snare

WHITEPAPER

THE GENERAL DATA PROTECTION REGULATION

PREPARING YOUR BUSINESS WITH SNARE

In May 2018, the General Data Protection Regulation ("GDPR") will come into effect, marking a drastic shift in the compliance landscape. This regulation is firmly rooted in the desire for greater protection of individuals privacy and the unification of data protection laws in the European Union ("EU"). It imposes a strict regulatory framework for the handling of Personally Identifiable Information ("PII") and applies to any data collected about a European resident or citizen, by any company operating within, or external to, the EU. The regulation sets stringent rules around how organisations handle PII from collection to processing, storage, sharing and deletion.

Where a business fails to meet the requirements of the GDPR, they are subject to fines by EU regulators. There are two key areas of consideration that the regulation applies to (i) the reporting of data breaches, and (ii) compliance and data protection by design.

(I) REPORTING OF DATA BREACHES

The GDPR requires companies to report data breaches, and notify those directly affected, as soon as they are aware of an incident, without undue delay and where foreseeable within 72-hours of the breach being detected.[1] According to the regulation, a data breach is *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."*[2]

(II) COMPLIANCE AND DATA PROTECTION BY DESIGN

Data protection by design refers to the preventative measures that a company can take to reduce the risk, and severity of a breach. Requiring companies to look holistically at their business policies to ensure the requirements of the regulation are met; at both the technical and organisational level.

---

[1] *The European Parliament and the Council of the European Union (EU) 679/2016 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data*, art. 33.
[2] [1] art. 4, def. 12.

IN BRIEF:		
WHAT'S HAPPENING? In May 2018, the GDPR will come into effect – impacting businesses established in, that conduct business with, or monitor individuals within, the EU. The regulation specifically concerns the management of personally identifiable information.	**WHY IT MATTERS?** The GDPR imposes a hefty financial penalty on a failure to comply. Requiring businesses to notify authorities, and affected customers within 72-hours of a breach being detected. A failure to do so will result in a penalty of up to €21 million, or 4% of annual revenue – whichever is greater.	**HOW CAN SNARE HELP?** Snare is a log management platform that can greatly aid in the detection of security breaches by centrally collecting, monitoring and managing log data and user activity. Equipping you with the capacity to meet the GDPR requirements.

This is based on several "foundational principles":

1. A proactive, not reactive security posture
2. A respect for user privacy
   - Consideration for the right to data protection
   - Privacy as the 'default' setting
   - Transparency around data collection
3. End-to-end data security

WHY SHOULD YOU PAY ATTENTION?

It is essential if you have a business that falls under the jurisdiction of the regulation, that you make the necessary security changes to your digital infrastructure prior to May 2018. As a failure to do so could not only result in hefty fines (of up to €21 million, or 4% of annual revenue – whichever is greater) for an undue delay in reporting a breach, but also significant reputational damage.

DOES THIS REGULATION CONCERN YOU?

The GDPR has a broad territorial scope, applying to any business that is established in the EU, or any business that offers goods or services to, or monitors, data subjects in the EU.[3] Regardless of geographic location, if you are a business which processes the personal data of a EU citizen, you ought to comply. Thus, it may be best to err on the side of caution if you suspect that the GDPR will encompass your business activities.

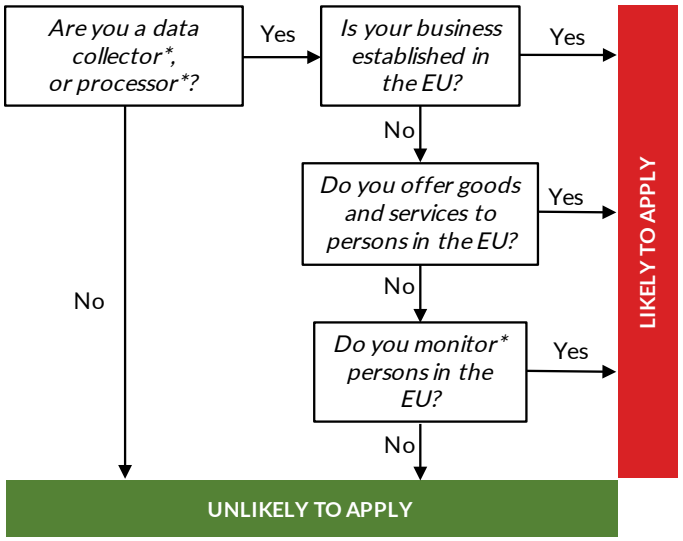
[3] [1] art. 3

HOW CAN SNARE HELP?

The Snare platform has been used for over two decades by hundreds of companies to monitor their IT security actively, and meet national, international and industry compliance standards; such as ISO27001/2, PCI DSS, and HIPAA. The platform can be used to meet the GDPR security and privacy requirements, by minimizing the risk exposure in your infrastructure design, and by reducing the impact of potential breaches. Snare centrally collects and manages log data and user activity so that you can better monitor your infrastructure's security.

Log data is your digital DNA – forensic analysis can reveal security breaches by highlighting what happened, when it happened, where it happened, who was involved and where they came from. Most IT environments consist of

Check if your business is impacted:



multiple heterogeneous devices, systems, and applications; that each generate distinct log entries – millions of data points generated daily, in which only a few could reveal a breach. Manual exploration of logs can be a headache for IT security teams, as they are searching for 'a needle in the haystack'. To actively detect breaches, log analysis is required. Snare takes the headache out of analysing your log entries by providing advanced log analysis tools, and reporting capabilities.

THE SOLUTION

The Snare Agents, Snare Central and the Snare Reflector can be combined to collect and monitor activity across distinct areas, including:

- **User movements** through the IT environment - access to systems, applications, services and file access; and
- **Data integrity monitoring**
  - Identification of system changes; including configuration or system policy changes
  - Extractions of data from the system; monitoring removable media usage, and file transfers to third-party applications and system logs

With the Snare reflector, you can reflect your logs to third-party SIEMs, or other analytical platforms for processing. However, the powerful reporting and alerting facilities of Snare Central, combined with the flexible collection and filtering abilities of the Snare Agents, can provide you with the capacity to meet the GDPR regulatory requirements. The platform detects critical issues, provides timely notifications, and empowers the security team to conduct comprehensive forensic investigations.

For example, Snare can be used to monitor privileged users at various levels. Many organisations use either Active Directory ("AD") or Lightweight Directory Access Protocol ("LDAP") for their user authentication across desktop logins, server access, remote VPN access, and sometimes within applications. Snare agents can provide user access monitoring, and facilitate analysis of privileged groups on both the AD and LDAP servers. The log data that is processed allows administrators to monitor and manage various important elements.

For example, they can:

- **Review disabled accounts** and associated usage;
- **Review user access** to ensure that privileges are 'up-to-date';
- **Perform** 90-day inactive user reviews;
- **Remove stale objects** from AD

Furthermore, Snare can provide real-time triggers from threshold and alerts on a pattern of activity, or match on a number of specific events. Whilst, also facilitating data access reviews for PII via file activity monitoring and database query tracking. Data is your business's most valuable asset, and the central focus of the GDPR. Thus, it is crucial that you understand it, manage it and protect it. The integration of an effective collection, analysis and reporting platform in Snare, can provide you with the capacity to meet the GDPR requirements.

ADDITIONAL RESOURCES:

To find out more about how Snare can help you, visit: http://www.intersectalliance.com/

To access the full regulation, visit: http://ec.europa.eu/justice/dataprotection/reform/files/regulation_oj_en.pdf