MailStore Advisory

Email Archiving and the EU's General Data Protection Regulation (GDPR)

The future of European data protection begins on 25 May 2018, when the General Data Protection Regulation (GDPR)[1] becomes effective in the EU.

The new regulation represents a broad-reaching harmonization of data protection laws in the EU. In the past, regulations varied greatly from country to country. The end goal is standardization, and a simpler process, but there will be new challenges in understanding the regulations, and determining the most effective way to comply with them. The new regulations affect all EU companies – and many of the companies outside the EU that collect or utilize data of EU residents.

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Here are some areas of data protection the GDPR will touch upon:

- Technical and organizational security measures such as the encryption of data
- Audit requirements when using IT systems to store and process personal data
- Documentation of consent when processing personal data
- Strict requirements on the design of consent and the purpose when processing personal data
- Rights of individuals regarding personal data (i.e., right to erasure)
- Sharing data across geographic regions
- New regulations on sharing data internationally, scope of international applicability of the GDPR, and the introduction of a supervisory authority as the lead authority and sole point of contact (acting as a one-stop shop)

All aspects of business operations are affected by these items. Data protection will play a greater role in the day to day processes of a company due to the new possibilities of imposing sanctions: fines of up to 4% of the annual worldwide turnover or €20 million and the ability to hold managing directors and executive boards personally liable.

What is a major prerequisite for meeting the compliance requirements?

One major prerequisite for compliance with the GDPR is to maintain orderliness and transparency when handling personal data. That includes everything from data collection to storage, access, and processing to deletion/erasure of the data.

Email archiving is a crucial element of any data governance policy. Professional email archiving makes it significantly easier to carry out data governance at a company. Without using a professional email archiving solution, many companies have little control of where and how email is used and accessed. It is often unclear where email is stored, whether additional local copies exist, and whether email records are complete.

How does MailStore Server support customers to enable GDPR compliance or a corresponding data compliance policy?

It is a duty of the entire company to comply with the organizational, technical and administrative provisions of the GDPR. In this regard, MailStore Server can help you immensely with implementing data compliance for email communications.

Several requirements in the GDPR are based on requirements from other local regulatory bodies. The point is to provide a high level of coverage in terms of the protection goals for IT security.

MailStore Server enables you to ensure the completeness of your company email archives. It has featured functions that support you in your data compliance and in turn with compliance with the GDPR. Here are some ways the MailStore Server helps you manage your email archives, and comply with GDPR:

Efficient, fast full text search function

- The integrated functions in MailStore Server enable you to search for and extract data from all emails and file attachments. It means you can efficiently provide requested information to third parties and you can provide timestamped proof of email access history.

Retention periods

- Specific personal data and related documents need to be stored in an auditable manner and protected from deletion and manipulation in accordance with local, federal or industry specific statutory periods. The right to erasure stands in opposition to this. MailStore Server provides features for erasure and storage management that comply with both requirements. You are therefore able to erase data that has been archived in an auditable manner in accordance with the GDPR and prove it has been carried out.

Security best practices

- The encryption methods employed by MailStore Server protect archived data, and the options provided by the permissions feature enable you to reduce the number of people authorized to consult the data to a minimum, in compliance with GDPR. A cryptographic signature that can be added to exported emails ensures that exported emails remain protected from tampering, even outside of the archive.

Automated audit log

- MailStore Server also features an audit log that provides you with seamless and detailed log of the activities within the archiving system.

Note: To comply with GDPR, there may be further technical and organizational security measures that the user and/or their service provider needs to perform in a specific workflow organization, in addition to the corresponding use and configuration of MailStore Server.

For more information on MailStore Server

Further information about other security and compliance enablement features of MailStore Server can be found under:
https://www.mailstore.com/en/products/mailstore-server/compliance-features/

If you have further questions regarding email archiving and MailStore Server, our sales team is happy to help:

MailStore Software GmbH
Cloerather Str. 1-3
41748 Viersen
Germany

Email: sales@mailstore.com
Phone: +49-2162 50299-12 (international)
Phone: +1-800 747-2915 (U.S.)
www.mailstore.com