RAPID7

EU GENERAL DATA PROTECTION REGULATION (GDPR):

10 THINGS TO HELP SECURITY TEAMS PREPARE

The EU GDPR is one of the biggest changes in data privacy regulations. Here is what Security Teams need to know before the changes are enforced on May 28, 2018.

EU GENERAL DATA PROTECTION REGULATION (GDPR): 10 THINGS TO HELP SECURITY TEAMS PREPARE

The General Data Protection Regulation (GDPR) regulates the privacy and handling of European Union (EU) citizens' personal data. GDPR replaces the existing EU Data Protection Directive, and unifies data protection laws across the EU with a single set of rules. Securing, monitoring and protecting the systems and applications that process and store personal data are key to GDPR compliance, and security teams and incident responders all have a part to play.

1. Pen tests are your friend. If you've never had one done, or it's been a while, this is a great place to start when preparing for GDPR. Attacking your systems and environment to understand your weak spots will tell you where you need to focus, and it's better to go through this exercise as a real-world scenario now than wait for a "real" attacker to get into your systems. You could do this internally using tools like Metasploit Pro, and you could employ a professional team to perform regular external penetration testing services as well. Article 32 says that you need to have a process for regularly testing, assessing, and evaluating the effectiveness of security measures. Read more about penetration testing in this toolkit.

2. Encrypt data, both at rest and in transit. If you are breached, but the Personal Data is in a render unintelligible to the attacker, then you do not have to notify the Data Subjects (see Article 34 for more on this). There are a lot of solutions on the market today—have a chat with your channel partner to see what options are best for you.

3. Have a solid vulnerability management process in place, across the entire ecosystem. If you're looking for best practice recommendations, take a look at our blog post. Ensuring ongoing confidentiality, integrity, and availability of systems is part of Article 32. If you read Microsoft's definition of a software vulnerability it talks to these three aspects.

4. Backups. Backups. Backups. Please take backups. Not just in case of a dreaded ransomware attack, but because they are a good housekeeping facet in case of things like storage failure, asset loss, natural disaster, even a full cup of coffee over the laptop. If you don't currently have a backup vendor in place, Code42 has some great offerings for endpoints, and there are a plethora of server and database options available on the market today. Disaster recovery should always be high on your list regardless of which regulations you are required to meet.

5. Secure your web applications. Privacy-by-design needs to be built into processes and systems; if you're collecting Personal Data via a web app and still using http/cleartext, then you're already going to have a problem. The latest General Data Protection Regulations require you to make code changes to your web forms and applications, so this is a good moment to ensure your SDLC is baking in security early in the cycle so you can find and fix issues faster.

6. GDPR standardises Personal Data Breach Reporting requirements, so now is a good time to review and update your Incident Response processes. If you need help setting up your incident response program, or you'd like to have a second pair of eyes review what you have today, we'd be happy to help. And if you are unlucky enough to find yourself in a potential breach situation, it's vital to engage with an incident response team. Accelerating containment and limiting damage requires fast action. Rapid7 can have an incident response engagement manager on the phone with you within an hour.

7. Detect attackers quickly and early. Finding out that you've been breached 5 months after the fact is an all too common scenario (current stats from Mandiant say that the average is 146 days after the event). If you don't know you're under attack, then you have no ability to mitigate damage. If you're in the same situation as the 60% of organisations that told us they have no way of detecting compromised credentials (which has topped the list of leading attack vectors in the Verizon DBIR for the last few years), you're more likely to find out way too late that an attacker was hiding in plain sight. User Behaviour Analytics provide you with the capabilities to detect anomalous user account activity within your environment, so you can investigate and remediate fast.

8. Lay traps. Deploying deception technologies like honeypots and honey credentials are a proven way to spot attackers as they start to poke around in your environment and look for methods to access valuable Personal Data. If you prevent a breach, you don't need to report back to the Supervisory Authority.

9. Ensure you can prioritise and respond to the myriad of alerts your security products generate on a daily basis. If you have a SIEM in place, that's great, providing you're not getting swamped by alerts from the SIEM and that you have the capability to respond 24x7 (attackers work evenings and weekends, too). If you don't have a current SIEM (or the time or budget to take on a traditional SIEM deployment project), or you are finding it hard to keep up with the number of alerts you're currently getting, take a look at InsightIDR—it covers a multitude of bases (SIEM, UBA, and EDR), is up and running quickly, and generates alert volumes that are reasonable for even the smallest teams to handle. Alternatively, if you want 24x7 coverage, we also have a Managed Detection and Response offering which takes the burden away, and is your eyes and ears regardless of the time of day or night.

10. Don't forget about cloud-based applications. You might have some approved cloud services deployed already, and unless you've switched off the internet it's highly likely that there is a degree of shadow IT (a.k.a. unsanctioned services) happening too. Making sure you have visibility across sanctioned and unsanctioned services is a vital step to securing them, and the data contained within them.

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

RAPID7

QUICK GUIDE

What You Need to Know About the **General Data Protection Regulation (GDPR)**

The General Data Protection Regulation (GDPR) regulates the privacy and handling of European Union (EU) citizens' personal data. GDPR replaces the existing EU Data Protection Directive, and unifies data protection laws across the EU with a single set of rules.

Key Changes

Key changes that may impact organisations include:

- **Privacy-by-design** – Data protection must built into business processes and systems from the start and provided by default.
- **Data retention** – Personal data should only be kept for as long as is necessary, then the data must be securely destroyed or anonymised.
- **Right to be forgotten** – Users are able to request for their data to be deleted; they can also request for a copy to be sent to a third party.
- **Mandatory breach notification** – Any breaches of personal data must be reported to Supervisory Authorities within 72 hours of discovery, and depending on the extent of the breach, to affected Data Subjects without delay.
- **Penalties for non-compliance** – Fines up to 4% of a company's annual worldwide turnover or €20million, whichever is higher.

Common Questions

What is Personal Data?
Any information which can directly or indirectly identify a 'natural person', whether it's to do with their private, professional, or public life. This includes their name, birth date, email address, IP address, bank details, medical information, and more.

Who will be affected?
The GDPR will apply to any organisation that handles any personal data of an EU citizen. This means that companies based outside the EU that provides goods and services to individuals living in the EU will need to comply with the new law.

When will it come into effect?
GDPR was approved and finalised in 2016. The new law will becomes effective on May 25th 2018

Why should I care now?
The countdown has already started. For some organisations, required changes to their IT security and data privacy program will be extensive. Organisations found to be in breach of GDPR risk significant fines.

How to Prepare

- Start by getting an understanding of what personal data is being held and who has access to it.
- Limit access based on business need and implement monitoring to detect any unauthorised access.
- Perform an assessment of what security controls you have in place to protect the data, how effective they are, and where the gaps are.
- Develop a plan to improve your security program, looking at people, process, and technology.
- Implement a personal data breach notification process, including incident detection & response capabilities.

Need help getting started?

Implementing the CIS Top 20 Critical Controls is a good place to start.

Download the quick guide
www.rapid7.com/7-steps

RAPID7

SOLUTION BRIEF

General Data Protection Regulation Article 32

Get on the fast track to compliance with Rapid7

Organizations around the world are scrambling to leave no stone unturned in preparation for the General Data Protection Regulation, or GDPR. Article 32 of the GDPR requires controllers and processors of EU citizens' personal data to ensure a level of security "appropriate to the risk." Given Rapid7's risk-based security approach, it's safe to say we have a solution designed to address your compliance-based initiatives and challenges. Don't get us wrong—we won't be a silver bullet—but we understand GDPR compliance is complex, and we know how to help you get there.

OUR SOLUTIONS

HOW OUR TECH EXPEDITES COMPLIANCE

- **InsightVM | Vulnerability Management**

  Section 1b of article 32 requires "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services." Attacks involving exploits can affect all of these areas, so closing vulnerability gaps is paramount to your security program. This is where InsightVM comes in: The modern network is no longer comprised simply of servers and desktops; remote workers, cloud and virtualization, and mobile devices mean your risk exposure is changing every minute. Utilizing the power of Rapid7's Insight platform and the heritage of our award-winning Nexpose solution, InsightVM provides a fully available, scalable, and efficient way to collect your vulnerability data, turn it into answers, and minimize your risk.

- **InsightAppSec | Application Security**

  Web applications are often the first place personal data enters your organization, and they also happen to be juicy targets for attackers. Web app vulnerabilities continue to be the most common source of data breaches according to the annual Verizon Data Breach Investigations Report. You need a powerful tool that identifies all of those risks—one that crawls your entire application, provides accurate results, and is easy to deploy, use, and integrate seamlessly within your existing security operations. InsightAppSec is built upon Rapid7's Insight platform and leverages our proven application security testing engine to combine ease-of-use with powerful crawling and attack capabilities. You'll be up and running in no time, getting visibility into your application vulnerabilities within minutes.

- **InsightOps | IT Operations**

  IT teams have a strong part to play here, too; you need to quickly and simply make sense of the swathes of data tucked away in the myriad of logs across your ecosystem—logs which hold the keys to performance issues, which could impact the availability of vital data processing systems. InsightOps features clear, customizable alerting and a killer search function. It provides you with visibility into the dreaded shadow IT, enabling you to ensure personal data isn't hiding—or worse—leaking out of your environment unbeknownst to you. Bottom line: If you can't see it, you can't secure it.

Think resourcing's a challenge? It doesn't need to be: our vulnerability management and application security solutions are available as managed services.

DECADES OF KNOWLEDGE AND EXPERIENCE AT YOUR FINGERTIPS

Compliance is no simple task, and it usually implies an involuntary investment in additional resources. The good news for you? Rapid7's team members are armed with a world-class tech stack and are on call to impart their decades of expertise—without a massive undertaking on your end.

- **Consulting Services**

  Section 1d of article 32 requires "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing." The importance of doing this (and it's not just for compliance reasons), is that by not putting your program through its paces, you're leaving it for an attacker to do it for you. Rapid7 Consulting Services have a selection of offerings to help you assess how well your program will perform (or how it has played out in the past) when the inevitable happens. Our experts can provide a GDPR-focused security assessment, during which we review your current state, assess for gaps using industry best practices, and recommend optimal changes fully tailored to your organization's specific needs.

- **Incident Response Services**

  Ever wondered how your incident response processes and security program will perform in the event of a breach? Whether you've got a fully-fledged blue team, or you've just gotten started with a formal incident response setup, running through a breach readiness assessment will allow you to understand how you stack up against best practices extracted from our intel around attacker behavior.

- **Penetration Testing Services**

  Knowing your enemy helps you better defend against them. We at Rapid7 realize personal data is a profitable target for hackers, so we have intimate knowledge of their techniques, the tools they use, and how they think and act. We also believe that good security begets good compliance. This mindset extends to our penetration testing services: Every company's network and challenges are unique, so our penetration testers diligently tailor their methods and attack vectors for each engagement.

Have the expertise to perform in-house offensive security? Awesome. Arm your team with Metasploit Pro to safely simulate real world attacks and phishing campaigns.

YOUR GDPR JOURNEY DOESN'T END HERE...

Gain confidence that your team is prepared for GDPR compliance; have our experts perform a GDPR Readiness Assessment.

Need help with other facets of GDPR compliance?
Check out our GDPR Compliance Toolkit.

About Rapid7

With Rapid7, technology and security professionals gain the clarity, command, and confidence to safely drive innovation and protect against risk. We make it simple to collect operational data across systems, eliminating blind spots and unlocking the information required to securely develop, operate, and manage today's sophisticated applications and services. Our analytics and science transform your data into key insights so you can quickly predict, deter, detect, and remediate attacks and obstacles to productivity. Armed with Rapid7, technology professionals finally gain the insights needed to safely move their business forward. To learn more about Rapid7, visit www.rapid7.com.

ENLIST OUR EXPERT TEAM (OR JUST LEARN MORE)

North America: +866.7.RAPID7 | sales@rapid7.com
EMEA: +44.118.207.9300 | emeasales@rapid7.com
APAC: +65.3159.0080 | apacsales@rapid7.com

Learn More: www.rapid7.com/gdpr

RAPID7

SOLUTION BRIEF

General Data Protection Regulation (GDPR) Articles 33 & 34

How to expedite compliance with Rapid7 solutions

Does your organization handle the personal data of EU citizens (regardless of your geographic location)? Chances are you're already prepping for the General Data Protection Regulation (GDPR). We know GDPR compliance is no small undertaking—that's why Rapid7 has solutions and services to support you along the way. Articles 33 and 34 of the GDPR require data controllers to report personal data breaches to a supervisory authority without undue delay and, where feasible, within 72 hours of breach discovery. Additionally, data controllers must also communicate to the affected EU citizens if there is a high risk that the breach will affect their "rights and freedoms."

Solid breach responsiveness is clearly vital, but the best offense is a good defense. Ideally organizations would prefer for these processes to not be invoked in the first place. And, to state the obvious, breaches don't start and end at notification; you need to have the right people, processes, and technology to be able to detect, investigate, and respond.

Our experts have stellar backgrounds in incident response, averaging over ten years of experience, as well as unparalleled understandings of the attacker mindset. This wealth of knowledge doesn't just manifest via our services offerings—our technologies are built on this expertise.

OUR SOLUTIONS

InsightIDR: The SIEM You Always Wanted

InsightIDR, our User Behavior Analytics (UBA)-powered SIEM solution, was crafted based on our team's incident response experience. InsightIDR enables you to detect attackers earlier in the attack chain using advanced user behavior analytics, endpoint detection and response, and deception technologies. Investigations are a breeze with visual search and meaningful context. The last thing we want is hundreds of noisy, meaningless alerts every day, so we've saved you from them as well. Unlike traditional SIEM projects, our customers are up and running in a few hours—not months or years.

Don't take our word for it: See the difference for yourself with a free 30 day trial of InsightIDR, which includes a step-by-step walkthrough (and no need to wade through endless pages of documentation).

Incident Response Services

Just getting started with your incident response program, or looking to improve what you have in place today? We can provide valuable insight regardless of where you are in the process. Whether it's building out an entire program from scratch, reviewing your current setup, helping build out a roadmap to take things to the next level, or putting your program through its paces to see how it would stand up against a breach, Rapid7's Incident Response Program Development services are flexible to your individual needs and challenges. We also have a multitude of Incident Response services that include tabletop exercises, compromise assessments, and blocks of incident response retainer hours. Our experts can be counted on when you need them most—even in the face of the worst.

Managed Detection and Response

Don't have the time or resources to hunt for threats and attackers? We've got your covered. Whether it's day or night, weekday or weekend, our Managed Detection and Response service can monitor your environment for malicious behaviors that—left undetected—could lead to a disastrous data breach. Should an incident occur, we pivot from detection to response and work with you to take step-by-step actions toward remediation.

YOUR GDPR JOURNEY DOESN'T END HERE...

Gain confidence that your team is prepared for GDPR compliance; have our experts perform a **GDPR Readiness Assessment**.

Need help with other facets of GDPR compliance? Check out our **GDPR Compliance Toolkit**.

About Rapid7

With Rapid7, technology and security professionals gain the clarity, command, and confidence to safely drive innovation and protect against risk. We make it simple to collect operational data across systems, eliminating blind spots and unlocking the information required to securely develop, operate, and manage today's sophisticated applications and services. Our analytics and science transform your data into key insights so you can quickly predict, deter, detect, and remediate attacks and obstacles to productivity. Armed with Rapid7, technology professionals finally gain the insights needed to safely move their business forward. To learn more about Rapid7, visit **www.rapid7.com**.

ENLIST OUR EXPERT TEAM (OR JUST LEARN MORE)

North America: +866.7.RAPID7 | sales@rapid7.com
EMEA: +44.118.207.9300 | emeasales@rapid7.com
APAC: +65.3159.0080 | apacsales@rapid7.com

Learn More: www.rapid7.com/gdpr