SOLUTION GUIDE

GDPR & DATA SECURITY

EUROTEKUK
MANAGED IT SOLUTIONS

The clock is officially ticking for organisations to get their data protection policies in order, now that the final draft and approved text have been made available for the General Data Protection Regulation to replace the existing EU Data Protection Directive. The new regulation will come into effect in 2017 and will require businesses to put a much stricter focus on data protection.

The headline items for organisations that collect or process EU citizen records are:

- They must notify their supervisory authority of a data breach within 72 hours
- The subject will have the right to retract consent, request data erasure or portability
- They may face fines of up to 4% of their worldwide turnover, or €20 million for intentional or negligent violations.

These increased sanctions mean it is vital that the final legislative text be fully understood by a number of key stakeholders within the business, and that businesses start planning ahead as soon as possible. Underpinning all of this is the fact, no matter how big a company is, that businesses have to begin thinking about their security in terms of when they will face an attempted data breach, rather than if. Only when businesses accept this will they be able to plan and execute successful security defences and policies.

To help them with that here are five key steps to help organisations perform a basic assessment of their current data protection strategy and any potential gaps that need filling.

Identity

The first task is to identify whether they are considered a data controller or processor. They must then review the obligations these carry (such as issuing notices and obtaining consent) and regularly review existing and new processes around PII. They can then discover where this data resides –at-rest, in-motion and/or in-use – have a record of processing activities and understand how this data is protected.

Protect

Once PII has been identified it must then be protected. Encryption and access control are common control standards, but managing encrypted data across multiple business processes is a hugely difficult task. Data sovereignty and lifecycle are key, alongside data flows to third parties, monitoring for data leakage from negligent or malicious employees and external data theft.

Detect

If an organisation suffers data loss then it is vital to detect the breach and identify if PII records were lost or stolen. If so, the business must notify the authorities within 72 hours of the discovery to initiate a full investigation. The investigation will focus on identifying the source and destination of the breach through information from Data Leakage Prevention (DLP) and Data Theft Prevention (DTP) tools. Data forensics will help to pinpoint the stolen data, so the business can issue notice to any affected data subjects.

Response

Incident response is critical to protecting citizen data. In addition to the mandatory data breach notification requirement, organisations must also ensure they have implemented and tested an incident response plan.

Recovery

In the aftermath of a data breach, businesses must ensure they maintain ongoing communication with the relevant authorities. This ensures loss factors are managed and keep affected data subjects regularly informed.

SOLUTION GUIDE

GDPR & DATA SECURITY

EUROTEKUK
MANAGED IT SOLUTIONS

Vendor	Products	How they help meet GDPR requirements
TREND MICRO	**Integrated Data Loss Prevention** All Trend Micro solutions	Integrated DLP from Trend Micro helps identify regulated content being moved around or out of the organization, wherever it is a USB, email, SaaS applications, web, mobile devices, and cloud storage. It plugs into every Trend Micro solution, all managed through a single console.
	Intrusion Prevention Vulnerability Protection, Deep Security and Threat Protection	Deep Security is a unified solution that secures virtual, cloud, physical, and hybrid environments, providing a single platform that includes integration with VMware, Amazon AWS and Microsoft Azure. Vulnerability Protection helps prevent the exploitation of known exploits and vulnerabilities, and secures critical business applications.
	Breach Detection Deep Discovery	Trend Micro Deep Discovery enables the detection, analysis and response to ransomware and targeted attacks in real time. This is essential in reducing the time to a breach discovery, and subsequent response.
	Email Security Cloud Email Security	Trend Micro Cloud Email delivers continuously updated protection to stop spam, malware, spear phishing, ransomware, and advanced targeted attacks before they reach the network, and includes Social Engineering Attack Protection to prevent data loss from spear phishing.
	Encryption Smart Protection	Smart Protection with XGen includes Endpoint Encryption, with automated enforcement of policy-based encryption of file/folders, media and port/device control that's an essential requirement of GDPR.
HEAT software	**Device Control** Provides granular visibility, control and encryption of removable devices and hard drives.	Data in transit should be encrypted, and Device Control enables the encryption and management of removable media (USB storage, optical media, memory cards). This includes encrypting data, black/whitelisting specific drives and blocking any data transfer or removal.
	Application Control Identify all applications in an environment and enforce a comprehensive whitelist policy that stops unauthorized applications.	Once sensitive data is identified, it's essential to prevent it being stolen or accessed without authorisation. Application Control prevents any non-approved application or program running (such as ransomware or malware), helping prevent unknown data breaches.

SOLUTION GUIDE

GDPR & DATA SECURITY

EUROTEKUK
MANAGED IT SOLUTIONS

Vendor	Products	How they help meet GDPR requirements
GUIDANCE SOFTWARE	**EnForce Risk Manager** A data risk management solution that proactively drives a 4-stage process to identify, categorize, remediate, and report on sensitive data.	EnForce Risk Manager provides remediation and secure data collection capabilities relating to Article 5-7, 9 that individuals have the "right to erasure or to be forgotten" and allows organisations to put a practical Data Retention Policy in place to control and even pseudonymize relevant data in compliance with (Art 6 (4) (e)) of the GDPR.
	EnCase Endpoint Security An endpoint detection and response solution that provides anomaly-based detection, automates and accelerates incident response process, and remediates traces of any threat.	GDPR's article 35 requires organisations conduct Data Protection Impact Assessments when the rights and freedoms of data subjects are at risk. EnCase Endpoint Security provides visibility into laptops, desktops, and servers to validate security alerts, detect machine anomalies, scan for IoCs in a highly scaled manner and triage security incidents.
	EnCase eDiscovery Allows IT and litigation support teams to conduct early case assessment, collection and preservation from all computer platforms that is legally defensible and judicially accepted.	EnCase eDiscovery enables companies to transfer legally-necessary evidence and digital proof relating to data breaches to relevant third parties (such as data protection authorities) and legal counsels of victims. This tool is ideal for managing large volumes of data. (Art. 24, 82)
	EnCase Endpoint Investigator A forensic software solution designed to perform remote, discreet, secure, internal investigations.	EnCase EndPoint Investigator helps organizations comply with the GDPR time-reporting standards with easy access to remote evidence collection, preservation and preliminary breach analysis to define the extent of damages and reveal the legal consequences. (Art. 33).
netwrix	**Netwrix Auditor** A visibility and governance platform that enables control over changes, configurations and access in hybrid cloud IT environments. www.netwrix.com/GDPR_Compliance.html	Netwrix Auditor means an organisation can quickly spot who performed what activity, where and when across a hybrid cloud IT infrastructure. The actionable audit intelligence helps protect sensitive assets against insider threats or external attackers, prevent data breach, and maintain continuous GDPR compliance. Compliance with other regulations (such as PCI or ISO) is available as standard.

SOLUTION GUIDE

GDPR & DATA SECURITY

EUROTEKUK
MANAGED IT SOLUTIONS

Vendor	Products	How they help meet GDPR requirements
UCOPIA	**UCOPIA Guest Access Management** A physical or virtual on-premise solution enabling organisations to manage and collect guest & user data on all Wi-Fi connections.	UCOPIA integrates security into Wi-Fi Authentication and internal directory, and was designed to meet these GDPR standards and process. The product was conceived from the ground up to meet and exceed the standards set by the previous EU Directive 2006/24/EC ensuring data is retained, accurate and consent for collection has been granted by the user.
Trustwave Smart security on demand	(**SIEM**) Security Information and Event Management	SIEM Enterprise unifies the logs and reports from products across their network to detect threats, manage risk and compliance requirements and understand security incidents.
	(**MST**) Managed Security Testing	Trustwave MST reveals vulnerabilities and the consequences of exploitation. Security testing helps businesses identify their network-connected assets, learn how they are vulnerable to attack, and understand what could happen if those assets were compromised.
	(**MSS**) Managed Security Services	Trustwave MSS is a portfolio of integrated technologies with unparalleled threat intelligence, breach detection capabilities and the ability to map and protect the entire data footprint.
	Database Security	Trustwave's Database Security solutions help discover and assess the contents of data repositories, and then provide comprehensive and granular controls to measure and mitigate risks to the confidentiality, integrity and availability of all information.