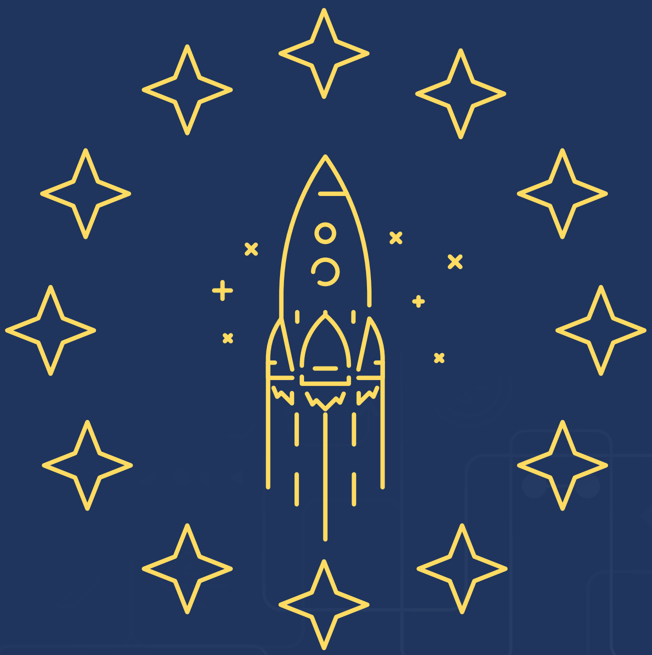
RESOLVE SYSTEMS™

The Definitive Guide to the General Data Protection Regulation for Cybersecurity Teams

3 Ways Accelerating Incident Response will Help you Comply



Introduction

May 25, 2018 will most likely be a typical spring day in Europe, but for marketers, legal, and regulatory leaders, the date may feel like a coming storm. This date signifies when the General Data Protection Regulation officially becomes law and forever changes how enterprises collect, store, and use customer data.

Even with 2+ years notice – as the initial vote was in 2014 and adopted in 2016[1] – companies are still scrambling to comply. Most preparation and documentation for the GDPR is geared towards the business services side, potentially leaving IT, and particularly cybersecurity, in the dark.

How does the GDPR affect cybersecurity teams with data integrity increasing in necessity as well as now EU compliance? Let's examine this need for legislation, objectives of the regulation, and how a 72 hour cyber breach notification window could actually become a reality.

Table of Contents

Need for Legislation

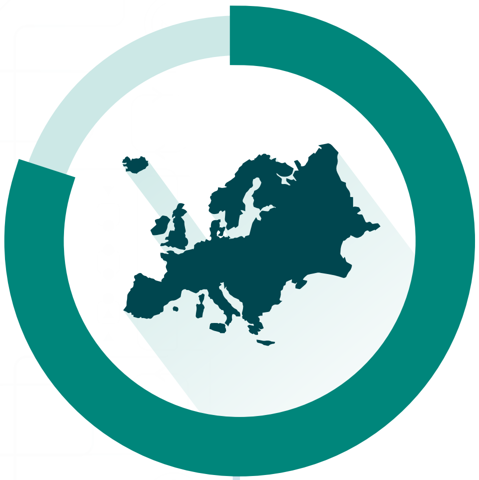
Rapid technological developments and globalization have brought new challenges for the protection of personal data.

Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organizations, while ensuring a high level of the protection of personal data.[2]

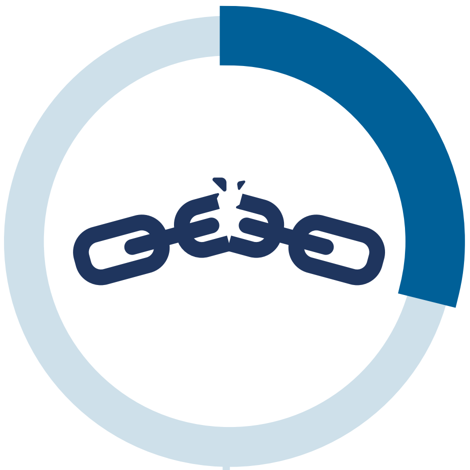
An increase of cyberattacks in Europe is pushing demand for more advanced legislation to protect personal data. 2017's WannaCry, Petya, Bad Rabbit, etc. continue to affect global enterprises and Europe's citizens are less confident of the protection of their personal data than ever before.[3] The Internet of Things (IoT) is already a reality in today's economy – Gartner estimates 8.4 billion connected digital devices in 2017[4] and 6 billion by 2020 in the European Union (EU) alone.[5] Even as recently as January 2018, Norway reported an attempted breach to steal patient data from a hospital system.[6]

4,000+ ransomware attacks have occurred worldwide every day since 2016[7]

Enter: The General Data Protection Regulation.



80% of European companies were affected by cyber incidents in 2016[8]



29% of companies reported loss or damage of internal records as a result of a cybersecurity Incident[9]

Objectives of GDPR

Replacing the Data Protection Directive 95/46/EC[10], the General Data Protection Regulation (GDPR) is one of the strictest and most advanced data protection regulations ever passed.

Not only does this legislation have global impacts, but also imposes tight data protection requirements and substatial penalties for non-compliance for any business around the world that collects or processes EU resident data.

Data Protection Directive 95/46/EC
Protects the fundamental rights, freedoms, and right to privacy of natural persons with respect to the processing of personal data.

Where is GDPR applicable?

GDPR is meant to strengthen citizens' rights, simplify rules for corporations, and regulate the processing by an individual or enterprise of personal data of an EU citizen. GDPR applies to any person or company:

- *Collecting or processing data of an EU citizen, regardless of global location*
- *Anyone selling goods or services or monitoring behavior of a resident of the EU*

GDPR will transform an enterprise's approach to data privacy and have marketers, in particular, focus on closely controlling critical data. With more attention on marketing and legal, the security incident response aspect is being overlooked. So, what are the key parts of the regulation, and how will those affect security and IT teams?

87% of people in the EU say they avoid disclosing personal information online due to cybersecurity concerns[11]

Key Parts of the General Data Protection Regulation

1. Right to Erasure

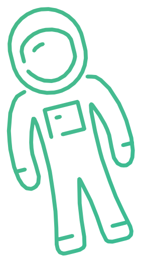
The most discussed aspect is the right to be forgotten, which means any EU citizen can have all personal data deleted or destroyed without delay including any links to, copies of, or replications of that personal data. This does not distinguish between data a company collects from customers and data a company collects from employees.

Read more: Article 17 of the GDPR

2. Right to Data Portability

GDPR is designed to give control of personal data back to an individual. One mandate to support this is for an individual to request and thus receive their data in a structured, commonly used, and machine-readable format. When it comes to GDPR, data portability means sending the consumer a spreadsheet which includes all collected personal data.

Read more: Article 20 of the GDPR



3. Assign a Data Protection Officer

Under GDPR, data controllers must assign a Data Protection Officer (DPO) who informs and advises a company about relevant security obligations, monitors compliance, and is the point of contact with the supervisory authority on any processing issues.

Read more: Article 37 of the GDPR

Do you need a Data Protection Officer?

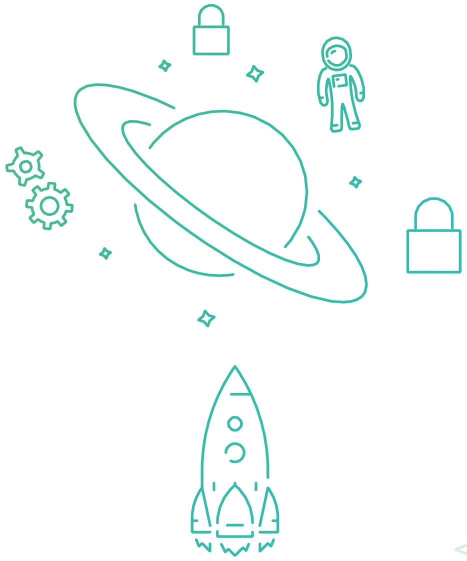
- *Does local law require it?*
- *Is your data processed by a public authority?*
- *Are you regularly monitoring or processing sensitive, personal data including racial, ethnic, political, religious, or genetic on a large scale?*
- *Does your organization lack knowledge of data protection law and practices?*

4. Report Security Breaches

Any security breach which compromises personal data must be reported (at least in phases) within 72 hours after becoming aware. Non-compliance with this mandate must have reasons for the delay and will come with hefty fines. One caveat to the 72-hour-window notification is if the personal data breach is unlikely to result in a risk to the rights and freedoms of the person.

Documentation outlining possible outcomes, actions taken to resolve the breach, and facts associated with what was taken all has to be submitted within 3 days!

Security incident response processes will have to be focused on this, and accelerating response will be mandatory moving forward.



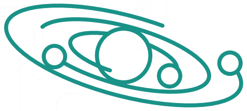
Ramifications of Noncompliance

The penalties of noncompliance with GDPR are severe, with fines for violations broken down:[12]

Minor Violations (whichever is greater)	More Serious Violations (whichever is greater)
€10 million Maximum fine	€20 million Maximum fine
2% of prior year's global revenue	4% or prior year's global revenue

> **Last year we issued more than one million pounds in fines for breaches of the Data Protection Act, so it's not a power we're afraid to use.**

- Elizabeth Denham, UK Information Commissioner ICO,
January 18, 2017



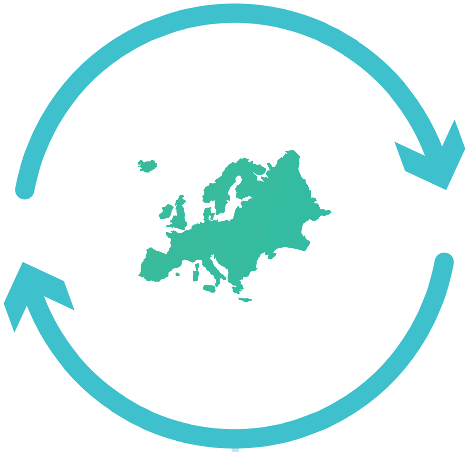
Measuring Security Incident Response for GDPR

How effective are EU enterprises now in terms of security incident response?
“The effectiveness of the European Union’s response to cybersecurity is difficult to gauge since the concept is challenging to operationalize and measure.”[13]

When considering the mandate of notification within 72 hours, why is security incident response so difficult to measure now?

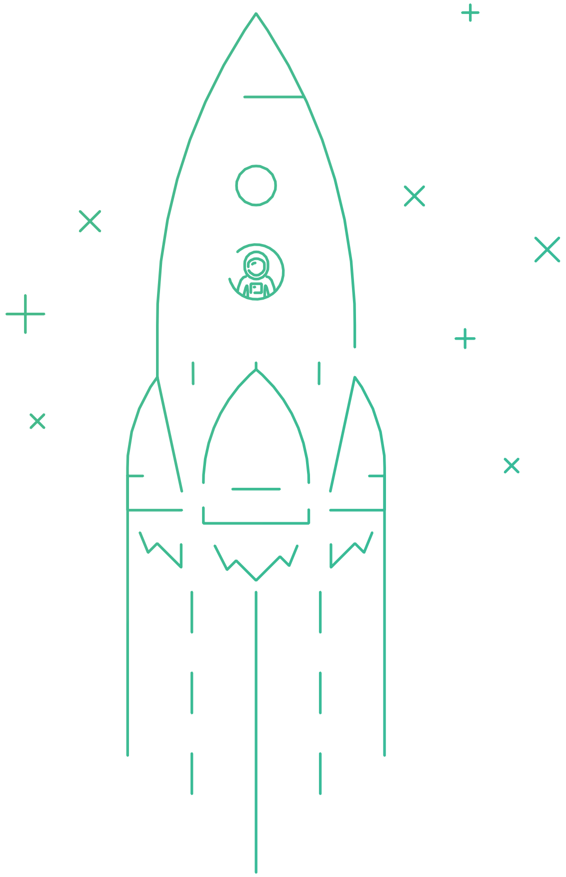
- The issue of how to measure the effectiveness of cybersecurity effort is subjective
- Reporting fragmentation within the EU of identifying/addressing implementation changes and response
- Lack of an automation and orchestration platform with standards-based playbooks to accelerate response

Only **10%** of UK businesses report having a formal cyber security incident management process.[14] The larger the company, the more likely they have a security incident response plan, but is it enough to withstand GDPR?



All **28 states** of the European Union will have to update their data processes and protections and everyone – from marketing to legal to IT and cybersecurity teams – will be impacted.

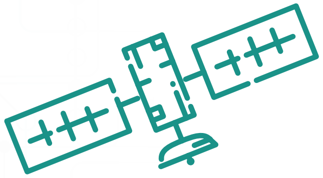
Resolve Systems' Automation and Orchestration Platform to Accelerate Security Incident Response Time



3 Ways Accelerating Incident Response will Help you Comply

The most critical facets of GDPR, for cybersecurity teams, are protecting personal data and disclosing it within 72 hours. No matter where the location of your headquarters, SOC, or server, organizations will need to notify impacted customers of the breach, regardless of if the company is based in the EU or not.

With limited time to notification, an automation and orchestration platform – like Resolve – can accelerate security incident response.



Our recommendations to prepare for a 72-hour-turnaround are:

- Assess your current incident response process and instill consumer confidence with not only prevention and detection tools to protect personal data, but also prepare for the inevitable breach with an enterprise-wide incident response platform.
- Mitigate the risk of fines by meeting deadlines associated with GDPR. Avoid paying €20m or up to 4% of annual revenue which impacts your bottom line and most likely your job. Adaptive and human-guided automation provides the entire SOC with the tools necessary to respond to a breach – quickly.
- Utilize an automation and orchestration platform to reduce the mean time to respond. Standards-based playbooks, out-of-the-box automation, and process guidance reduces false alerts and quickens the time it takes to detect, validate, and respond to breaches. Depending on the severity of the breach, you have to notify your consumer. Wouldn't it be nice to say you've already responded to the incident?

Resolve Systems is solely focused on accelerating incident response, across the entire enterprise.

References

(1) https://www.eugdpr.org/gdpr-timeline.html

(2) http://www.privacy-regulation.eu/en/recital-6-GDPR.htm

(3) http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2171

(4) https://www.gartner.com/newsroom/id/3598917

(5) https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination

(6) https://www.csis.org/programs/cybersecurity-and-warfare/technology-policy-program/other-projects-cybersecurity

(8) PWC, Global State of Information Security Survey, 2016, https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey/cybercrime.html

(9) https://www.pwc.com/us/en/cybersecurity/information-security-survey.html#insight3

(7) https://ec.europa.eu/commission/news/cybersecurity-and-free-flow-non-personal-data-eu-2017-sep-19_en

(10) http://whatis.techtarget.com/definition/EU-Data-Protection-Directive-Directive-95-46-EC

(11) http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2171#p=1&instruments=SPECIAL&surveyKy=2171

(12) https://www.eugdpr.org/key-changes.html

(13) http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf

(14) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf

About Resolve Systems

Resolve Systems is the global leader in providing a single platform for enterprise-wide incident response, automation and process orchestration for Security Operations, IT Operations, Network Operations and service desk teams.

Resolve accelerates incident response and resolution by supplying engineers with partially or fully customized human-guided automations, powerful real-time incident collaboration and the omnipresence to orchestrate existing systems, across silos.

Headquartered in Irvine, California, USA with operations in EMEA and APAC, Resolve Systems works with nearly 100 of the largest global firms and is majority owned by funds affiliated with Insight Venture Partners, a leading global private equity and venture capital firm investing in high-growth technology and software companies

About Insight Venture Partners

Insight Venture Partners is a leading global venture capital and private equity firm investing in high-growth technology and software companies that are driving transformative change in their industries. Founded in 1995, Insight has raised more than $13 billion and invested in nearly 300 companies worldwide. Our mission is to find, fund and work successfully with visionary executives, providing them with practical, hands-on growth expertise to foster long-term success.

For more information on Insight and all of its investments, visit www.insightpartners.com or follow us on Twitter.

RESOLVE SYSTEMS™

resolvesystems.com

North American Headquarters
2302 Martin Street
Suite 225
Irvine, CA 92612
T: +1.949.325.0120

EMEA Headquarters
60 Cannon St
Suite 119
London EC4N 6LY, UK
T: +44 (20) 37432123

Asia Pacific Headquarters
1 Fullerton Road
#02-01, One Fullerton
Singapore 049213
T: +65 6832 5513