

WHAT YOU NEED TO KNOW ABOUT THE EU GENERAL DATA PROTECTION REGULATION

WHAT IS THE GDPR?

It is a new regulation which aims to **strengthen** data protection rights for individuals within the European Union.

It replaces the 1995 directive and aims to **future-proof** data protection in the EU, whilst also unifying various national laws.

The GDPR will also apply to **non-EU** organisations which process data of EU residents.



When will these changes take place?

2016

Adoption of the new regulation. Businesses have **2 years** to comply

2018

Complete implementation and **strict enforcement** of the EU GDPR

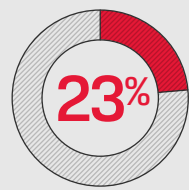
From **2018 onwards** companies should use state-of-the art security to protect personal data



In case of a data breach businesses will face fines of up to 4% of their annual global revenue or €20 million (whichever is greater) and must inform their national supervisory authority



Studies



The average cost of a data breach increased by 23% since 2013

€3.7m

The average cost of a data breach for large organisations in the EU

The highest costs occur in the

HEALTH, EDUCATION & FINANCIAL SECTORS

5 Steps to becoming GDPR compliant

1

Awareness



Understand the new regulation and what it means

2

Evaluation



Understand who uses and has access to data

3

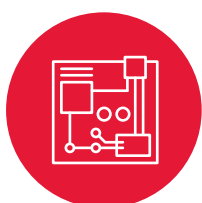
Policy



Define your strategy for data on the move

4

Technology



Consider **hardware encryption** and **endpoint-management** options

5

Education



Ensure your staff are aware of the GDPR, and best practice data protection policies

A SMALL USB CAN CAUSE A LOT OF TROUBLE

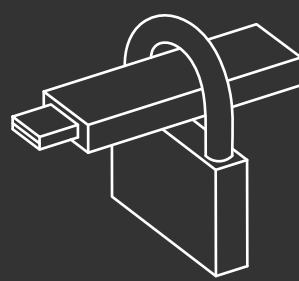
Employees carrying data out of the office increase the risk of data being **compromised**.

Leaving a company open to **hefty fines**, recovery costs and a potential PR disaster.

Remember, this can apply to data you not only **need** to protect, but **want** to protect.

Encryption is the best way to be safe.

Kingston encrypted products minimize the risks of moving data on USB drives and ensure your critical and sensitive data is protected.



Did you know?

If a USB is lost or stolen and the data on it is **encrypted** then this is a

SECURITY BREACH

not a data breach and may not have to be reported.

Kingston Encrypted USB Drives

Encrypted USB Drives	DataTraveler 2000	DataTraveler Vault Privacy	DataTraveler 4000 G2
Security	XTS	XTS	XTS
Certification	-	FIPS 197	FIPS 140-2 Level 3
Anti Virus	-	✓	-
Customisable	-	✓	✓

Also available as anti-virus version

This model features easy-to-deploy anti-virus protection from ESET that protects the drive's content from viruses, spyware, Trojans, worms, rootkits, adware and other Internet-borne threats. The ESET NOD32® anti-virus engine provides instant alerts. This anti-virus protection requires no installation and comes with a five-year pre-activated licence.

Customisable

Customise drives in a variety of ways, including dual password, serial numbering, co-logo, number of attempted password entries, minimum password length and customised product identifier, to meet internal corporate IT requirements.

www.kingston.com/encrypted



Get a small but **important** item ticked off the GDPR to-do list by investing in **256-bit AES hardware-based encryption**

Sources

Ponemon Institute: 2015 Cost of Data Breach Study Global Analysis
European Commission: Reform of EU data protection rules
(http://ec.europa.eu/justice/data-protection/reform/index_en.htm)



Kingston

TECHNOLOGY