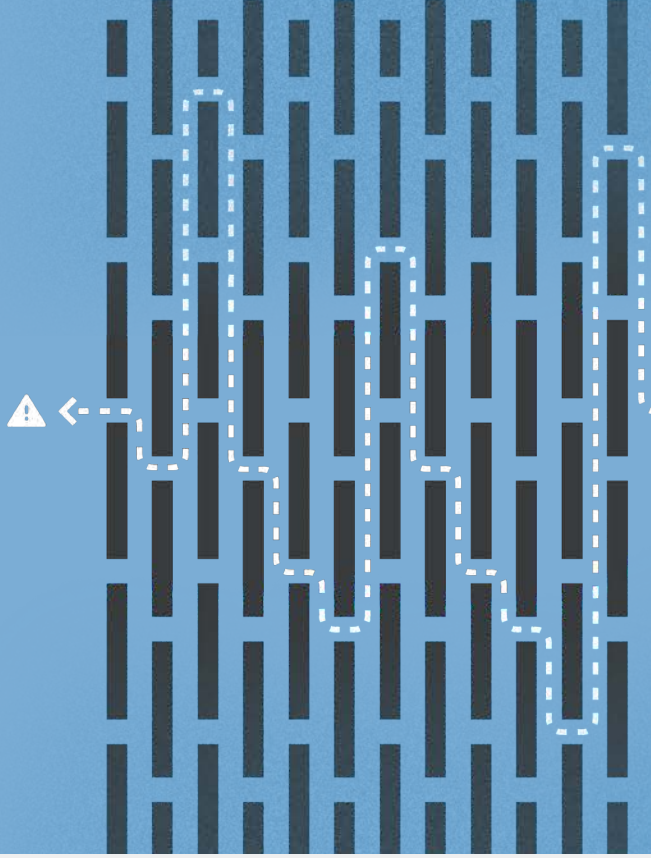
The European Union's General Data Protection Regulation (GDPR) was adopted in April 2016 and became enforceable from May 2018.

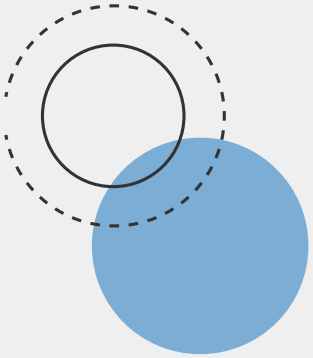


GDPR replaced the 1995 Data Protection Directive. It was designed to standardize data privacy laws across Europe, to protect EU citizens' personal data, and to reshape how organizations approach data privacy. Its key pillars include stronger rights for individuals, more stringent obligations on data processors and controllers, and heavier penalties for non-compliance. Businesses were compelled to revisit their data-handling practices, leading to global changes in data protection standards. While many praised its intent to empower users, some criticized it for the increased regulatory burden and ambiguity in certain provisions. Nonetheless, GDPR has set a global precedent for data protection legislation.

The GDPR emphasizes the importance of safeguarding personal data. For security teams, this means ensuring that personal data stored in emails or documents is securely stored, encrypted, and accessible only to authorized personnel. Breaches involving such data may lead to hefty fines. The regulation necessitates:

1. Clear policies
2. Regular risk assessments
3. Prompt breach notifications

GDPR Components Relevant to Email & Cloud Environments



In essence, GDPR has made data security a paramount concern for organizations, particularly for those handling large volumes of personal data in emails or stored documents.

Mandate	Citation	Description	Implication	Material's Solution
Data Protection Principles	Article 5	Personal data must be processed lawfully, fairly, and transparently.	Organizations must handle email data transparently and legally.	Identify PII in workspaces and monitor the transmission of emails containing PII.
Security of Processing	Article 32	Implement appropriate technical and organizational measures.	Emails storing sensitive data must be encrypted and securely stored.	Identify, label and implement access controls for PII at the message-level.
Data Breach Notification	Article 33 Article 34	Notify authorities and affected individuals of breaches within 72 hours.	Prompt action required on email data breaches.	Reduce PII exposed in a breach and know exactly what was accessed. If an attacker does gain access to PII, organizations will know precisely the scope of the impact.
Right to Erasure ('Right to be Forgotten')	Article 17	Individuals can request the deletion of their data.	Emails containing personal data may need to be deleted upon request.	Quickly and easily find all messages containing an individual's PII across all accounts.