GDPR for non-Europeans

Guidebook

Genetec™

Contents

Introduction

The concerns around cybersecurity and personal privacy are growing in response to an ever-increasing number of high profile stories in the media. Individuals, organizations, and governments are developing new ways to protect data at every level. This spring, a set of regulations from the European Union will become enforceable. Its potential impact will be far-reaching, and non-compliance will be costly.

We know that keeping up as governments introduce regulations, particularly in the face of advancing technology, can be a daunting task. That's why we've put together important information that can help you keep your systems and data secure all while protecting everyone's right to privacy.

The Genetec Team

What is the GDPR?

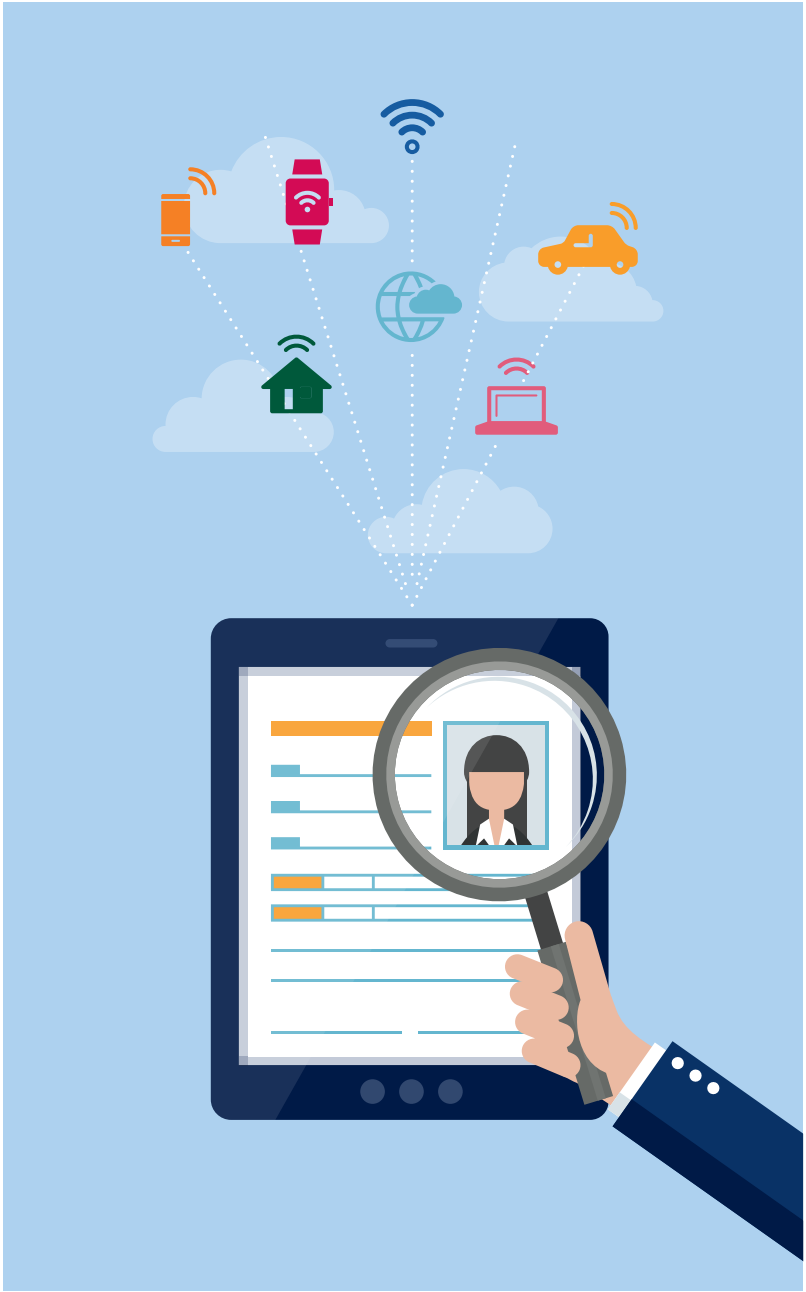
The European Union's General Data Protection Regulation, or GDPR, is a set of rules for collecting, processing, storing, and transmitting the personally identifiable information (PII) of EU residents.

Its main goal is to unify and strengthen the protection of EU citizens' personal data. The regulation also gives individuals new rights to access and erase PII and imposes new requirements for organizations in response to a data breach.

What is personally identifiable information?

Personally identifiable information, or PII, is defined as any information that can be used to identify a specific individual, either directly or indirectly. This includes a person's name or aliases, home and email addresses, data collected by IoT devices, financial information, and image.

A lot of the data collected by physical security systems can be considered PII, including video, cardholder activity and information, and license plate numbers.



What does the GDPR cover?

Under the GDPR, individuals have a host of new rights, including the right to be forgotten, which means their personal data will be removed from an organization's system. They have the right to request that their PII not be processed for direct marketing.

To increase transparency, the regulation includes mandatory breach reporting rules that require organizations report a breach within 72 hours of detection. In addition, the GDPR sets out new record-keeping requirements for managing, modifying, storing, and analyzing PII.

Why does it matter?

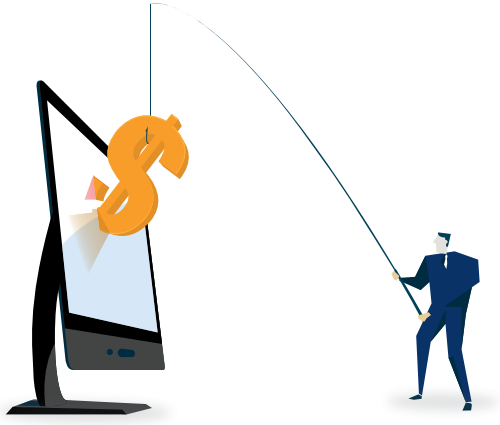
The GDPR affects any organization collecting or holding personal data from EU citizens. This means that, in addition to EU-based companies, multinational organizations that conduct business in the EU or have EU residents visiting their websites also have to comply.

Even if an organization is not using the data collected for tracking purposes, it must still follow the new set of rules to properly protect data and abide by the new rights for individuals. Basically, if an organization has a web presence in the EU, it has to do its homework.

Why could this affect you?

The GDPR was developed, in part, to help protect against and mitigate the risks associated with cyberattacks. But, regardless of size or location, any organization in the world can be vulnerable to criminal cyber activity that results in a data breach. With our increasingly integrated global economy, a breach in one region can have a serious impact on an organization in another.

A data breach has the potential to expose your valuable or sensitive information, which can negatively affect your reputation and damage brand recognition. More than that, a data breach can be costly as you work to close and recover from it. These costs rise as your team works to ensure that your entire system is clean.



What are the potential fines for non-compliance?

Under the GDPR, penalties for non-compliance are steep. Fines can be up to €20 million or 4% of global annual turnover – whichever is higher. And, of course, in the case of a data breach, these fines are over and above what an organization incurs during containment and recovery.

It's estimated that the average cost of a data breach is $3.6M. In all cases, the financial impact of a data breach increases with time, so rapid detection and containment are key to minimizing both data and monetary losses.

When the mean time to containment is less than 30 days, the estimated average total cost of a data breach is $2.83M. The average cost to companies that take more than 30 days is $3.77M.

What can Genetec do to help?

Genetec solutions help protect PII by design. We offer a wide range of on-premises and cloud-based options that give you better control over the data you collect and help you answer personal information access requests.

Our solutions help protect your data by encrypting and anonymizing the PII captured, stored, or transmitted by your system. Built-in authentication tools help keep data from getting into the wrong hands, and our group-based authorization management tools allow you to control user activity.

To learn how Genetec solutions can help you comply with stringent regulations, including the EU's GDPR, visit our Trust Center at www.genetec.com/trust.


123 ABC

We build secure solutions that help you protect the everyday without compromising privacy.

genetec.com/trust