CYLANCE

BUSINESS BRIEF

PROTECTING DATA UNDER THE GDPR

GDPR Compliancee

Preparing for GDPR compliance with endpoint artificial intelligence (AI) based technology that prevents cyberattacks from ever executing, will protect EU members' personal data in the near-term, as well as when virus and malware strategies inevitably evolve.

WHAT IT IS

With cybercriminals threatening nations globally, cybersecurity is taking a front seat in many regions, most notably the European Union (EU), which has adopted regulations to combat the threats. Against the backdrop of increasingly sophisticated cyberattacks, the EU has set forth rules and procedures for enhanced cybersecurity, along with penalties for noncompliance, in the form of the General Data Protection Regulation (GDPR). This new body of mandated policies and procedures aims to protect EU member personal information collected and/or stored by organisations, with regulation for the following stipulated:

- Data privacy by design and default
- Data Protection Officers (DPO)
- Data breach reporting and security
- International data transfers
- Investigative, corrective, and advisory powers of supervisory authorities
- Right to compensation and liability

WHO IS AFFECTED

The GDPR applies to any organisation that stores personal data from residents of any EU member state. Thus, having a presence in Europe, or engaging in the collection of data from European based customers is sufficient for institutions to fall under the GDPR umbrella. Even UK organisations operating in a post-Brexit world will be expected to comply with the GDPR.

Once enforced, the GDPR could result in severe financial penalties for non-compliance. Not only can the EU impose penalties, but residents of EU member states are authorised to pursue litigation of their own for damages suffered due to a breach of the GDPR.

About Cylance

Cylance is the first company to apply artificial intelligence, algorithmic science and machine learning to cybersecurity and improve the way companies, governments, and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist.

By coupling sophisticated machine learning and artificial intelligence with a unique understanding of an attacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats.

WHY THIS MATTERS

Complying with the GDPR means organisations face several fixed costs (e.g., empowering the DPO, conducting audits, preparing for data access requests) and variable costs associated with a breach (e.g., notification, investigation, actual monetary theft, penalties, loss of reputation/business). Fortunately, the following quick wins can greatly reduce variable costs, mostly by preventing any attacks from being successful in the first place:

- **Upgrade software** — While the overall impact of the recent global WannaCry attack was far less than it could have been, hundreds of thousands of affected endpoints could have been protected with updated software. According to the BBC, "A security update — or patch — was released by Microsoft in March to protect against the virus, but it appears many organisations have not applied the patch — or may still be using outdated systems like Windows XP."[1] As a side note, this breach, though minimal in financial damage, under the GDPR, could have resulted in fines of €20 million for each company or organisation affected.
- **Protect vulnerable endpoints with real-time antivirus (AV), anti-malware, and anti-spyware software** — As evidenced by many successful phishing schemes, employees often are still tricked into opening malicious attachments or links in emails that can begin an infection. AI based endpoint products that evolve as threats evolve provide constant, up-to-date endpoint protection, preventing an attack from ever executing, and ensuring long-term GDPR compliance and lower costs.

RECOMMENDED ACTIONS

Organisations set up firewalls, install AV programs, apply file filters, run intrusion detection, and regularly update software to keep cybercriminals out, but no protection is 100% effective. The human interaction element at most endpoints renders them the weakest link in any security chain. With this in mind, endpoints are best secured with AI based advanced endpoint protection.

Using machine learning to predict, prevent, and stop malware and cyberattacks, Cylance AI based solutions can stop attacks before they execute. Read about Cylance blocking WannaCry since 2015 and more:

- Why Cylance Blocked the WannaCry Ransomware Attack
- Read a Cylance Customer Case Study
- Want to know if you've been breached? Get a Compromise Prevention Assessment to determine if a security breach has happened or is actively occurring in your environment.

Certified for engagement across Europe, Cylance is a valued partner for protecting personal data of EU member states and ensuring compliance with the GDPR.

[1] "NHS cyber-attack: Amber Rudd says lessons must be learnt," May 13, 2017, BBC News

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

CYLANCE