Trend Micro

DATA PROTECTION AND THE GDPR:

Using State-of-the-art Cybersecurity to Achieve Compliance

WHAT IS IT?

On May 25, 2018, the European Union's (EU) General Data Protection Regulation (GDPR) will take effect. This regulation standardizes data protection legislation across the EU and updates data protection laws to cover previously unforeseen data usage patterns. The GDPR mandates that organizations anywhere in the world processing EU citizen data, including large enterprises, small and medium businesses (SMBs), governments, and even sole proprietors, reassess their data processing controls and put a plan in place to better protect EU citizen data.

WHAT ARE THE IMPLICATIONS?

With 1,935 confirmed data breaches in 2016[1] and many more in 2017 from well-known companies around the world, it is clear that data protection is an issue that needs to be addressed. Viewed as one of the most aggressive data protection regulations in the world, the GDPR is designed to consistently protect personal data for EU citizens, meaning that any organization interacting with an EU citizen and storing their data will be subject to fines for non-compliance—even organizations based in countries outside the EU, such as the U.S. or Australia.

While some organizations are looking at the GDPR as an opportunity to increase the association of their brand with protection of user data, and for overall business growth, there are also potential negative impacts from non-compliance. The maximum size of the potential fines is significant: 4% of global revenue or €20M, whichever is larger. Importantly, fines are not the only potential impact of non-compliance: the GDPR gives Supervisory Authorities the power "to impose a temporary or definitive limitation including a ban on processing," which means they could actually prohibit an organization from doing business.

In the event of a privacy event (e.g., breach), supervisory authorities must be notified within 72 hours, and must deliver critical information, including the details on the number of EU citizens impacted and how the incident happened.

With significant potential negative impacts in mind, it's important to prepare your organization to effectively protect personal data and achieve compliance with the GDPR.

> "Too often, when S&R professionals face a daunting challenge, **they search for a single technology to solve it.** In the case of data security, such a technology does not exist. Instead, **you need a framework** that outlines how you discover, classify, analyze, and ultimately defend data with a mix of security processes, technical controls, and a willingness to instill a culture that respects and appreciates privacy."
>
> Forrester, "Protect Your Intellectual Property and Customer Data from Theft and Abuse", Stephanie Balaouras, July 12, 2017

Trend Micro solutions are powered by XGen™, a smart, optimized, and connected security approach.

WE CAN HELP WITH GDPR COMPLIANCE

Trend Micro provides state-of-the-art security solutions that:

- Protect personal data
- Protect employees
- Protect IT infrastructures
- Protect cloud data
- Detect, respond, and report on breaches

WHAT CAN YOU DO?

The GDPR is a multi-faceted regulation that includes people, process, and technology guidelines, all focused on data protection. State-of-the-art security can play a pivotal role in compliance, helping to ensure that technology married to people and process is effective.

As threats to data continually evolve and as recommended by leading analyst firms, it is important to take a multi-layered strategy to data protection that will both protect your organization and also fit with the way you run your business. Ultimately, you need to be able to protect your organization from threats, detect when malicious activities are happening, and respond to incidents rapidly and efficiently.

[1] 2017 Verizon Data Breach Investigations Report

TREND MICRO CAN HELP

As a multi-faceted regulation with global ramifications, the GDPR will impact many aspects of an organization's technology and security strategy. Trend Micro can help address many of the state-of-the-art technology requirements highlighted in the regulation with XGen™ security, a smart, optimized, and connected approach to layered security that applies across the enterprise.

SMART

A smart defense leverages a cross-generational blend of threat defense techniques to protect personal data against known and unknown threats at any stage of processing. While new security techniques can address new threats, current techniques are still useful for data protection. State-of-the-art security requires a cross-generational blend of techniques to enable the most appropriate and efficient approach for addressing each threat–there is no such thing as a security silver bullet. XGen™ security protects against the full range of known and unknown threats using a cross-generational blend of threat defense techniques that applies the right technique at the right time.

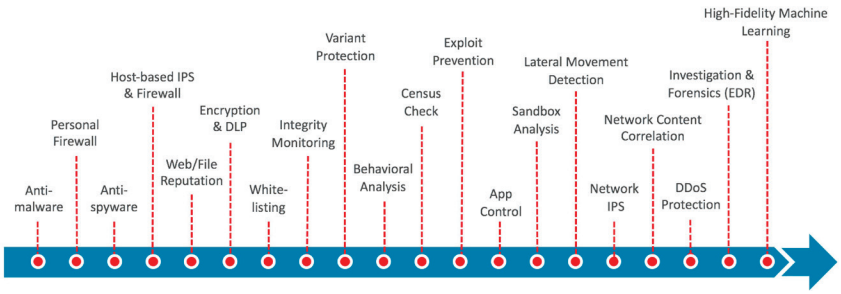

Figure 1: Leverage a cross-generational blend of threat defense techniques for state-of-the-art security

OPTIMIZED

Optimization of security techniques for your environment is critical to the success of a deployment. Security techniques must secure both legacy and new enterprise environments, including public cloud and containers. Integration with leading environments helps to enable visibility across users, servers, and networks, giving you the ability to analyze and assess the impact of threats, and, in the face of a 72-hour breach reporting requirement, quickly report on incidents across the enterprise. XGen™ security delivers security solutions designed for and tightly integrated with leading platforms and applications, like VMware, Amazon Web Services (AWS), Microsoft® Azure™, Google Cloud, Office365, and more.

CONNECTED

A connected defense helps to both prevent and remediate personal data breaches by sharing real-time threat intelligence and automated security updates across all security layers. This helps to stop threats–like ransomware– before they can impact personal data. Trend Micro Connected Threat Defense, powered by XGen™ security, protects, detects, and responds to sophisticated attacks and provides a 360-degree view of your organization's networks, endpoints, and hybrid cloud environments.

To help you on your journey to GDPR compliance and beyond, Trend Micro delivers state-of-the-art security through our XGen™ security strategy, enabling organizations to leverage cybersecurity solutions that address threats today and tomorrow, while fitting in with the needs of your business.

To learn more, visit trendmicro.com/gdpr

GDPR QUICK SUMMARY

- Fines for non-compliance of up to 4% of global annual revenue or €20m (whichever is higher)
- Ability to force an organization to stop processing information, which could force business stoppages
- Applies to any organization processing or storing EU citizens' data–even if based outside the EU (e.g., United States, Australia, etc.)
- Applies to data processors and data controllers
- Firms must ask their customers for explicit consent for the use of any personal data. This will also apply to data that was collected historically, therefore requiring new opt-in requests to be delivered
- A Data Protection Officer (DPO) must be appointed to deal with GDPR compliance
- Mandatory breach notifications must be given within 72 hours to the local data authority
- Right to erasure (right to be forgotten) means consumers can request the deletion or removal of personal data when there is no compelling reason for its continued processing
- Right to data portability allows consumers to copy or transfer personal data with ease from one IT system to another safely and securely, without hindrance

TREND MICRO™