Complying with General Data Protection Regulation

General Data Protection Regulation (GDPR) covers a wide range of data security issues, including data protection, accountability, data processing, consent from subjects, and privacy.

Because your organization does business in Europe, you have to ensure that the way your company handles data is in compliance with all parts of GDPR. The fines for non-compliance are extremely high, so you have little room for error.

You want to use Splunk to manage GDPR in-scope systems to ensure compliance. Specifically, you want to monitor who accesses what systems, what connections occur in your environment, whether systems are patched appropriately, and a number of other key indicators to guarantee compliance with GDPR and facilitate your ability to prove compliance.

Required data

- Authentication data
- Firewall data
- Proxy data
- Antivirus data
- System log data

How to use Splunk software for this use case

You can run many searches with Splunk software to help ensure compliance with GDPR. Depending on what information you have available, you might find it useful to identify some or all of the following:

- Access to unencrypted resources
- Activity from expired user identity
- Expected host not reporting events
- Geographically improbable access detected
- Device with outdated anti-malware
- Systems with the update service disabled
- New connection to device
- Unauthorized connection through firewall
- Unauthorized access to Splunk indexes
- Unauthorized access to systems
- Brute force access behavior detected

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Next steps

Measuring impact and benefit is critical to assessing the value of compliance operations. When implementing this use case, you should track the number of out-of-GDPR-compliance incidents detected over time. In addition, review compliance office requirements and reporting policies, and have a method of developing and maintaining an asset and identity catalog with in-scope attributes.

This use case is also included in the Splunk Security Essentials app, which provides more information about how to implement the use case successfully in your security maturity journey. In addition, these Splunk resources might help you understand and implement this use case:

- Conf Talk: A day in the life of a GDPR breach
- Conf Talk: Monitoring GDPR compliance With Splunk
- White Paper: How machine data supports GDPR compliance
- Blog: GDPR: Go beyond compliance. Deliver a ‘data trust’ revolution
- Blog: Knowledge is power: Guidance from ICO and NCSC on GDPR security outcomes
- App: Splunk Security Essentials
- Blog: 7 High-Risk Events to Monitor Under GDPR: Lessons Learned from the ICO’s BA Penalty Notice