RAPID7

SOLUTION GUIDE

GDPR Compliance: How Rapid7 Can Help

Learn how Rapid7 solutions and services can help your organization prepare and comply with the EU General Data Protection Regulation (GDPR).

The General Data Protection Regulation (GDPR) protects the personal data of EU citizens regardless of the geographical location of the organization or the data. Organizations around the world must be compliant with GDPR by 25th May 2018. Changes to people, processes and technology are required to ensure that personal data is correctly controlled, processed, maintained, retained and secured. Penalties for infringement of the General Data Protection Regulation can be up to €20,000,000 or 4% of worldwide annual turnover, whichever is the greater amount.

Security is just one aspect of GDPR compliance, and we recognize that you will need to engage with multiple vendors plus conduct a host of assessments and process reviews in order to fully cover all requirements. If you haven't already done so, engaging with a partner is strongly recommended.

HERE'S HOW RAPID7 HELPS YOU PREPARE AND COMPLY WITH THE GENERAL DATA PROTECTION REGULATION

Article 32 – Requirement for controllers and processors to implement a level of security appropriate to the risk

Vulnerabilities and risk go hand-in-hand. Securing assets, and their surrounding eco-system, that handle and process Personal Data is an important step in any security program. Ensuring you have the right technology and processes in place to collect the right data and prioritize based on risk will help you drive your remediation efforts. GDPR stipulates that organizations ensure ongoing confidentiality, integrity, and availability of systems – wording which ties back to Microsoft's description of a security vulnerability: "A security vulnerability is a weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product.".

- **Know your network and identify weak points.**

  Use Nexpose to conduct a thorough vulnerability assessment of risks across vulnerabilities, configurations, and controls, and prioritize risks for remediation based on threat exposure and business impact. Automatically audit your systems for compliance with secure configurations, password policies, and access control requirements.

- **Assess applications for vulnerabilities.**

  Web application attacks are the #1 source of data breaches. Use AppSpider, our Dynamic Application Security Testing solution, to dynamically scan your web, mobile, and cloud applications for vulnerabilities (including those that allow unauthorized persons to bypass authentication controls), and generate interactive reports for remediation.

- **Short of resources and time? Managed services are an ideal solution.**

  Rapid7 have managed offerings for both vulnerability management and application security, providing you with the security benefits but without the burden of operational overhead. Just think of our experts as an extension of your team.

- **Have a process for regularly testing, assessing, & evaluating the effectiveness of security measures.**

  Simulate real-world attacks by penetration testing your defenses and evaluate the effectiveness of security measures at protecting personal data with Metasploit. Closed-loop integration of Metasploit with Nexpose enables you to validate the exploitability of vulnerabilities in Metasploit and automatically prioritize for remediation in Nexpose.

Articles 33 and 34 – Notification of breaches

Personal Data Breaches have already proved costly for organizations who experienced them first hand. According to IBM and Ponemon, the average consolidated cost of a breach in 2016 was $4 million. The General Data Protection Regulation requires Data Controllers to report breaches to a Supervisory Authority within 72 hours of discovery, however it is an all to frequent occurrence for breaches to go undetected for months. Implementing a relevant breach notification process will tick a compliance box, but this alone will not change your security posture, or help you mitigate damage in the unfortunate event of a breach.

- **Look through the eyes of an attacker.**

  Penetration testing services give you an attacker's perspective of your eco-system, providing you with an understanding of how and where you are most vulnerable to security breaches and data exfiltration.

- **Develop a top-notch Incident Response Program.**

  Rapid7's Incident Response Program Development service will help you determine the people, process, and technology necessary to ensure your organization can move with speed and purpose in the event of an incident.

- **Monitor user behavior, detect attackers earlier, and investigate security incidents faster.**

  InsightIDR provides the ability to tag systems containing personal data as "restricted," then monitors all activity on these systems for unauthorized access. Leverage user behavior analytics to detect security incidents and accelerate investigations with instant user context, endpoint interrogation, and advanced search capabilities.

- **Incident Response that doesn't sleep.**

  Don't have in-house 24x7x365 incident response capabilities? No problem. Rapid7's Managed Detection and Response service can provide you with round-the-clock monitoring and incident response assistance. Early detection results in faster mitigation, which could make the difference between needing to report a data breach and having the ability to prevent attackers from reaching highly-coveted personal data.

Penalties can be up to €20,000,000 or 4% of gross worldwide revenue for previous year, whichever is higher.

We're here to help

If you're looking for help with your GDPR security preparations please visit www.rapid7.com/gdpr for more information or email us at info@rapid7.com.