Libraesva and GDPR

This document applies to the Libraesva Email Security Gateway and to the Libraesva Email Archiver.

Introduction

The GDPR is not the first privacy legislation: it builds and improves over existing legislations that already defined strict requirements for the management of personal data and clear responsibilities and roles for the “data processor” and the “data controller”.

If you manage personal data you were already subject to privacy regulations before the GDPR. Privacy requirements in the GDPR aren’t completely new or totally different from the legislation that predates it.

GDPR introduces some new important concepts like “privacy by design”, which is mostly about company processes and encourages those already widely used “good practices”.

So, nothing completely new but still it is a good opportunity to review our privacy and security posture.

The following paragraphs provide clarifications that can help identifying the role of the Libraesva appliances in relation to personal data.

Remember: the focus of the GDPR are the processes, not the tools.

Libraesva ESG and Archiver on-premise

Libraesva is ISO27001:2017 certified for “software design, development and support in the security field” and for “provision of cloud services”.

In an on-premise installation of the Libraesva appliances, Libraesva provides you with the software, the security updates and the support services. You provide the infrastructure and the management.

In this configuration the data is stored on your own infrastructure and Libraesva does not have access to it.

The appliances do not provide to Libraesva any personal data. The emails and their metadata always remain on your own appliance within your own infrastructure.

Libraesva does not have any administrative right on your appliance. You get to decide what is stored, for how long and who has access to the data with which privileges.

Libraesva can gain access to your appliance only through the “remote support” feature. The “remote support” is possible only if initiated by yourself through the web or console interfaces of the appliance. Libraesva cannot autonomously connect to the appliance, only through the active action of enabling the “remote support” connection, which can be done only by the administrator of the appliance.

The “remote support” is an exceptional measure that may be agreed, if necessary, with our support service during the management of a support ticket. Outside of this remote support context, we cannot access your appliance.

Libraesva ESG and Archiver as cloud services

If you are also buying from us the Libraesva cloud service, all of what has been said above about the on-premise setup applies to you, but there’s more.

When your appliance is in our cloud we are also providing the hosting service. Your appliance is still private and you retain all of the administrative rights, however in this case we also provide the infrastructure, therefore we are a processor in relation to the data.

We provide the cloud service through cloud infrastructure operators that adhere to the CISPE code of conduct. You can read in this code of conduct all of the details about the security and privacy of the infrastructure.

Please note that our model is the “private cloud” model: you have your own virtual machine and your retain full administrative control over your appliance, just like in the on-premise scenario. Libraesva personnel can access data associated to customer appliances for the purpose of providing customer support, incident management, diagnose issues and in any circumstance where this should be needed in order to guarantee the service.

NOTE: On the Libraesva Archiver you can choose where to store the email archive. You can set-up data volumes outside of the infrastructure provided by Libraesva, for example you can use S3 or S3-compatible buckets as your email storage. In this case the data is not stored on

Libraesva's infrastructure.

Libraesva PhishBrain cloud service

PhishBrain is a cloud service provided by Libraesva through Libraesva's cloud infrastructure and through cloud infrastructure operators that adhere to the CISPE code of conduct. You can read in this code of conduct all of the details about the security and privacy of the infrastructure.

Currently PhishBrain cloud service is hosted in Europe (Italy), UK (London), US (New York). Customers get to choose the region at account creation time.

Data submitted to phishing pages is not collected nor stored.

PhishBrain manages the following personal information of account administrators and recipients of phishing campaigns: name, email address, phone number (if provided), ip address of user actions on phishing campaigns (opening, clicking, submitting data). Administrators are in charge of collecting consent from recipients.

Libraesva LetsDMARC cloud service

LetsDMARC is a cloud service provided by Libraesva through Libraesva's cloud infrastructure and through cloud infrastructure operators that adhere to the CISPE code of conduct. You can read in this code of conduct all of the details about the security and privacy of the infrastructure.

Currently LetsDMARC cloud service is hosted in Europe (Italy), UK (London), US (New York). Customers get to choose the region at account creation time.

LetsDMARC manages the following personal information about the users of the service: name, email address.Such customer data is stored in the region the customer chooses to create the account in.

Data breach requirements for cloud services provided by Libraesva

When Libraesva provides the cloud service, Libraesva is the **processor** and the customer is the **controller** of the data.

As a processor, Libraesva must notify a data breach to the controller without undue delay after becoming aware of it (GDPR Art 33(2)).
If Libraesva becomes aware of unauthorized access to any customer personal data and such unauthorized access results in loss, disclosure or alteration of that data, Libraesva will notify the customer without undue delay. The notification will describe the nature of the security breach, the consequences of the breach and the measures taken or proposed in response to the incident.

Taking into account the nature of the processing and the information available to the processor, Libraesva will assist the controller in ensuring compliance with its obligations to notify data breach to the supervisory authority and data subjects (GDPR Art 28(3)(f)).

In the event of a data breach the client has the right to terminate immediately the contract.

Libraesva ESG features for the privacy

Libraesva ESG provides the following privacy-related features which you can take advantage of in your path towards the compliance to the GDPR.

- “Right to erasure” or “right to be forgotten”: with a single operation you can easily erase all of the information about one user, both from the email archive and from the metadata
- BEC (Business Email Compromise) protection engine: it prevents targeted attacks impersonating company managers (also called “whaling”)
- DLP (Data Loss Prevention) engine: prevents accidental loss of sensitive information
- Logging: all of the logs can be archived remotely in real time through the standard rsyslog protocol
- Auditing: all of the sensitive information are logged in an non-erasable audit log
- Email tracking prevention: removes beacons in emails that can track the phisical location of the reader and gather intelligence about working habits

- Phishing and malware protection: over 90% of the data breaches start in this way

Libraesva Archiver features for the privacy

Libraesva Archiver provides the following privacy-related features which you can take advantage of in your path towards the compliance to the GDPR.

- Privacy officer: if assigned to a tenant, the privacy officer authorization will be required for any access to personal data, including by system administrators
- Encryption: the whole email archive can be encrypted with AES-256
- “Right to erasure” or “right to be forgotten”: the administrator can delete all email related to an individual and purge the data from the storage
- Auditing: a non-modifiable and non-deletable audit log logs all the data access operations from any user
- Certified timestamping: RFC3161 certified timestamp is automatically applied to all archived email and verified every time an email is retrieved
- Granular user role dfinition: user roles are defined as collections of over 80 capabilities and user roles can be created to match the company policies