FAQ

Mimecast & GDPR Compliance

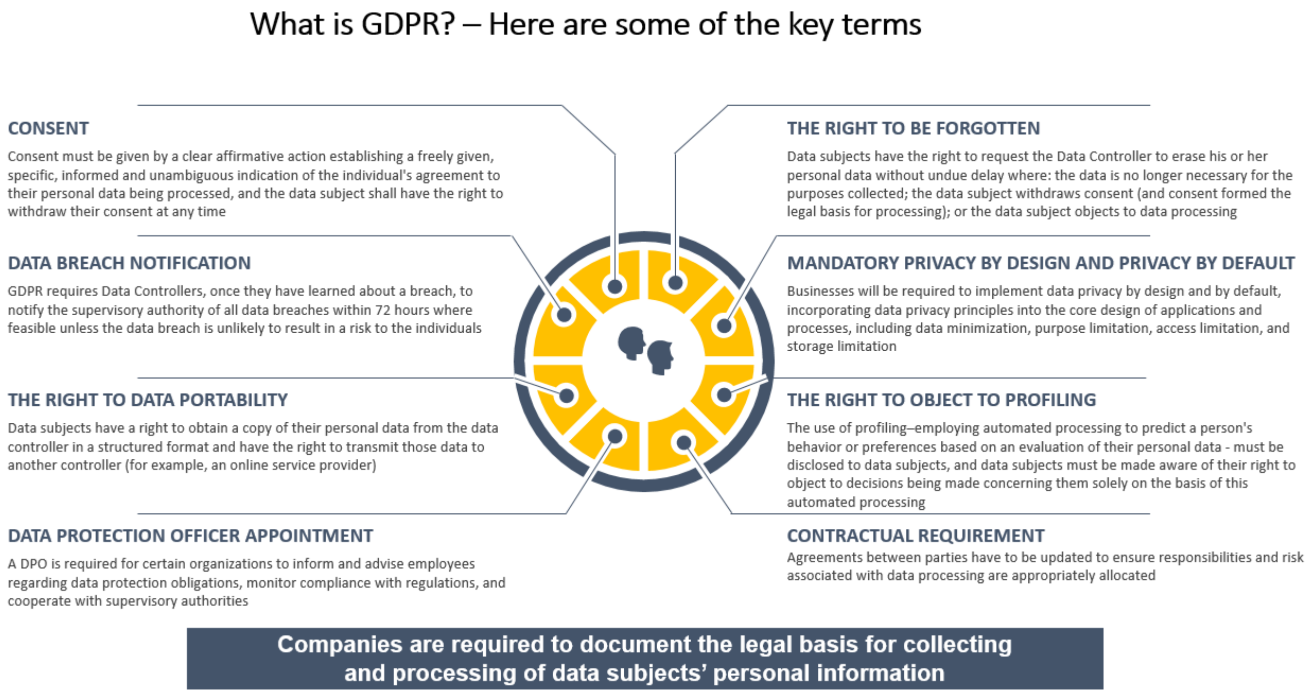
Contents

Please be advised that this FAQ is not intended to provide legal advice regarding your requirements under the GDPR. Please contact your legal team if you have any questions regarding your organization's compliance obligations with the regulation.

What is the GDPR?

The General Data Protection Regulation (GDPR) is the new data protection regulation from the European Union (EU), with an enforcement date of May 25, 2018. Organizations anywhere in the world that collect or process personal data in the EU must comply with the new regulation.

Some key concepts and terms:



What is GDPR? – Here are some of the key terms

CONSENT

Consent must be given by a clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the individual's agreement to their personal data being processed, and the data subject shall have the right to withdraw their consent at any time

DATA BREACH NOTIFICATION

GDPR requires Data Controllers, once they have learned about a breach, to notify the supervisory authority of all data breaches within 72 hours where feasible unless the data breach is unlikely to result in a risk to the individuals

THE RIGHT TO DATA PORTABILITY

Data subjects have a right to obtain a copy of their personal data from the data controller in a structured format and have the right to transmit those data to another controller (for example, an online service provider)

DATA PROTECTION OFFICER APPOINTMENT

A DPO is required for certain organizations to inform and advise employees regarding data protection obligations, monitor compliance with regulations, and cooperate with supervisory authorities

THE RIGHT TO BE FORGOTTEN

Data subjects have the right to request the Data Controller to erase his or her personal data without undue delay where: the data is no longer necessary for the purposes collected; the data subject withdraws consent (and consent formed the legal basis for processing); or the data subject objects to data processing

MANDATORY PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

Businesses will be required to implement data privacy by design and by default, incorporating data privacy principles into the core design of applications and processes, including data minimization, purpose limitation, access limitation, and storage limitation

THE RIGHT TO OBJECT TO PROFILING

The use of profiling–employing automated processing to predict a person's behavior or preferences based on an evaluation of their personal data - must be disclosed to data subjects, and data subjects must be made aware of their right to object to decisions being made concerning them solely on the basis of this automated processing

CONTRACTUAL REQUIREMENT

Agreements between parties have to be updated to ensure responsibilities and risk associated with data processing are appropriately allocated

Companies are required to document the legal basis for collecting and processing of data subjects' personal information

GDPR only affects EU-based organizations, right?

Untrue. The GDPR applies to almost every organization around the world that collects or processes data within the EU. Applicability of compliance requirements is thus based on the location where the personal data is collected, processed and/or stored, not the location of the organization.

What constitutes "Personal Data"?

Personal data is defined as "any information relating to an identified or identifiable natural person ... who can be identified, directly or indirectly ... by reference to an identifier." Identifiers listed in the GDPR include name, identification number, location data, and other online identifying factors, such as physical, mental, and cultural, among others.

Why is it so important to address email and its data stores as part of GDPR readiness?

Over 90 percent of cybercrime exploits begin with email, making it the single biggest threat vector to organizations and the data they manage. Furthermore, not only are emails a common vehicle to share and exchange personal data; email servers are prime repositories for data as names, email addresses, and associated contact information.

It's therefore critical to ensure appropriate protection is in place (including defense against attacks, encryption, data leak prevention etc…) along with a review of what personal data is being retained and how easily it can be accessed by authorised personnel.

How can Mimecast help customers manage the GDPR?

While Mimecast can aid our customers' GDPR compliance efforts, it is important they evaluate their individual requirements for GDPR compliance based on an analysis of their systems, processes and the types of personal data that are collected, processed and/or stored. Mimecast can help customers in their GDPR compliance journey in the following ways:

- The Mimecast Email Security Gateway with Targeted Threat Protection helps customers defend against various forms of email-borne attacks (including phishing, ransomware and impersonation) that can lead to the loss of personal or sensitive data that is subject to GDPR compliance requirements. Protection also extends to data leak prevention (DLP), Secure Messaging and secure large file sharing capabilities.

- The Mimecast Cloud Archive is an immutable repository of all email communication and metadata. It offers fine-grained control – including fast e-discovery, smart tagging, case review and data export tools – to support our customers' IT administrators, compliance and legal teams with their responsibility to respond quickly to data subject requests exercising their rights under GDPR. More information on supporting Data Subject Access Requests can be found in our KB article here. Administrators can also configure distinct archiving policies for individuals or groups that work intensively with customer information or other forms of personal data. An integrated backup and recovery capability helps eliminate data silos.

- Mimecast's Mailbox Continuity service ensures always-on access to email and data, for end users, administrators, compliance and legal personnel. Mimecast helps ensure email can continue to flow and authorised people can access the archive for search and compliance support needs at all times. Whether email is on-premises, in the cloud or hybrid, we offer a 100% uptime SLA to protect against breaches impacting email, natural disasters, human error or technology failure.

- All Mimecast services are managed from a single, web-based console, with all actions logged and auditable to support compliance.

Find more information on how Mimecast services can support your GDPR compliance efforts by visiting https://www.mimecast.com/solutions/archive/gdpr-for-email/

How is personal data stored in the Cloud Archive?

The Mimecast Cloud Archive provides tamper-resistant storage protecting the integrity of stored personal data. Immutable audit logs keep a record of all access to the Cloud Archive, including searches performed and archive messages viewed.

Real-time notifications and additional security options selected by our customers are enforced for each search by entering a "search reason", which is logged for audit purposes.

Granular role-based controls determine the level of access IT administrators have and tasks they can perform, such as viewing specific personal data or exporting a restricted set of data within the Mimecast Cloud Archive.

Can Mimecast assist customers in limiting the amount of personal data that is retained in accordance with the GDPR?

Retention of messages containing personal data is automatically managed based on our customers' predefined settings. Retention schedules can be adjusted or customised using various attributes such as content, people, location or department.

In cases where GDPR data retention requirements apply, IT Administrators may need to remove messages containing personal data from the Cloud Archive permanently (known as a purge) or reduce the time these messages are stored there.

Adjustments can be set to either expire emails immediately or to expire emails after a certain number of days. Retention adjustments cannot be used to extend the retention period of emails beyond maximum retention settings.

Mimecast uses a single instance storage service, meaning any email that is subject to a retention adjustment is updated or expired in its entirety for all recipients of the message. Once a message is expired it is not recoverable.

Can Mimecast offer customers complete GDPR compliance?

No. GDPR compliance requirements extend well beyond email-centric security, resilience and operations, and involves privacy and governance processes wherever personal data is stored or processed (e.g., customer records, contact databases, CRM systems, ERP platforms etc). Email resilience and management is only part of the story.

Will Mimecast products and services comply with requirements under the GDPR?

A dedicated team has been established to align GDPR compliance requirements with our products and services. You can read our public commitment here.

Has Mimecast appointed a Data Protection Officer (DPO)?

Yes, we have appointed Mark Bilbe as our DPO. You can find more information about the DPO on the GDPR Center. Mark can be contacted at DPO@mimecast.com

Is Mimecast a data processor or data controller?

As it relates to most of our products and services that we provide to our customers, Mimecast serves as data processor. For most Managed Service Provider (MSP) customers, we are a sub-processor. Through the administration of our business operations, generally speaking, we function as a data controller.

Has Mimecast commenced a gap analysis of GDPR requirements against its current operating model?

Yes, both systems / applications and processes are being risk assessed through Data Protection Impact Assessments (DPIAs).

What has Mimecast done to meet the GDPR requirements of Privacy by Design and Privacy by Default?

We have implemented appropriate technical and organizational measures designed to protect personal data that you can read more about here.

Has Mimecast implemented have controls implemented to monitor, detect and report a personal data breach?

Mimecast has a formal incident reporting process. All Mimecast staff who deal with customer systems are trained on what constitutes a personal data breach and how to report it. The incident management roles and responsibilities of Mimecast staff, contractors and third-parties are formalized and documented. Mimecast has established an Incident Response Team, which includes regional incident handlers for each territory of operation. Mimecast implements the SANS Institute Six-Step Incident Response Methodology that covers: 1. Preparation; 2. Identification; 3. Containment; 4. Eradication; 5. Recovery; and 6. Lessons Learned.

Has Mimecast implemented data security policies such as Breach Notification, Privacy Statement and Information Security?

Yes, Mimecast has implemented certain security policies designed to protect personal data. Our Privacy Statement and Information Security Policy are available on our website. https://www.mimecast.com/privacy-statement/

What process does Mimecast have in place to notify customers or data subjects when the intended use of their data changes?

Mimecast provides an option for customers and data subjects to subscribe to receive updates to any changes in key GDPR policies through the Mimecast Preference Center here.

Does Mimecast conduct privacy awareness/training for employees with access to personal data?

Yes, Mimecast staff attend Information Security Awareness training both as a new starter and through regular reinforcement.

Do Mimecast employees follow Security Policy?

As a general rule, Mimecast employees, contractors and applicable third parties are responsible for implementing and acting in accordance with Mimecast's security policies, including our Information Security Policy found here. These requirements include:

1. Protecting assets from unauthorized access, disclosure, modification, destruction or interference;
2. Executing relevant security processes or activities specific to their role; and
3. Reporting security events and incidents or potential events or other security risks to Mimecast

Does Mimecast contract with third party sub-processors that may also have access to customer personal data?

A list of Mimecast sub-processors with potential access to customer data can be found at https://www.mimecast.com/company/mimecast-trust-center/gdpr-center/sub-processors/

A Data Processing Agreement (DPA) and other contractual requirements are in place between Mimecast and its sub- processors to ensure the appropriate privacy and security control measures are in place to secure personal data.

Does Mimecast have a documented process for correcting inaccurate personal data when asked by a data controller?

Mimecast is able to provide assistance to customers where necessary to correct any customer data held directly by Mimecast.

We also have a KB article to help customers process these requests - https://community.mimecast.com/docs/DOC-2972

What certifications does Mimecast hold and what standards has Mimecast attained in respect of data security and/or data protection?

At Mimecast, we hold ourselves to high security and privacy standards. We have implemented security and data protection measures that span the technology, operations, and legal aspects of protecting customer data, including GDPR. We constantly undertake and maintain numerous certifications and audit reports to provide transparency and communicate internal controls to our customers and partners.

The list of certifications, attestations, and assessments achieved by Mimecast include the following:

- ISO 22301 Certification: Business Continuity Management System (BCMS)
- ISO 27001 Certification: Information Security Management System (ISMS)
- ISO 27018 Certification: Protection Controls for Personally Identifiable Information (PII)
- SOC 2 Attestation Report: Internal Controls for Security, Availability, Processing Integrity, Confidentiality, and Privacy
- HIPAA/HITECH Compliance Assessment Report: Protection and Security of Patient Information

Additional information about Mimecast certifications, attestations, and assessments is available in our Trust Center.

Has Mimecast self-certified under the EU-US Privacy Shield to address transfer of personal data out of the EU to the US?

Yes, Mimecast has filed our certification with the US Department of Commerce.

Does Mimecast transfer data between data centers outside of the EU?

Customer data is hosted in the hosting jurisdiction indicated on their purchasing documents, Mimecast is a global organization with a global support model. Email metadata is viewable to our support personnel globally because we provide a “follow the sun” support model. The locations from where we provide support are identified in the Trust Center here. Additionally, the content of email may be accessed by a small set of Mimecast personnel outside of the specified hosting jurisdiction in order to: (i) address a specific support query (and, in such case, customer email content will only be accessible after a customer grants permission); (ii) to ensure the proper working of the systems; or (iii) as otherwise stated in our agreements with customers. Any such access rights are restricted to a small set of personnel who have to be approved by our security team and assigned specific roles. Any access would need to have a logged reason and ALL ACTIVITY is visible on our customer’s audit log. Therefore, our customers are aware of access to their data. Additionally, all such access is confirmed and monitored by the Mimecast security team.

Do Mimecast products have data retention periods identifying what data should be retained and when it should be deleted?

Customers control the retention / destruction settings for their data through their accounts. Customers’ data retention periods are reflected in their account settings and, depending on the package purchased, policies can be created where specific data can have differing retention settings. Data is deleted after the retention period expires using Mimecast proprietary software.

What processes does Mimecast provide to ensure governance and audit over elevated access rights on information systems?

Mimecast’s web applications do not give Mimecast support staff the ability to read or access a customer’s email content unless access is granted by the customer’s administrator, in order to ensure the proper working of our products, or as otherwise stated in our agreements with customers. If, for example, our customer opened a help desk ticket, our customer support would be able to view email metadata only for the purposes of troubleshooting. If further analysis is required, the customer would have to manually grant access to view the content of the email. Access rights are restricted to a small set of personnel who have to be approved by our security team and assigned specific roles. Any access would need to have a logged reason and ALL ACTIVITY is visible on our customer’s audit log. Therefore our customers are aware of access to their data. Additionally, all such access is confirmed and monitored by the Mimecast security team.

Please provide details of what security measures are used to protect personal data (including backups).

Mimecast takes the protection of personal data, in fact all customer data, very seriously. You can read more about the technical and organizational security measures we have taken here.