mimecast

SOLUTION BRIEF

Simplify GDPR Compliance for Email

The new European Union General Data Protection Regulation (GDPR) gives EU residents more control over how their personal data is used. It's a positive step forward for individuals' privacy rights, especially considering the opportunities and risks of the internet and digital economy. It's also intended to help make data protection law simpler and clearer for companies and government agencies. It does however impose new obligations on organizations globally that market, track, or handle personal data of EU residents.

GDPR will become effective on May 25, 2018. Organizations must demonstrate they have proper controls over the processing and security of personal data, including how data is used, stored, kept up to date, accessed, transferred and deleted. EU residents can also request organizations with personal data about them to stop using it, transfer it or ultimately, delete it. It's therefore imperative that organizations review – and likely overhaul – the way they handle personal data today, or face the potential for substantial fines up to €20 million or 4% of global revenue, whichever is greater.

GDPR's Implications for Email

Personal data is a broad category that includes information relating to identifiable natural persons, such as names, email addresses and phone numbers. By design, email systems hold a huge volume of personal data and remain the number one attack vector, including phishing and ransomware. GDPR obligations demand that organizations take sufficient steps to secure email and the data it holds. They must also manage live, backup and archive copies of data with the same level of rigor.

This is particularly painful for organizations that maintain backup tapes, since GDPR could potentially require the recall and erasure of all data related to an individual. Using a cloud-based archive can help minimize risk and allow a swift response to an individual's access and possible deletion request. Adequately protecting email systems against attack, whether on-premises, in the cloud or hybrid deployments, becomes even more essential. Basic email security like spam and virus protection don't go far enough, with the latest advanced security needed to thwart ever more sophisticated and determined attackers.

KEY CAPABILITIES:

- Commitment to GDPR compliance across services and corresponding contractual assurances
- Single-console management of comprehensive email cyber resilience, covering security, archiving, and continuity
- Advanced email security designed to protect against the latest attacks
- Flexible configuration, allowing tiered or department-specific policies
- Integrated archive, backup and recovery with single-instance storage
- Fast, powerful archive search, e-discovery and review
- Unlimited concurrent searches and number of mailboxes per search
- Robust encryption of data at rest and in transit

Mimecast Services Supporting GDPR Compliance

Mimecast provides numerous ways to help simplify GDPR compliance for email.

Security

Mimecast's email gateway and Targeted Threat Protection suite offer a comprehensive front-line of defense against advanced email attacks like ransomware, impersonation and phishing that use weaponized attachments, malicious URLs and social engineering to steal data and credentials. Robust encryption and data leak prevention (DLP) also help ensure personal data doesn't get into the wrong hands. Detailed logs and forensics, accessed natively or via API within SIEM systems, can be used to help investigate a threat or breach to aid in breach notification.

Archiving

The Mimecast Cloud Archive delivers complete and secure preservation of email data with SLA-backed rapid search. Fine-grained search, e-discovery, smart tagging and review tools make it possible to process subject access requests, right to be forgotten and erasure requests fast. Data export and secure delivery help with data portability requirements.

ALL RIGHTS RESERVED | 360-002

mimecast®

SOLUTION BRIEF

Granular retention policies can be applied at domain, group and individual level, making it easy to set distinct archiving policies for individuals and teams that work intensively with customer information or other forms of personal data. Role-based access controls ensure admins, legal, compliance and other teams see only the data they need. Full user and admin audit logs help audit compliance with policy, as well as to monitor all internal access.

Email Continuity

With all the right protection and controls in place, what happens if primary email systems fail or can't be accessed? With no company email, employees could use personal email, which likely doesn't meet compliance requirements. Such personal email usage by employees could be a significant risk. Mimecast Mailbox Continuity is engineered to ensure always-on email and archive access even when on-premises or cloud email systems like Microsoft Office 365 are down. Security and archive policies are maintained and protected, helping to ensure consistent GDPR compliance even in a disaster situation.

An Integrated Platform

All Mimecast services are delivered through a 100% cloud platform. All security, archiving, recovery and continuity services are fully integrated, making setup, ongoing management and consistent policy setting and enforcement simpler and faster.

Conclusion

It is clear that GDPR will raise the stakes – as well as the risks – associated with the collection, transport, and storage of personal data in the EU and internationally. Organizations that control personal data need to take appropriate steps to bring their policies and practices in line with this new, stringent regulation.

Because the regulation's architects deliberately set potential penalties high to motivate compliance, a strategy simply to proceed with business-as-usual and pay fines in the event of exposure invites serious business impact. Improper processing of personal data in emails can make any organization vulnerable to significant reputation damage and potential financial loss.

Mimecast is committed to GDPR compliance across all services by the enforcement date in May, and is providing contractual assurances to customers. Our portfolio of robust, cloud-based, cyber resilience services for email can be a vital component of GDPR compliance strategies.

Watch the video: Making Email Safer for Business

Learn how Mimecast can help ensure that you realize the full value of your email, safely and securely.

mimecast.com/how-we-do-it

Mimecast (NASDAQ: MIME) makes business email and data safer for thousands of customers with millions of employees worldwide. Founded in 2003, the company's next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management.