proofpoint

COMPLY WITH THE EU GDPR WITH PROOFPOINT

KEY BENEFITS

- Understand where and how data is being used.

- Protect personal data at risk of exposure by setting automatic data retention and deletion periods.

- Identify and resolve compliance gaps in real time.

- Prevent unauthorised access to personal data and the applications that process them.

- Block impostor emails, credential phishing, and malicious payloads aiming to steal personal data.

The General Data Protection Regulation (GDPR) is data privacy legislation that aims to regulate the collection, processing, storage, deletion, transfer, and use of personal data of European Union (EU) residents—it goes into effect on May 25, 2018. If you have end users, customers and employees in the EU—even if you're based somewhere else—you need a GDPR solution that helps you discover, protect and monitor personal data. Any company handling EU personal data will have to comply with the new rules.

The regulation mandates that controllers of personal data "implement appropriate technical and organisational measures…in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

To comply with GDPR, organisations need multiple security technologies and controls working in strategic harmony against policy violations, compliance risks, and advanced threats. Proofpoint's unified cybersecurity platform protects personal and sensitive data anywhere, on any device, across any channel. We can help you identify and classify personal data, protect EU personal data, and respond and report on potential incidents.

The key Proofpoint solutions that help you comply with the GDPR are:
- Information Protection
- Email Protection
- Advanced Threat Protection

IDENTIFY AND CLASSIFY PERSONAL DATA

You can't protect what you can't see. Fundamentally, the GDPR is about giving data control back to the individual. EU residents will gain the "right to access" their personal data and the "right to be forgotten," or request that their data be deleted from all data stores.

Few organisations have the visibility they need to identify, retrieve and delete personal data in email, file shares, data stores, SharePoint sites and cloud applications. To be prepared for individual discovery requests and regulatory audits, your organisation must identify where personal data is stored and be able to collect, search and retrieve that data quickly.

Proofpoint Information Protection helps you manage this data governance process. You can:
- Automate the identification of personal data across various channels
- Remediate compliance breaches in real time
- Quarantine, delete, or revoke access to data at risk of exposure

PROTECT PERSONAL DATA

A breach of the personal data of EU residents can lead to fines of up to 2% of global revenue. In addition to giving EU individuals more control of their data, organisations must do everything they can to protect personal data and prevent the theft or loss of that data. And by protecting the individual, you inevitably protect your business from targeted attacks.

Fight data theft

Over 70% of data breaches are caused by external criminal activity, and an estimated 91% of all cyber attacks occur through email; that's why securing this channel is critical. Proofpoint Email Protection and Targeted Attack Protection empower you to defend your email ecosystem against inbound imposter emails and credential phishing attacks by:

- Assessing the reputation of each sender via email attributes, including sender/recipient relationship, headers and content
- Detecting, analysing and blocking malicious attachments and URLs before they reach the inbox
- Responding to and mitigating the impact of the threats that do make it into the inbox

Prevent accidental data loss

Email is the top threat vector for attacks against your organisation. It's also a critical risk vector for outbound data loss. Preventing confidential information from being leaked in outbound email messages must be a top priority to lower the risk of a data breach. With Proofpoint Email Data Loss Prevention, you can:

- Gain complete visibility and control over all email leaving your enterprise
- Set over 80 fine-tuned policies—based on geography, data type, purpose and security controls—that automatically find, classify and block messages that contain EU data subject personal data
- Encrypt identified personal data and monitor it as it's shared through email

Train your users

Technical controls alone are not enough. Articles 39 and 47 of the regulation state that organisations must raise awareness and train staff involved in data processing operations. It's not enough to create privacy policies. Your end users need to understand that they are accountable for meeting data protection requirements. This can only happen by investing in privacy awareness training for employees who handle the personal data of EU residents. With Proofpoint's GDPR security awareness training module, you can:

- Improve your employees' data handling skills and awareness of the new legislation
- Provide users with immediate feedback to drive lasting behavioral change
- Ensure that your users are protecting personal and corporate data effectively

RESPECT THE PRIVACY OF YOUR EMPLOYEES

Article 88 of the GDPR states that you must "safeguard the [Employee's] rights…with regard to…monitoring systems at the work place." Article 29 Working Party recommends that businesses "should consider certain types of traffic whose interception endangers the proper balance between their legitimate interests and employee's privacy—such as the use of private webmail."

Employers have a legitimate need to monitor employee business activity to protect from cyber threats. Eliminating personal webmail as a source for cyber threats enables companies to reduce their potential exposure. With Proofpoint Targeted Attack Protection for Personal Email Defense, you can:

- Keep personal webmail personal with a web-isolation service
- Monitor and inspect web traffic without the risk of inadvertently collecting personal data
- Ensure employee privacy is protected with violating compliance standards

RESPOND AND REPORT

Security breaches have become the new normal. That's because threats change and attackers evolve. No defence can stop every incident. That's why GDPR compliance is an ongoing effort.

Article 33 of the GDPR mandates that your business, once aware of a breach of EU personal data, must describe the nature of that breach, the consequences of the breach, and the measures taken to address the breach. All this in 72 hours!

Cybersecurity is more than any moment in time—your cybersecurity strategy must be sustainable to be able to identify and report on incidents and breaches. With Proofpoint Threat Response and Emerging Threat Intelligence you can contain threats quickly and understand the scope of incidents for fast, accurate disclosure as required under GDPR.

Powered by the cloud, Proofpoint's solutions can be deployed right away and adapt as threats evolve. Maintain trust, ensure compliance and safeguard the security of EU personal data with our advanced cybersecurity solutions.

Take the Guesswork out of GDPR
FIND OUT WITH A FREE ASSESSMENT
proofpoint.com/us/contact

COMPLY WITH THE EU GDPR WITH PROOFPOINT

ENHANCE

DISCOVER

Document and Report
Leverage technology to provide structured, consistent, and automated reporting.

PROTECT

DISCOVER
Identify the current state of EU personal data
- Data Discover
- Cloud App Security Broker

PROTECT
Protect all identified EU personal data
- TAP for Personal Email
- GDPR Security Awareness and Training
- Target Attack Protection (TAP)
- Email Protection
- Email Encryption
- Email DLP

ENHANCE
Monitor effectiveness, respond to incidents, and report on data breaches
- Emerging Threat Intelligence
- Threat Response