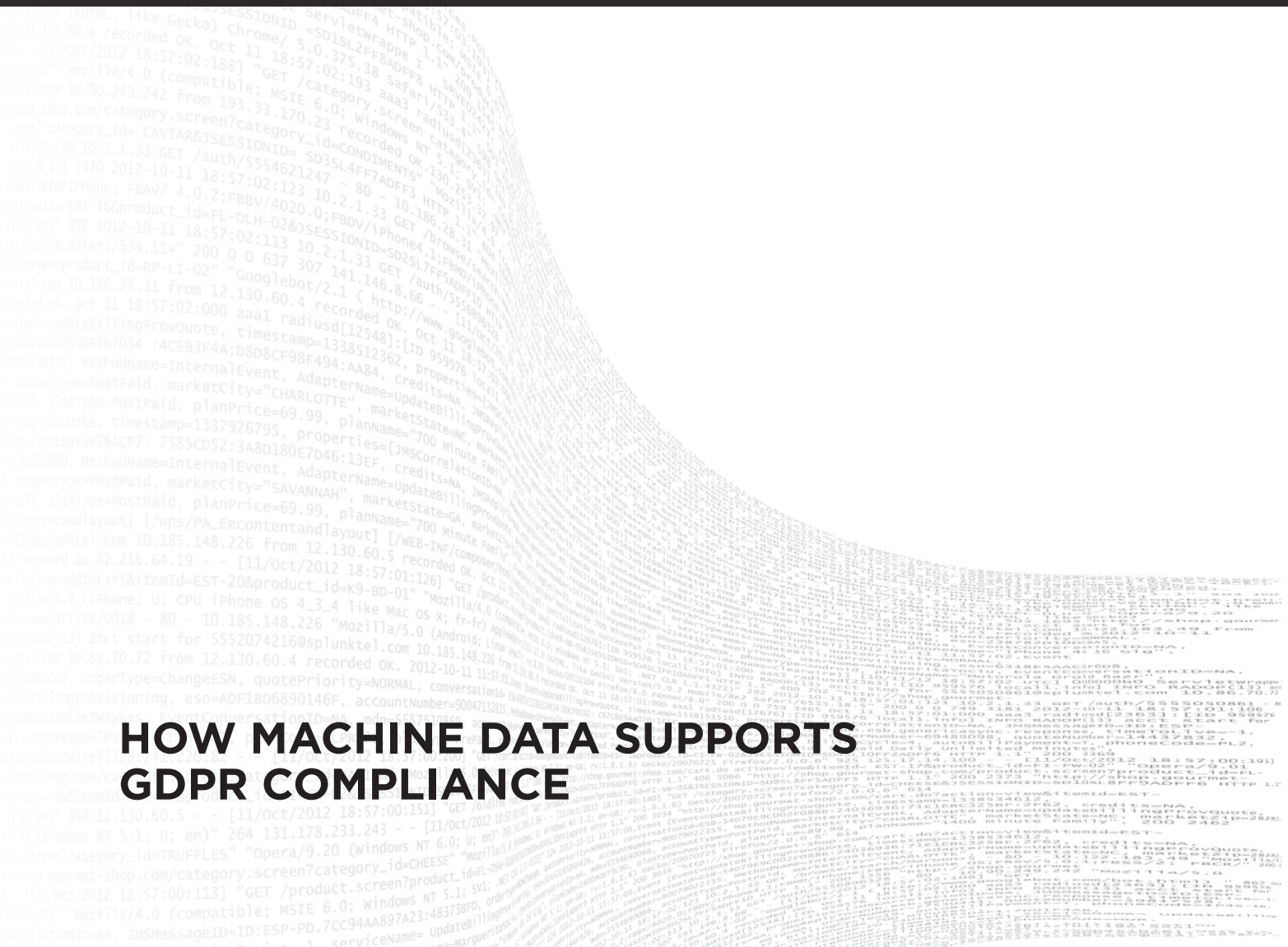
splunk>

WHITE PAPER

HOW MACHINE DATA SUPPORTS GDPR COMPLIANCE



Overview: The General Data Protection Regulation

In 2012, the European Commission proposed a comprehensive reform of European Data Protection Directive 95/46/EC, which established a set of data protection principles that each member state adopted into local law, resulting in a patchwork of data protection requirements across the European Union. This patchwork approach made compliance costly and challenging for global business.

In April 2016, the European Parliament adopted the new General Data Protection Regulation (GDPR) that replaces the patchwork approach with a single, harmonized law binding across all member states of the EU. The GDPR provides greater predictability and efficiency for business and offers EU citizens increased data protection rights in the new digital age. The GDPR will take effect in May 2018. Key requirements include:

- Increased rights for data subjects, i.e. the right to "be forgotten" and data portability
- Software developed with security in mind (privacy by design and by default)
- Pseudonymisation or encryption of personal data (privacy by design and by default)
- Secure processing of data
- 72-hour notification for breaches of personal data
- Fines of up to €20 million or four percent of annual turnover, whichever is greater

Further, the GDPR does not simply apply to EU domestic business, ***but to companies worldwide that target their goods and services to European citizens.***

How Machine Data Can Help With Compliance

Machine data provides a useful record of the activity of your customers, users, processed transactions, applications, servers, networks and mobile devices. Insights gained from machine data can support any number of use cases across an organization and can also be enriched with data from other sources. We identified below three use cases that can help support your GDPR compliance program, regardless of the nature of your industry or deployment – on-premises, in the cloud or hybrid.

1. Security Management and Breach Notification

Article 32 – Security of Processing

Scenario: An employee from your human resources department gets a targeted phishing email asking them to reset their system password. The phishing email wasn't caught by your spam filter and the email formatting looked legitimate, so your employee clicked on the link, and suddenly his access credentials were in the hands of an attacker – the very same credentials your employee uses to access your HR system of record – putting the personal data of your entire workforce at risk.

The GDPR requires security of processing (Article 32), meaning that organizations processing personal information must implement "appropriate technical and organizational measures to ensure a level of security appropriate to the risk". This includes taking into account state of the art technical measures to prevent unauthorized access to personal data.

Insights from machine data provide early warning of threats to your digital infrastructure. Your digital environment produces massive volumes of activity logs that can be used to identify anomalies in user behavior and detect unauthorized access. For example, machine data can tell you whether there is logon activity associated with an employee who is out-of-office on vacation or due to illness, raising a possible red flag. You can also identify when a new mobile device is enrolled in your system or logs into a VPN, providing early warning of compromised credentials that can help you prevent data exfiltration. Machine data analytics can do this quickly and in real time.

Article 33 and 34 – Notification

The GDPR requires breach notification and communication. This means that organizations must notify supervisory authorities within 72 hours of becoming aware of a personal data breach that could harm the rights and freedoms of EU citizens (Article 33) and must notify the affected individuals without undue delay (Article 34). The notification must contain, among other things, information about *the nature of the breach, including the number of data subjects affected,* and your steps for remediation.

"In light of the tight timescales for reporting a breach – it is important to have robust breach detection, investigation and internal reporting procedures in place."

ICO (Information Commissioner's Office) on the GDPR Breach Notification

---

Insights from machine data allow organizations to quickly detect, investigate and scope breaches. Detailed analysis can be performed to track how and when the attacker came into the environment, which systems and data were accessed and when, how many people/records were affected and what remedial measures need to be taken – all of which helps you meet your notification requirements.

2. Data Protection Audits

Article 58 – Supervisory Investigative Powers

Scenario: You have a breach that was caused by an undisclosed vulnerability: you scoped the attack, discovered personal data was exposed, identified affected individuals, reported the breach and took remedial measures to mitigate the risk. Now, the affected individuals want compensation and the supervisory authority wants to perform a data protection audit to see if your security "took into account state of the art" technologies to secure your processing activities.

The GDPR grants each supervisory authority the power to carry out investigations in the form of data protection audits and issue warnings, reprimands or bans on data processing (Article 58) and assess fines of up to €20 million or four percent of an organization's total worldwide annual turnover - whichever is greater. Additionally, Article 82 gives any person who has suffered material or non-material damages the right to receive compensation. Fines can only be avoided if a party can show that it was not in any way responsible for the event giving rise to the damage. To do this, organizations will need to document their actions and demonstrate their compliance to the supervisory authority.

Machine data provides the historical information organizations need to demonstrate to controllers and supervisory authorities that they had


```
{ [-]
   ClientIP: 101.235.6.6
   CreationTime: 2017-04-11T03:32:43
   EventSource: SharePoint
   Id: 2af64672-f9ca-4c25-0274-08d40c2fb043
   ItemType: File
   ListItemUniqueId: 43b04c3c-8a3f-400e-8c9c-d79addbfc112
   ObjectId: https://broncos-my.sharepoint.com/personal/anthony_milford_broncos_com_au/Documents/Copy of Asset player HR
Actions  Recruitment Report (AE 1).XLS
   Operation: FileUploaded
   OrganizationId: a74a1efc-372d-476c-802c-9cbbe5a5c71e
   RecordType: 6
   Site: d983b062-461e-4ef5-b237-2fafe2071f0f
   SiteUrl: https://broncos-my.sharepoint.com/personal/anthony_milford_broncos_com_au/
   SourceFileExtension: XLS
   SourceFileName: Copy of Asset player HR Actions  Recruitment Report (AE 1).XLS
   SourceRelativeUrl: Documents
   UserAgent: Microsoft SkyDriveSync 17.3.6517.0809 ship; Windows NT 10.0 (10586)
   UserId: anthony.milford@broncos.com.au
   UserKey: i:0h.f|membership|10033fff8ae39bf3@live.com
   UserType: 0
   Version: 1
   WebId: c6820655-bf56-425d-b22d-41fd55da3045
   Workload: OneDrive
}
```


Example of machine data accessing a file with PI information

appropriate security controls in place and proactively worked to mitigate the risk. Whether it's technical configurations and their changes, password reset history or update history, machine data can be used to document all of these and many other key security considerations.

3. Search and Report on Personal Data Processing

Article 15, 17, 18 and 28 (Data Subject Rights)

Example Scenario: Your organization provides payroll services throughout Europe for small businesses. As a result, you're processing large amounts of personal data every month, and from time to time you get requests from clients for processing reports. One of your former customers recently suffered a data breach and reaches out to you as part of a data privacy audit their supervisory authority is conducting. You are asked to provide a report documenting who accessed the customer's personal data at your place of business in the last 12 months. They also want proof that you removed their personal data from your system (including any backup copies) after your contract was terminated.

The GDPR grants EU citizens the right to know what personal data is being processed about them, with whom it is shared and where it is processed (Article 15). Data subjects can also ask that their personal data be corrected (Article 16) or deleted (Article 17). Processors are required to ensure that only authorized persons process the personal data and when the processing is complete and the contract terminated, the controller can request that all personal data be deleted or returned, including in some cases any existing backup copies.

Machine data gives organizations end-to-end visibility into their processing activities – critical information for GDPR compliance. Machine data can help you to demonstrate what personal data was accessed, by whom, how it was used and when it was deleted.

Thousands of enterprises rely on the Splunk platform to improve security, increase efficiencies, make data-driven decisions and gain tactical and strategic advantages. However every environment has its own unique machine data footprint. Do you want to learn more about your footprint and conduct a GDPR Workshop? **Just ask us!**

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com