GPB fine.[5]

- **Severity Level 1 monetary fine**: Failure to adhere to the core principles of GDPR with respect to data processing, infringement of personal rights, or transfer of personal data are the most severe and subject to a maximum potential fine of up to 20M Euros or 4% of total worldwide turnover/revenue, whichever is higher.

[3] European Parliament: "New EU rules on data protection put the citizen back in the driver's seat," 17 Dec 2015.

[4] TaylorWessing International Data Protection and Information Law Group: "The cost of (non-)compliance," October 2015.

[5] SOPHOS white paper: "The EU General Data Protection Regulation," February 2017.

- **Severity Level 2 monetary fine**: Failure to comply with the technical and organizational requirements of GDPR (such as appointment of a Data Protection Officer or completion of an impact assessment) is subject to a maximum potential fine of up to 10M Euros or 2% of turnover/revenue, whichever is higher.
- **Business risks**: Other potential costs are those arising from security incidents, including loss of customer confidence or satisfaction, decline in revenues, decline in market share, negative press, or the risk of legal action from individuals harmed by breaches.

Q: HOW WILL FINES BE DETERMINED AND ENFORCED?

A: Although the intent was to standardize business processes regarding data protection, the final version of the regulation gives member states individual discretion to determine sanctions for infringement of GDPR. The designated SAs have the power to issue substantial administrative fines which should be "effective, proportionate and dissuasive." While some SAs may turn out to be more proactive than others, penalties are expected to be greater than they are currently.[6]

Q: WHICH CYBERSECURITY TECHNOLOGIES DOES THE GDPR REQUIRE COMPANIES TO IMPLEMENT?

A: GDPR purposely avoids mandating specific technologies to prevent breaches and protect private data, out of recognition that information technology security evolves quickly. Instead, organizations are expected to take into account current technologies and best practices in designing their processes and procedures. In any post-breach investigation, a company will likely have to defend its approach to security and privacy protection and the technologies it chooses to deploy. For that reason, organizations should carefully assess, evaluate, and document their decisions, particularly:

- Who in the company is accountable and responsible for achieving compliance
- What the company's strategy is for security and who advised the company in creating that strategy
- What the plan and timeframe were for reaching compliance
- How compliance was validated
- How compliance will be maintained and measured

Q: WHAT DOES ENHANCING NETWORK VISIBILITY HAVE TO DO WITH GDPR?

A: One of the foundations of IT security is being able to see all of the traffic moving through your network(s). Network blind spots are commonly used as a foothold for malicious malware and can lead to a data breach and exposure of personal data. The best visibility architectures reduce the opportunities for malware, botnets, and other attacks to get a foothold. Some common weaknesses in network visibility are:

[6] TaylorWessing International Data Protection and Information Law Group: "Enforcement and sanctions under the GDPR," April 2016.

- **Virtual and cloud-based traffic**: Virtual and cloud-based traffic needs to have the same level of inspection and analysis as traffic between traditional physical devices. You need a visibility architecture with the ability to see inside these environments and inspect communications for threats.
- **Dropped packets**: You also need to make sure your visibility engine is strong enough to process growing volumes of traffic at sufficient speed and without dropping any packets. Overloaded engines that drop packets or become congested when running multiple filters can create blind spots and vulnerabilities.
- **Inefficient use of inspection and monitoring tools**: An engine with the ability to filter packets by user, device, application, or geolocation can help tools work more efficiently by sending them only the data they are designed to monitor. With greater efficiency, your existing infrastructure can process more traffic, leaving you more budget to spend on advanced deep packet inspection tools.
- **Not planning for downtime**: Security infrastructure is great when it is working but you need to consider what happens if you suffer a failure in a system, software, link, or power supply. Keep your security defenses strong with a visibility architecture that can automatically shift traffic to backup tools and maintain full inspection and analysis.
- **Being overwhelmed by security alerts**: The IT staff can be overwhelmed following up on all the alerts issued by firewalls and intrusion prevention systems. To overcome this issue, some companies are deploying special-purpose filters to block all communications with IP sites associated with threats and attacks and to reduce the number of alerts.

Q: WE ALREADY HAVE BREACH PREVENTION AND DETECTION IN PLACE; IS THAT ENOUGH?

A: Breach detection is an important part of GDPR compliance, but the new regulation also has a strong emphasis on protecting individual rights in a digital world where personal data is easily shared and transferred without the specific consent or knowledge of the person it relates to. In order to comply with those aspects of GDPR, you will need to have policies to assess risk, demonstrate compliance, document action taken, offer individuals control over their data, and enable timely notification of any persons whose data is compromised.

Q: WHAT ARE SOME OF THE WAYS IXIA CUSTOMERS ARE PREPARING FOR GDPR?

A: Planning and executing a strategy to achieve GDPR compliance is multi-faceted and spans beyond what Ixia, alone, provides. However, the following are typical projects where we can assist companies in their preparation for GDPR:

- **Achieving visibility in the cloud**: Ixia provides cloud-native access of traffic in both private cloud and public cloud environments. Ixia CloudLens uniquely filters and processes packets at the source, to eliminate the need to transmit packets back to a centralized monitoring location. The architecture supports greater scalability, network agility, and security. Find out more at CloudLens Public and CloudLens Private.
- **Monitoring encrypted traffic**: The key to using data encryption is to not let it lull you into a false sense of security, as cyberattacks are frequently embedded in encrypted traffic. It is vitally important to decode and inspect encrypted traffic. Ixia's high-performance visibility engine provides visibility to encrypted traffic without compromising security using role-based controls and bidirectional decryption capability. Learn more at Visibility Features: SecureStack-SSL Decryption.

- **Identifying and masking personal data**: Ixia first developed this feature to secure "personally identifiable information" (PII) such as credit card and social security numbers in data sent to monitoring and analysis tools, but it is also ideal for GDRP purposes. Administrators can obscure any data pattern they choose with an easy-to-use graphical interface or use Ixia's pre-defined templates. Find out more at Visibility Features: PacketStack-Data Masking.

- **Testing security infrastructure**: In addition to achieving visibility, organizations should validate that their network infrastructure is robust and defends against breaches. Ixia test solutions help ensure correct implementations and configurations and simulate network traffic at high volume, that includes personal data, as well as malware and other threats. Find out more at BreakingPoint.

- **Deploying resilient security solutions**: Ixia's resilient security solutions ensure you'll still be protected if your security infrastructure suffers a temporary outage or you need to take a device offline for upgrade or maintenance. Ixia's high-performance packet processors are uniquely able to share the workload and provide near-instant recovery in the event of a failure. Find out more at Security Resilience.

- **Integrating real-time application and threat intelligence**: Pre-filtering known bad IP addresses and traffic out of the data that flows to your security solutions will enhance the performance of your tools and reduce the number of alerts the security team needs to follow up on. Find out more at ThreatARMOR™.

Disclaimer: This information is not legal advice nor is it a comprehensive review of the GDPR. The GDPR is complicated data protection regulation and you should consult your own legal advisors as required.

IXIA WORLDWIDE

26601 W. Agoura Road
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800

(Fax) 1.818.871.1805

www.ixiacom.com

IXIA EUROPE

Clarion House, Norreys Drive
Maidenhead SL64FL
United Kingdom

Sales +44.1628.408750
(Fax) +44.1628.639916

IXIA ASIA PACIFIC

101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
(Fax) +65.6332.0127