

WHAT DOES THE 72-HOUR

GDPR NOTIFICATION RULE MEAN TO YOU?

GENERAL DATA PROTECTION REGULATION

01

ARTICLE 33

The mandatory 72-hour breach reporting rule applies to all companies collecting or processing personal data in the European Union. Failure to comply will result in a fine of up to **10,000,000 EURO** or **2% of annual revenue** (whichever is higher).

GPDR DATA BREACH REQUIREMENTS

02

Within **72 Hours** after a **data breach** has been discovered, an organization must:

- Carry out a thorough investigation
- Inform regulators and impacted individuals of the breach
- Identify what personal data has been impacted and how
- Draft a comprehensive containment plan



That's a big ask, right? Well, there is more.

GDPR also requires a detailed forensics report to be provided **within 72 hours**.

UNDERSTANDING WHAT NEEDS TO BE PART OF THE REPORT

03

- ☑ Nature of breach
 - ✓ Who accessed what and when
 - ✓ Who are these users
 - ✓ How is that data being used
 - ✓ Impacted individuals
- ☑ Record of work that has been done to prevent a breach
- ☑ Estimated impact of the breach
- ☑ Forensics details
- ☑ Mitigation or remediation plan
- ☑ Notify authorities within 72 hours and affected individuals without undue delay



IMPERVA DATA SECURITY SOLUTION

04

Prioritize most critical incidents using machine learning



Identify suspicious data access with behavior analytics



Monitor all data access activities-answering who, what happened, what data, and when



Provide detailed forensics breach report



Learn more at imperva.com/gdpr

© 2018, Imperva, Inc. All rights reserved.
Imperva, the Imperva logo, SecureSphere, Incapsula, CounterBreach, ThreatRadars, and Camouflage and design are trademarks of Imperva, Inc. and its subsidiaries. All other brand or product names are trademarks or registered trademarks of their respective holders.

IMPERVA