GDPR Compliance

Checklist: A 9-Step Guide

www.alienvault.com

Intro

The GDPR, or General Data Privacy Regulation (EU) 2016/679, will come into force in May of 2018. It has the potential to significantly alter the way businesses handle and store data. At over 200 pages long, the regulation consolidates and replaces the many local data protection laws such as the UK's Data Protection Act 1998, the Belgian Privacywet, or the German Bundesdatenschutzgesetz (BDSG). The main differences lie in the severity of the potential fines and new requirements such as breach notification, right to access, right to be forgotten, and so forth.

The primary objective of GDPR is to strengthen security and privacy protection for individuals. While GDPR shares many principles from its predecessors, consisting of 11 chapters, 99 articles, and 187 recitals, it is by no means a minor adaptation.

Section 1:

Who GDPR Applies To

The GDPR places legal obligations on all data controllers and processors. A data controller is defined as the entity which determines the purposes and means of processing personal data, and the data processor is defined as the entity which processes the personal data on behalf of the controller. GDPR applies to processing carried out by organizations within the EU as well as organizations outside the EU that process or control data related to living EU residents or nationals.

It primarily focuses on individual data, which is defined in two categories of 'personal data' and 'sensitive personal data'. Personal data includes data such as email and physical addresses as well as any information that can be used as an online identifier, e.g. an IP address. Sensitive personal data casts a wider net and covers data elements such as health, biometric, or genetic data.

If you don't already have the required security tools and controls in place, your organization will need to implement several new security controls, policies, and procedures in order to demonstrate GDPR compliance. For security and privacy-conscious organizations, the new regulation should not bring about too much technical overhead. For those that haven't yet achieved compliance with the data protection laws that GDPR replaces, the impact will be much greater.

GDPR requires organizations to maintain a plan to detect a data breach, regularly evaluate the effectiveness of security practices, and document evidence of compliance. Instead of specific technical direction, the regulation puts the onus on organizations to maintain best practices for data security.

Section 2:

Nine Steps You Can Take to Prepare for GDPR Compliance

Step 1: Implement a Security Information and Event Management (SIEM) tool with log management capabilities that adhere to compliance requirements.

Article 30 of GDPR states that each controller, and where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.

A SIEM is typically a fundamental security tool for many organizations. By implementing a SIEM, companies can monitor all user and system activity to identify suspicious or malicious behavior. This is achieved by centralizing logs from applications, systems, and the network and correlating the events to alert where undesirable activity is detected.

You can then investigate the cause of the alarm and build up a view of what has occurred by determining if a particular attack method was utilized, looking at related events, source and destination IP address, and other details.

You must also take into consideration data stored or processed in cloud environments. If personal data is in the cloud, it is within the scope of GDPR, and therefore it is beneficial to choose a SIEM that can maintain a record of activity across your public and private cloud infrastructure as well as on premises.

Ask yourself:

- Do you have a way to centralize, analyze, and store log data from all your environments?
- Are you alerted in real time to any suspicious or anomalous activity?
- Do you have a way to securely store raw log data and to ensure its integrity?

Learn more about AlienVault® Unified Security Management™ (USM™) SIEM capabilities >

Step 2: Create an inventory of all critical assets that store or process sensitive data to allow for more stringent controls to be applied.

The GDPR is expansive and covers all IT systems, network, and devices, including mobile devices. Therefore, it is essential that you take stock of all assets across your infrastructure and establish where personal data is held.

It's important to inventory all assets and locations that process or store personal data, a task that seems simple on its surface, but is often an area where organizations struggle. This is especially true in dynamic IT environments, such as public cloud and in cases where employees are using BYOD or non-IT-sanctioned assets. It's worth noting that your company could be exposed to attacks and regulatory fines if employees process or store personal data on unapproved devices.

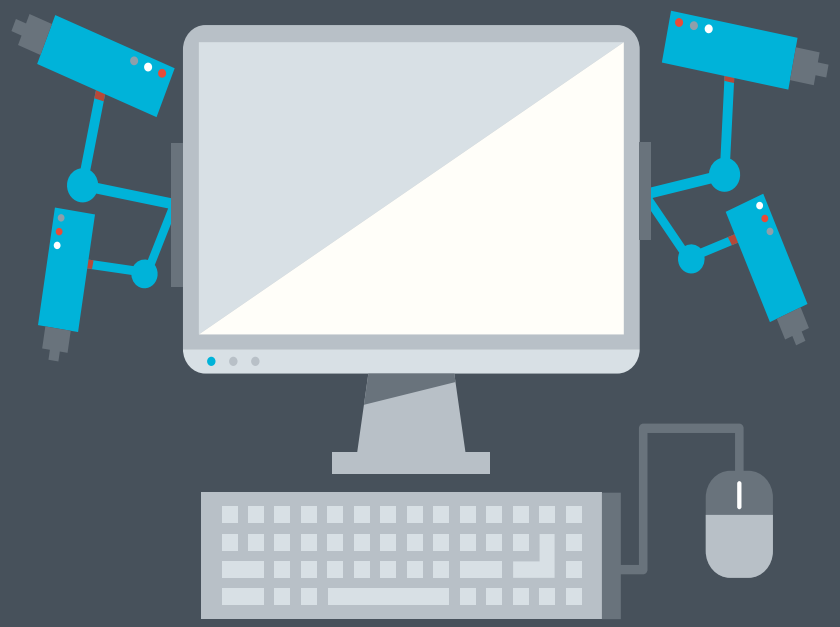
Without strong governance practices in place, it can be easy to lose track of assets. Therefore, it is important to sample your systems, networks, and data stores to determine if personal data is exposed outside your defined data flows and environments. Bear in mind that this is a process. Inventories will need to be updated on an ongoing basis as your business and technology changes.

Ask yourself:

- What assets are connected to my environment at any given time?
- Do those assets process or store any personal data?
- What ports and protocols are used when transmitting or accessing personal information?

Learn more about asset discovery with AlienVault USM >

Step 3: Undertake vulnerability scanning to identify where weaknesses exist that could be exploited.



New vulnerabilities in systems and applications arise almost daily. It is therefore essential that your organization stays on top of these weaknesses with regular vulnerability scanning. These vulnerabilities may exist in software, system configuration, in business logic or processes. So, it is important to consider all aspects of vulnerabilities and where they can exist.

However, simply finding a vulnerability is often not enough. There are multiple factors that need to be considered such as whether the systems are in scope of GDPR and what the business-criticality is, whether intrusions have been attempted, and how the vulnerability is being exploited by attackers in the wild.

Effective vulnerability assessment requires continuous scanning and monitoring of critical assets upon which personal data resides or is processed. It is equally as important to monitor cloud environments in addition to on-premises environments.

When a vulnerability is discovered, ask yourself:

- How many personal records could be exposed?
- Have any intrusions or exploits been attempted on the vulnerable asset?
- How is the vulnerability being exploited by attackers in the wild?

Learn more about vulnerability scanning with AlienVault USM >

Step 4: Conduct risk assessments and apply threat models relevant to your business.

Article 35 of GDPR requires organizations to conduct a data protection impact assessment (DPIA) or similar. Whereas Article 32 of the regulation requires organizations to “implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.”

The use of an information security framework can assist by providing a starting point for organizations to better understand the risks facing the business. Existing frameworks such as NIST, ISO / IEC 27001, or similar standards can assist companies in undertaking and supporting the DPIA process.

While GDPR does not specify a framework for risk assessments or threat modelling, a company’s adherence to any well-established and internationally recognized standard will make demonstrating compliance with Articles 32 and 25 much more likely in the event of a breach.

Ask yourself:

- In the event of a data breach, can I demonstrate that appropriate security controls were in place?
- Do I know what threats my organization faces and the likelihood of them materializing?
- Am I aware of which systems and businesses units are high risk?

Step 5: Regularly test to gain assurance that security controls are working as designed.

Article 32 of GDPR covers security of personal data processing. Among the examples it provides, it asks for a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Assessing and evaluating the effectiveness of security controls is by no means an easy feat. Usually, the larger the IT environment, the more disparate the technology stack, and the more complex the environment. Thus, the harder it is to gain assurance.

Three broad techniques exist to validate the effectiveness of security controls:

1. Manual assurance. This involves audits, assurance reviews, penetration testing and red-team activities.
2. Consolidated and integrated security products, so that fewer point products need to be managed and reported on.
3. The use of automated assurance technologies.

With these methods, you can gain a measure of assurance that your systems are secured as intended. However, it is worth remembering that assurance is not a one-time effort, rather an ongoing, repeatable process.

Ask yourself:

- What level of confidence do you have in your security tools?
- If a tool or system failed, would you be alerted automatically?
- Are all security tools being used as intended?

Step 6: Put in place threat detection controls to reliably inform you in a timely manner when a breach has occurred.

GDPR requires organizations to report to the regulatory body within 72 hours of being aware of the breach. For high-risk events, the controller must notify data subjects without undue delay (Article 31). According to the 2017 Verizon Data Breach Report (VDBIR)[1], the typical time-to-compromise continues to be measured in minutes, while time-to-discovery remains in weeks or months. In such circumstances, it's essential to have comprehensive threat detection capabilities that can detect issues as soon as they occur.

Threats can materialize internal to the company or externally. They can be on premises or in cloud environments. Therefore, it is important to be able to collect and correlate events quickly; and supplement the information with reliable threat intelligence to stay on top of emerging threats.

There is no one place or tool that will be a fit for all purposes. Sometimes a threat is discovered on the endpoint, the perimeter, or by analyzing internal traffic. Therefore, controls should be placed accordingly in the environment to increase the likelihood of detecting threats as soon as they occur.

Ask yourself:

- Will you be able to identify and respond to a breach as soon as it occurs?
- Are you aware of the types of attacks that your company is subjected to?
- Are employees aware of how to report a breach?

Learn more about threat detection with AlienVault USM >

---

[1] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Step 7: Monitor network and user behavior to identify and investigate security incidents rapidly.

GDPR is focused on ensuring that citizen data is gathered and used appropriately for the purposes it was stated. Therefore, it is important to focus not just on external threats or malware, but also to detect whether users are accessing data appropriately. Context is critical when evaluating system and network behavior. For example, an abundance of Skype traffic in the network used by your inside sales team is probably a normal part of operations. However, if the database server that houses your customer list suddenly shows a burst of Skype traffic, something is likely wrong.

There are many methods that can be deployed to monitor behavioral patterns. One method is to utilize NetFlow analysis, which provides the high-level trends related to what protocols are used, which hosts use the protocol, and the bandwidth usage. When used in conjunction with a SIEM, you can generate alarms and get alerted when your NetFlow goes above or below certain thresholds.

Ask yourself:

- Do you know what “normal” traffic looks like on your network?
- Would you be able to detect if a legitimate user is extracting customer data?
- Would a spike or drop in traffic raise alarms?

Step 8: Have a documented and practiced incident response plan.

To comply with GDPR regulations, organizations should have a plan in place to detect and respond to a potential data breach to minimize its impact on EU citizens. In the case of an attack or intrusion, a streamlined incident response process can help you respond quickly and effectively to limit the scope of the exposure.

If you have unified threat detection controls and processes in place to alert you to an incident, your incident response plan should be able to quickly and accurately determine the scope of impact. You should investigate all related events in the context of other activity in your IT environment to establish a timeline, and the source of attack should be investigated so as to contain the incident.

Once you have contained the incident, you should evaluate if a possible breach of personal data occurred and decide if reporting is required under GDPR. Then, you should prioritize and document all response and remediation tactics. Be sure to verify that your incident response activities have successfully remediated the issue. You will need to inform the regulator of all steps taken, and where necessary, inform any affected EU citizens.

Ask yourself:

- Are all relevant parties informed and aware of what to do in the event of an incident?
- Is the incident response plan practiced to ensure it works under real-world scenarios?
- Is documentation complete and up to date?

Learn more about responding to incidents in our AlienVault Insider's Guide to Incident Response >

Step 9: Have a communication plan in place to notify relevant parties

In the event of a breach, your organization must report to the regulatory body within 72 hours of being aware of the breach. For high-risk events, the controller must notify data subjects without undue delay (Article 31).

The notification given is required to at least:

- Describe the nature of the breach.
- Provide the name and contact details of the organization's data protection officer.
- Describe the likely consequences of the breach.
- Describe the measures taken or proposed to be taken by the data controller to address the breach and mitigate its adverse effects.

Ask yourself:

- Can I identify whether systems in scope of GDPR are affected in a breach?
- Do I have the contact details of the regulatory body that I need to notify?
- If need be, do I have a reliable mechanism to contact affected customers?

Section 3:

How AlienVault USM Can Help You

AlienVault Unified Security Management (USM) provides a unified security monitoring and compliance management platform to simplify and accelerate GDPR compliance readiness. By integrating multiple essential security capabilities into a single platform, AlienVault USM gives you visibility into your entire security posture and simplifies the compliance process.

Starting on Day One, AlienVault USM supports GDPR compliance readiness by helping you detect data breaches, monitor data security, and document your compliance readiness. The unified platform delivers asset discovery, vulnerability scanning, intrusion detection, behavioral monitoring, SIEM, log management, and threat intelligence updates all in a single pane of glass. It's advanced security orchestration and automated incident response capabilities help you to detect and respond to incidents faster and more efficiently, helping you to stop attacks sooner to prevent widespread data breaches.

Learn More

Accelerate GDPR Compliance with AlienVault USM

Video: Compliance Reporting with AlienVault USM

Explore AlienVault USM in our Online Demo

About AlienVault

AlienVault has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and **award-winning** approach, trusted by **thousands of customers**, combines the essential security controls of our all-in-one platform, AlienVault **Unified Security Management**, with the power of AlienVault's **Open Threat Exchange**, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures.

ALIEN VAULT