WALLARM AND GDPR

How Wallarm Can Help You Prepare For The New GDPR Standard

In 2016, the European Commission approved the most significant change in the EU Data Protection Directive since its inception in 1995. The new **General Data Protection Regulation** (GDPR) law becomes enforceable in May 2018. It is designed to strengthen security, give control of personal data to data owners in Europe, and to make sure that data regulations are consistent across all European countries.

As a security company, Wallarm recognizes the importance of data protection laws; we will demonstrate that Wallarm solution itself follows the guidelines and requirements of GDPR and that many of Wallarm's features can help our customers achieve GDPR compliance in their web applications.

WHAT'S IN GDPR?

The General Data Protection Regulation (GDPR) is a new European privacy law due to become enforceable as of May 25, 2018. The new General Data Protection Regulation (GDPR) will replace the EU Data Protection Directive, also known as **Directive 95/46/EC**. These new regulations aim to apply a single data protection standard to all states and citizens of Europe to enforce high-level data protection consistency throughout the EU. (**More on GDPR**)

THE KEY ASPECTS COVERED BY GDPR ARE

- **Who**
  Any organization that controls or processes data located in the EU or which collects or processes data originating from natural persons residing in the EU.

- **Standard Rules**
  Although there is a Supervisory Authority (SA) in each EU country, the laws they enforce are all the same, and a company looking to meet compliance standards has some flexibility to select the lead authority, which will than become a "one-stop shop" for GDPR compliance. This selection may be driven by communications/ language compatibility, physical location of the offices, or other considerations.

- **Privacy by Design and Default**
  One of the biggest innovations in the new regulation is Privacy by Design and by Default (Article 25). This requirement looks at the data protections and requires that the levels of protections be in line with the risks. For example, encryption or pseudonymisation may be required to protect personal data. Another question is whether there are appropriate secure defaults, development and business processes in place to limit data access and retention periods to those necessary.

- **Accountability and Access**
  EU residents have the right to get access to their personal data and information about how these personal data are being stored and processed. This is defined by The Right of Access (Article 15). Citizens can also fight decisions made by algorithms rather than humans. To comply with this and some other requirements, Data Protection Officers need to be appointed (Articles 37–39).

- **Reason and Consent**
  This point is rather obvious. There should be a legitimate business or public reason for needing the data and the person whose data it is should give consent. In the same spirit, Article 17 calls for personal data to be erased without "undue delay" when there is no more legitimate reason for storing the data, or upon the request of the data owner.

- **Data breaches and sanctions**
  While the company has a responsibility to provide adequate controls under GDPR, if a breach does occur, the company has to notify their SA in a timely manner or be subject to stiff fines and sanctions that can reach as high as €20M or 4% of the company's worldwide revenue.

DOES WALLARM COMPLY WITH GDPR?

Wallarm maintains security and compliance within all aspects of its cloud service as well as Wallarm Nodes that are installed on the customer's own infrastructure.

Architecturally, Wallarm solution consists of the Wallarm Nodes installed within a client's infrastructure and under the control of Wallarm's customers and Wallarm Cloud service. Wallarm Node installs as a Linux software module or a Docker container, and it is typically managed by the standard stack of IT management tools. Wallarm Node sends anonymized statistical application traffic metrics to Wallarm Cloud for machine learning analysis. Based on this statistical information, Wallarm Cloud generates application profiles and customized security rules every few minutes.

With regards to the application data, Wallarm consistently uses anonymization techniques.

Unlike encryption and other **pseudonymisation** methods mentioned in the GDPR that are reversible, Wallarm methodology is to calculate statistical application metrics, which strips out identifiable information completely, and thus excludes this information from the scope of the GDPR. For more information about the specifics of the application information that is sent to Wallarm cloud, refer to the **Wallarm Privacy FAQ**.

According to Article (26) of GDPR, "Whereas the principles of protection must apply to any information concerning an identified or identifiable person…whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable."

Thus, the application data used by Wallarm do not fall within the scope of GDPR.

At the same time, Wallarm recognizes the GDPR recommendations as good practices, and, as a SaaS provider, Wallarm looks to **C-SIG** for guidance in the code of conduct that specifies industry recommendations for translating the legal requirements into practical applications of the technical controls.

In addition, Wallarm network is fully compliant with the **NIS Directive**, in anticipation of the May 2018 GDPR compliance deadline.

The only data that potentially can be classified as personal information are corporate contact information for those employees who have been granted rights to access and administer the corporate Wallarm account.

Correct handling of this limited set of data is also ensured by the **Wallarm Terms of Service**.

HOW WALLARM HELPS WITH GDPR

Wallarm provides a number of features that will help enterprises and SaaS providers achieve GDPR compliance for their web applications and mobile applications using HTTPS-based APIs.

- **Protection from unauthorized access — Article 32**
  Wallarm protects vulnerable applications from access by malicious actors. Wallarm protects from OWASP Top Ten vulnerabilities as well as from many of Zero Day, thus reducing the number of possible data breaches and unauthorized accesses.

- **Protection from credential stuffing — Articles 24, 32**
  Credential stuffing are attacks where bad actors attempt to use illegally obtained authentication information in a different context. In many cases (as high as 90%), attackers tend to run credential stuffing attacks against APIs for mobile clients, which is inhibiting common prevention methods such as CAPTCHA. Wallarm protects from such unauthorized access.

- **Access controls — Articles 28, 32**
  Within the Wallarm application itself, every enterprise or SaaS customer is provisioned with a set of access controls for their employees and administrators, limiting the scope and operations to only those necessary.

- **Monitoring and Logging — Article 30**
  Wallarm integrates with corporate SIEM and issue-tracking infrastructure for monitoring and logging. The Wallarm Node is managed by DevOps tools such as Chef, Puppet, Ansible, and Salt. For monitoring and failover, Wallarm uses standard protocols such as SNMP, syslog, VRRP, and CARP.

- **Faster breach detection — Article 33**
  GDPR requires that once a breach is detected, notifications be immediately made to both the individual whose personal data might have been compromised and to the Supervisory Authority. Wallarm helps identify incidents across all the customers' applications in a timely manner as well as pinpoint the exact API where the problem has occurred, making it easier to identify the affected information.

- **Improved risk assessment — Articles 34, 35**
  Wallarm active threat verification capability, where Wallarm replays potential attacks to detect if they can result in a significant exploit, allows customers to properly understand the risks of personal information exposure.

- **Data protections built into the design phase — Article 25**
  Wallarm AST capability moves information protection earlier in the development cycle by creating automated security tests and enabling increased security testing coverage. This is in line with the Privacy by Design doctrine.

CONCLUSION

GDPR is an important compliance requirement, and even though it does not come into effect until May 25, 2018, it makes sense to start preparing and putting in place design and business processes that will make sure that all systems are in compliance by May 2018.

Customers using Wallarm for application protection can have confidence that the service itself is in compliance with GDPR and also that the features of the product help with both risk assessment and implementing systems that are GDPR compliant across the board.

ABOUT WALLARM

Wallarm is an innovative AI startup focused on web application and API security. With the help of machine learning, Wallarm reconstructs application context and API logic by looking at application requests and responses and uses this information to automatically create custom security protection rules for each application release, making it a great fit for CI/CD environments with frequent releases. Founded in 2013, Wallarm has already helped hundreds of SaaS and enterprise customers discover and fix critical vulnerabilities, automate web application and API runtime protection and prioritize security risks. Wallarm is a privately held company headquartered in Menlo Park, California and backed by Y-combinator, Partech Ventures, and other investors.

wallarm.com
100 Produce Dr. Suite L, South San Francisco CA 94080
(415) 940-7077