mailsphere

GDPR compliance

Why is GDPR coming into force?

GDPR is intended to update the existing Data Protection Directive of 1995 to bring them inline with the 21st century, creating a "harmonized, stronger & more coherent" data protection framework, backed by stronger enforcement, in all 28 EU Member States.

The update aims to account for two developments of the past few decades: the substantial increase in cross-border data flows in Europe's internal market, and the scale of personal data collection, use, and sharing enabled by rapid technological developments and globalisation. The GDPR aims to ensure a harmonised, consistent, and high level of protection of individuals in the EU, provide more confidence among the public about the protection of their data, especially with regard to online activity, and provide greater legal certainty for businesses.

At a time of increased cybersecurity threats and reports of large scale data breaches this must be welcomed by businesses. A clear framework to ensure better data security and demonstrable protection of individuals data assets. Allowing businesses to provide guarantees to individuals around their personal data being managed within a company's IT systems.

Who does GDPR apply to?

- Data "controllers" and data "processors." Specifically, any business that determines the purposes and means of processing personal data is considered a "controller." Any business that processes personal data on behalf of the controller is considered a "processor."
- Companies (controllers and processors) established in the EU, regardless of whether or not the processing takes place within the EU.
- Companies (controllers and processors) not established in the EU offering goods or services within the EU or to EU individuals.

Creating a "harmonized, stronger & more coherent" data protection framework.

What does this means for businesses?

The GDPR covers a range of topics applicable to your business, such as the rights of the individuals whose data is processed, what the data can be used for, and member state authorities to enforce the GDPR. Additionally, there are some key requirements related to what covered entities must do when it comes to securing, managing and using personal data:

- Security of processing. The GDPR requires controllers and processors to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk". The GDPR also requires that controllers shall only use processors that provide "sufficient guarantees" to implement appropriate technical and organisational measure to meet the GDPR's requirements.
- Notification requirements. In case of a personal data breach, the controller must notify the supervisory authority where feasible, not later than 72 hours after becoming aware of the breach. In addition, a processor must notify the controller without undue delay after becoming aware of a breach.
- Fines. Infringements of certain provisions of the GDPR can be subject to administrative fines up to €10-20 million, or up to 2-4% of a company's total worldwide annual revenues of the preceding fiscal year.
- Data protection audits. The GDPR gives data protection authorities investigative powers to carry out data protection audits, and also allows data controllers to conduct or mandate audits on processors. This language is designed to shift the focus of businesses away from organising their efforts to pass formal audits to maintaining regard for advanced cybersecurity technologies and data management practices.
- Provision of remedies. The GDPR defines multiple rights around personal data and the data subject being granted the ability to gain explanation, request change, removal, transfer or suspension of processing using their data.

Mailsphere is commited to supporting businesses meet full GDPR compliance, through the provision of advanced email security and easy identification of personal data.

Key Definitions

"Personal data"

Any information relating to an "identified or identifiable natural person" (the "data subject"). An identifiable person is "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."

"Processing"

Processing of data is also defined quite broadly - it includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction... and these operations can be automated or manual.

"Right to be informed"

This encompasses the obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how personal data is used.

"Right of Access"

Allows the data subject to know whether or not personal data is being processed and gain access to that personal data. This includes information about its purpose, the categories of data concerned, recipients whom the personal data have been disclosed to, the envisaged period for which the personal data will be stored and any available information as to its source.

"Right to rectification"

This requires that the controller will take action to correct errors in personal data or restrict further processing of personal data or to cease such processing altogether.

"Right to to erasure"

Or "Right to be forgotten" allows a data subject to have the his or her personal data erased and no longer processed.

"Right to restrict processing"

Ensure the data subject can exclude their data from being used in processing.

"Right to data portability"

Where data has been collected regarding a data subject, this ensures that the data can be moved from one operator to another with conditions that it does not adversely affect the rights and freedoms of others and where technically feasible.

"Right to object"

Prevents personal data being used for processing - in particular where automated decisions are being taken based on this data.

GDPR Compliance through Mailsphere

As well as providing advanced security for corporate email it is important to recognise that Mailsphere is also regarded as a processor within GDPR, as a result of storing email communications in the secure archive.

When a company is in receipt of a request under GDPR, Mailsphere will provide a dedicated process to manage the claim in relation to email data stored within the corporate email archive.

This process will support the following capabilities:

- Case Management - Enabling a new case to be managed within the Mailsphere portal.
- Data Identification - Through the advanced search facility, email can be searched and identified. Once identified the email can be assigned to the pending GDPR case. For users with full access permissions the email content can be reviewed either online or through a downloaded copy.
- Authorisation - Through a pre defined group of authoritative users within the company, when a case is submitted for authorisation the members of this group will be notified. Based on compliance rules a predetermined number of authorisers will need to approve the request for it to continue.
- Erasure - Once a case has been authorised the identified data will be purged from the company's archive with a autitable log of the process stored for future reference - excluding any personal data related to the data subject.
- Full audit of GDPR case management will be preserved within Mailsphere while ensuring data subjects identify is masked.

1

Identify

2

Analyse

3

Authorise

4

Erase