Complying with the EU GDPR

Mist Systems treats security as our highest priority obligation to our customers. This document outlines for Mist Systems customers how Mist is addressing the EU General Data Protection Regulation (GDPR).

The GDPR provides a personal data privacy and protection framework across the European Union. It takes effect on May 25, 2018. The GDPR prescribes strict data hosting and privacy rules that protect EU residents, even if their data is processed or hosted outside of the EU.

EUROPEAN UNION - GLOBAL DATA PRIVACY REGULATION

Under the GDPR, Mist customers are considered data controllers. Mist is a data processor. When a customer decides to deploy the Mist solution in its offices, retail business, or other environment, the customer is deciding to deploy a wireless local area network (LAN) using Mist Access Points that collect and process end user device information in order to offer additional services (e.g., way finding) or better manage that wireless network. Under the framework of the GDPR, data subjects are individuals permitted by Mist customers to access the customer's LAN. The GDPR requires data controllers to establish a legal basis to process their personal data, explain how personal data will be used, and in some cases, obtain consent from individuals. Data processors like Mist are obligated to process that personal data only as contractually instructed. This overview is not intended to cover the GDPR requirements for notice, consent (or other lawful basis for processing personal data) or opting out. This overview is intended to help Mist customers understand how deploying a Mist solution might trigger obligations for GDPR compliance, and how Mist maintains GDPR compliance as a data processor.

First, it's important to understand what level of personal information Mist processes for its customers. Only network management information (and no user traffic) flows from devices to the Mist Dashboard. A very limited set of device data is processed by Mist Systems. Mist collects device name, device type, operating system, MAC address, IP address, username, and signal strength of Mist APs ("Metadata"). In addition, if a customer has purchased location enabled services, Mist will process a device's geolocation information. The Metadata is owned by Mist customers. Mist does not associate this information with any other database that might enable Mist to determine the identity of an individual user.

Here is an overview for the steps Mist has taken to address the GDPR and data security requirements of Mist customers.

Information Security Program

Mist Systems has an active information security program administered by its Chief Information Officer (Mist's Data Protection Office). Mist has developed and adopted information security policies designed to protect the confidentiality, integrity and availability of device data and sensitive customer information

Data Security

The Mist Dashboard servers are hosted in a SOC2 Type 2 compliant datacenter; communication between Mist APs and the Mist Dashboard is encrypted; data within the cloud is stored using AES-256 encryption; a customer's access to the Mist Dashboard is secured by an https connection, using 2048-bit RSA key. Other security practices include:

- Audit logs are captured at a secure, centralized location.
- Principles of granting minimal privileges, access, and services are used.
- User access is highly restricted.
- Security is integrated within the development cycles and vulnerability scans are performed prior to releasing the code to production environment.
- Mist performs web security testing from the development to production stages.
- Mist scans for SQL injections, XSS and 700+ other vulnerabilities, including the OWASP Top 10.
- Mist software is continuously audited by the security team to prevent usage of shared secret keys.
- Refer to the Mist Security Technical Brief for further details of how we secure the Mist system.

Customers Can Authorize Mist to Access Metadata for Support

The Mist solution is designed to give customers options for how much device data Mist is able to access. For example, Mist customers have the option to temporarily authorize Mist Systems personnel to access and see that customer's metadata processed by the Mist Dashboard, if desired. The Mist Dashboard provides a simple switch that allows a customer to turn on/off access to Mist Systems personnel from viewing or accessing device metadata collected from the customer's employees, visitors or customers. The device metadata is still processed on the Mist Dashboard and visible to the customer. Mist believes this option allows the customer to have a higher level of security for its device data. Unfortunately, there is a trade-off with this higher level of security. Whenever a customer experiences a technical support issue with their Mist APs or the Mist Dashboard, Mist uses metadata to troubleshoot the issue, isolate the potential causes and provide a remedy to the customer. Without access to the metadata, Mist Systems has very limited ability to assist customers with technical support issues. The customers have the option of enabling Mist access, during technical troubleshooting, and disabling upon resolution. We believe this is an important available option for customers to control for the highest level of security for their data.

EU Mist Dashboard

Mist Systems is deploying an instance of the Mist Dashboard within the EU so that device data for customers who are based in the EU is processed and stored only in the European Economic Area (EEA). With the availability of the EU Mist Dashboard, customers can deploy their Mist powered network without any concern about transferring any personal data outside the EEA. However, even if it were necessary for Mist Systems to access this data, Mist provides the same level of protection for device data as is applied in the EU and the customer still has control to enable/disable this access, as desired.

Data Processing Addendum (DPA)

Mist Systems makes available to its EU based customers a standard data processing addendum incorporating the European Commission's Standard Contractual Clauses (SCC) to ensure alignment with GDPR requirements. The DPA provides customers with greater clarity and assurance as to how Mist will process and store personal data, if any. A copy of this addendum can be requested from the Mist support portal for active customers.

Pseudonymization

Article 4(5) of the GDPR defines pseudonymization as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information." With the limited, Metadata processed by Mist, we believe it is already pseudonymized as it is not possible for Mist to identify a specific individual without combining the Metadata with additional information. While Mist customers may have such additional information that, when combined with the Mist device data, enables identification of the data subject, Mist Systems does not require and does not seek this information. In order to allow Mist to continue to use a portion of the Metadata for product development, research, and industry reporting, Mist removes all usernames and MAC addresses from its database used for these purposes.

Mist Systems appreciates our customers' concern for data security and data privacy. We are committed to complying with applicable data protection and privacy laws, including the GDPR. Mist will continue to provide updates regarding compliance with GDPR, including details on how MIst plans to assist customers in responding to requests from data subjects about the personal data that is processed or stored as part of our customers deployment of the Mist solution.