proofpoint.

www.proofpoint.com

Proofpoint Security Awareness Training and GDPR

How Proofpoint Security Awareness Training can assist customers to comply with GDPR

Version February 14, 2019

Introduction

On 25 May 2018, the most extensive and far-reaching piece of European data protection legislation came into force—the European Union's (EU's) General Data Protection Regulation (GDPR) – replacing the 1995 European Union Data Protection Directive.

At its core, the GDPR aims to put EU residents in control of their personal and sensitive data. It regulates how their data is collected, processed, stored, deleted, transferred, and used. Any company that does business in the EU or handles the personal data of EU residents is obligated to comply with the regulation.

This applies to all companies processing personal data of EU residents—even companies that do not have physical operations in the EU. For any company collecting personal data on people located in the EU or for any company doing business in the EU, GDPR compliance is mandatory. Regardless of where data is processed, the GDPR requires that personal information be protected.

Learn more about the GDPR.

Developing a plan to comply with the new rules is critical for all organizations, including Proofpoint. Proofpoint is committed to compliance with the GDPR across our solutions and services. As a data processor, we maintain the privacy and confidentiality of the personal data entrusted to us.

Any company that does business in Europe or handles the personal data of EU residents must comply with the seven GDPR principles:

Principle 1: Lawfulness, Fairness, and Transparency

- Individual consent
- Right to Access
- Right to be Forgotten
- Right to Deletion

Principles 2 and 3: Accuracy and Purpose Limitation

- Data integrity
- Data must be accurate and up to date
- Right to correct
- Data process limitation

Principles 4 and 5: Data Minimisation and Storage Limitation

- Collect only necessary data
- Store data no longer than required

Principle 6: Integrity and Confidentiality

- 'Privacy by Design and by Default'
- Appropriate technical and organizational controls

Principle 7: Accountability

- Data Protection Officer

- Data breach notification
- Privacy impact assessment

This guide explains how Proofpoint can help you comply with GDPR, especially principles 1–6.

Proofpoint's Security Awareness Training provides SaaS-based information security awareness and training software to help organizations teach their employees secure behavior. PSAT solutions include an integrated platform with knowledge assessments, a library of simulated attacks, and interactive training modules, which have been proven to reduce successful phishing attacks and malware infections by up to 90%.

GDPR Regulation	Proofpoint
Principle 1: Lawfulness, Fairness, and Transparency	
Right to Access How does PSAT enable searches on information on a per-individual basis?	Through PSAT User Management, the customer's Admin can search on first name, last name and email address.
Right to be Forgotten How does PSAT help manage data retention and disposition?	The Admin has the capability to go into the User Management Application and select the "Destroy User Record". Deletion is not reversible.
Right to deletion Can PSAT permanently delete information?	PSAT removes a user, which deletes and obfuscates all user information, at the database level. If the user is re-added, they are treated as a brand-new user, and any previous actions or history previously associated to that user would not be associated to the newly added user. This applies to users being added via the online modal, CSV, or from End User Sync.
Principles 2 and 3: Accuracy and Purpose Limitation	
Data Integrity How does PSAT ensure that the data is not altered or corrupted?	The customer's Admin can edit, update and delete all user data.
Collect only necessary data What types of data are stored in the archive?	PSAT requires only an email address. First and Last names are optional.
Data portability How does PSAT ensure I can get my data?	PSAT enables via the User Report card to all export all user data via CSV file.
Automated profiling Does PSAT use data to automatically profile individuals?	No.
Transfer of data Is data being transferred to other locations?	Yes. A limited amount of personal data associated with threats that are identified by PhishAlarm and PhishAlarm Analyzer users as

	suspicious are transferred to Proofpoint's threat analysis systems, which are hosted by data centers located in the USA and Europe.
Principle 6: Integrity and Confidentiality	
Privacy by Design and by Default How does PSAT ensure that confidential data stays private?	Our Security Education Platform uses the following Personal Data ("Personal Data") residing in our production environment: Customer email addresses Customer first and last name (optional) Other information supplied by customer (optional) PSAT minimizes the use, collection, and retention of Personal Data to what is strictly necessary to accomplish our business purpose and mission. Customer email addresses are collected to administer training assignments and to conduct assessments within the customer's employee base. The email addresses are uploaded by the customer acting as administrator of the training and assessments. For our Managed Services offerings, customers provide the data to PSAT via encrypted emails with PSAT certificates. Alternatively and upon request, PSAT creates a sftp server for customers to upload files. PSAT limits access to Personal Data to customers with administrative roles in managing their training and assessments activities. These administrators have independent access to their employee's email addresses.
Data protection What steps has Proofpoint taken to protect the data?	PSAT uses state of the art controls to protect customer's data such as encryption, pseudonymization and capabilities to maintain the confidentiality, integrity, availability and resilience of processing systems and services. Specifically, an Administrator may anonymize users' email addresses, first names, and last names in the CyberStrength, Interactive Training Modules, and ThreatSim Anti-Phishing Simulation Tool reports. This option allows organizations to train and phish a group of users in order to gauge the group's susceptibility without identifying an individual's actions within the initiative. Reports within the Security Education Platform can be anonymized to ensure that no user Personal Data is available. Our Dynamic Reports support a Data Privacy feature, which obfuscates

	all Personal Data contained in Dynamic ThreatSim, PhishAlarm, and Training Module reports for individual administrator accounts. This feature is available to all PSAT customers, but may be particularly important to European customers or those who have data privacy concerns. Classic Reports can also be disabled, which will hide any report that contains Personal Data from our Training, ThreatSim, or CyberStrength reports, and User Report Cards and User Report Export. When both of these options are combined, all reporting performed by an administrator that required Personal Data to be masked will obfuscate the Personal Data in the reports. Customer Technical Support can assist you with these features.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats. www.proofpoint.com

Version February 14, 2019