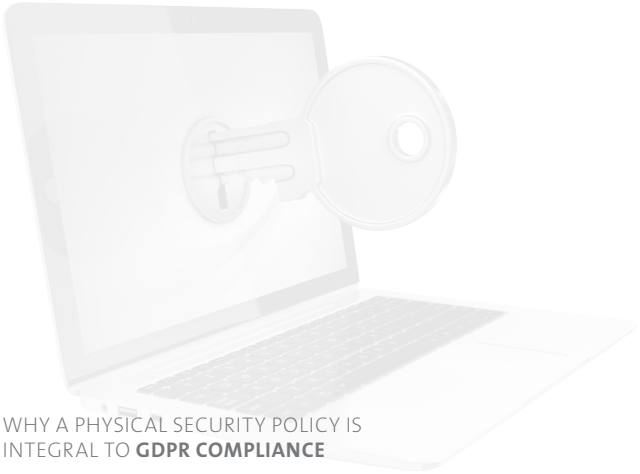
Kensington The Professionals' Choice™

Why a Physical Security Policy is Integral to **GDPR Compliance**

Disclaimer: *Nothing contained herein should be construed as legal advice. Organisations should consult legal counsel with regard to compliance with the General Data Protection Regulation or any other applicable laws or regulations.*

DATA PROTECTED

Contents



WHY A PHYSICAL SECURITY POLICY IS INTEGRAL TO **GDPR COMPLIANCE**

About **This Document**

*This white paper will give you **an overview of what the GDPR aims to achieve** and the problems it may present to organisations.*

WHY A PHYSICAL SECURITY POLICY IS INTEGRAL TO **GDPR COMPLIANCE**

The purpose of this paper is to give you an introduction to the EU's General Data Protection Regulation (GDPR) and how it will impact different businesses, so you can develop a framework for a hardware security policy for your own business, ahead of the regulations coming into effect in May 2018.

So what is the GDPR? It requires organisations to apply sound security practices to electronic and paper-based data and, in the case of a data breach, notify affected or potentially affected individuals. The GDPR's reach extends globally to all organisations that control or process personally identifiable data about people in the EU, regardless of the geographic footprint of those organisations. GDPR requirements apply to both electronic and paper-based personal data and means that all organisations should address GDPR requirements if they handle EU-originated personally identifiable data.

Securing data against hacking and malware is rightly top of mind for many organisations, however many fail to adequately address the physical security of IT hardware. More than half fail to use a physical lock for IT equipment[1]. This puts organisations at risk for non-compliance with GDPR and data subjects at risk from fraud and identity theft. With this in mind, Kensington encourages organisations to review their security policies and practices relating to electronic data.

An **Overview**

While the GDPR's main objective is to strengthen online privacy rights, physical hardware security has a significant role to play.

GDPR focuses on tackling the ever-increasing challenges towards data protection and privacy, exposure to security breaches, hacking and other unlawful processing.

*These points **identify the specific areas within the GDPR** that are new or strengthened rights for individuals.*

WHY A PHYSICAL SECURITY POLICY IS INTEGRAL TO **GDPR COMPLIANCE**

1

Data Portability and the Right to be Forgotten

- Individuals now have the right to transport their personal data from one organisation to the next.
- Personal data must be provided in a structured and machine-readable format.
- A person can request the deletion or removal of personal data.

2

Inventory

- Local authorities no longer have to be informed that personal data is being processed.
- Organisations must maintain a record of processing activities under its responsibility.

3

Data Protection Impact Assessments & Security

- DPIAs are a means to identify high risks to the privacy rights of individuals.
- Security requirements and recommendations should be based on a risk assessment.

4

Data Breach Notification

- Any breaches should be reported to the supervisory authority.
- Individuals affected by the breach should also be informed.

5

Data Governance and Accountability

- Organisations must also be able to demonstrate compliance with the GDPR.

Who Does It **Apply To?**

Any organisation that holds data on EU citizens (regardless of whether they are based outside the EU) is subject to the GDPR and it impacts everyone that deals with that information.

The GDPR applies to organisations within the EU as well as organisations outside the EU that process or control data related to living EU residents or nationals.

The GDPR primarily impacts:

Data Controllers - they say how and why personal data is processed

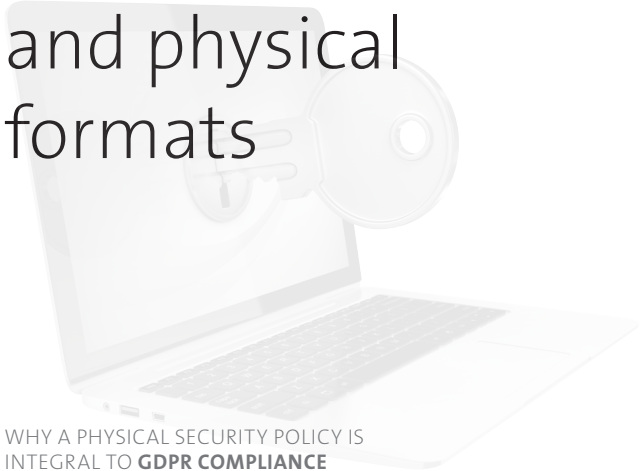
Data Processors - people acting on the controller's behalf

It is the responsibility of these two figures to ensure that their clients are fully compliant with all aspects of the GDPR, to avoid incurring any fines.

Effective and demonstrable GDPR compliance should involve all members of an organisation that deal with personal and sensitive information. For example, a salesperson's laptop will hold sensitive information about their customers and should be physically secured when they are working remotely.

A Data Processor or Data Controller may need to **appoint a Data Protection Officer** and keep records of all processing activities they perform on behalf of clients.

GDPR covers **personal data** & **sensitive personal data** in electronic and physical formats



It is important to consider what kinds of data the GDPR will apply to before constructing a compliance policy for your organisation.

Data within scope of the GDPR includes any information about an identifiable person and is divided in to two categories:

Personal data includes data such as an email or physical address as well as to any information that can be used as an online identifier - e.g. an IP address.

Sensitive personal data covers more intimate information including ethnic origin, political opinions, religion and health data. In general, organisations require stronger grounds to process this information than 'regular' personal data.

The GDPR is concerned with personal data handled by organisations in both **electronic and physical formats.**

A Business Framework for **GDPR Compliance**

By reviewing people, processes and technology, organisations will be able to construct clear frameworks of a data security policy, which will help support compliance in all areas of the GDPR.

WHY A PHYSICAL SECURITY POLICY IS INTEGRAL TO **GDPR COMPLIANCE**

Organisations have three main areas that must be reviewed in order to achieve GDPR compliance:

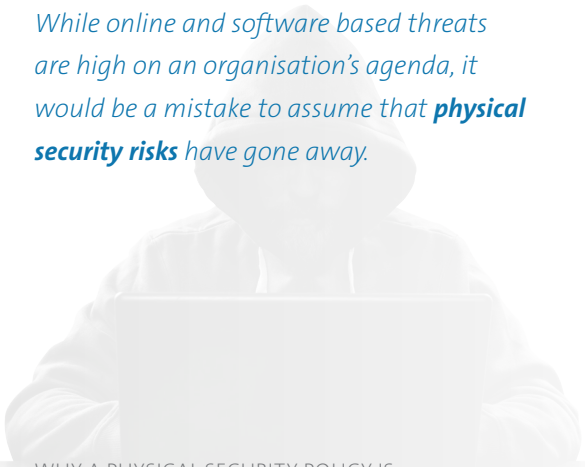
People - staff ownership and responsibility of any data processed by them within the organisation is critical. An organisation must set out clear rules to each and every employee for the proper management of all electronic data held within the business. These regulations put into action the requirements of the GDPR regarding the handling of all data. For example, you may wish to introduce clear rules about the use of sensitive data held on employee laptops and the process for deleting data.

Processes - this relates to the processes within the organisation. For example, to manage the use of data such as processing or storing data on customers. It is crucial that businesses are reviewing all of their current processes relating to data. Once gaps and weaknesses within their existing procedures are identified, a framework plan must be developed by the business that will see these areas strengthened or replaced, where necessary, in order to comply with the GDPR.

Technology - current IT capabilities and requirements should also be reviewed and adjusted accordingly before May 2018. It is up to the individual business to ensure that any existing systems that do not fully support the regulations are either improved or replaced, to avoid incurring any potential fines after the GDPR comes into effect.

Why Does **Physical Security** Matter?

*While online and software based threats are high on an organisation's agenda, it would be a mistake to assume that **physical security risks** have gone away.*



WHY A PHYSICAL SECURITY POLICY IS INTEGRAL TO **GDPR COMPLIANCE**

Having discussed what the GDPR requires businesses to do, it is now pertinent to address the issue of physical hardware security within organisations and why it is a key concern for businesses as they prepare to meet the GDPR's requirements.

After online-based threats and the unintended disclosure of data, **portable devices** and **physical loss** are the biggest source of data breaches[2]:

Every day, on average over **5 million data records are lost or stolen**[3], with more than **a third of businesses not having a physical security policy in place** to protect laptops, mobile devices and other electronic assets.[4]

Given the level of potential fines outlined by the GDPR, an increasingly mobile workforce and the growth of hot-desking, physically securing laptops and mobile devices is a sensible precaution, both in and out of the workplace. Locking down a device is a quick and easy way to deter theft - and also very effective.

Kensington offers a full range of **locking solutions** for a wide variety of laptops, including devices without a security slot. The SecureTrek™ range of cases can be physically anchored to a fixed object environments such as airports, hotels and trade shows.

Physical Security Still Accounts for **Many Common Security Breaches**

WHY A PHYSICAL SECURITY POLICY IS INTEGRAL TO **GDPR COMPLIANCE**

Of 697 data security incidents recorded between April and June 2017 by the UK's data protection regulator, the Information Commissioner's Office (ICO), 6% were due to the theft of an unencrypted device, with data being left in an insecure location or the theft of the only copy of encrypted data accounting for an additional 3.5%[5].

In the **financial sector** 25% of breaches are due to lost or stolen devices and are the most frequent cause of data leakage, being especially tempting targets because of the volume of sensitive data stored and used.[6]

Within **healthcare** physical theft or loss is the biggest cause of security incidents, accounting for 32% of over 100,000 incidents surveyed in 82 countries.[7]

Current IT capabilities and requirements should also be reviewed and adjusted accordingly before May 2018. It is up to the individual business to ensure that any existing systems that do not fully support the regulations are either improved or replaced, to avoid incurring any potential fines after the GDPR comes into effect.

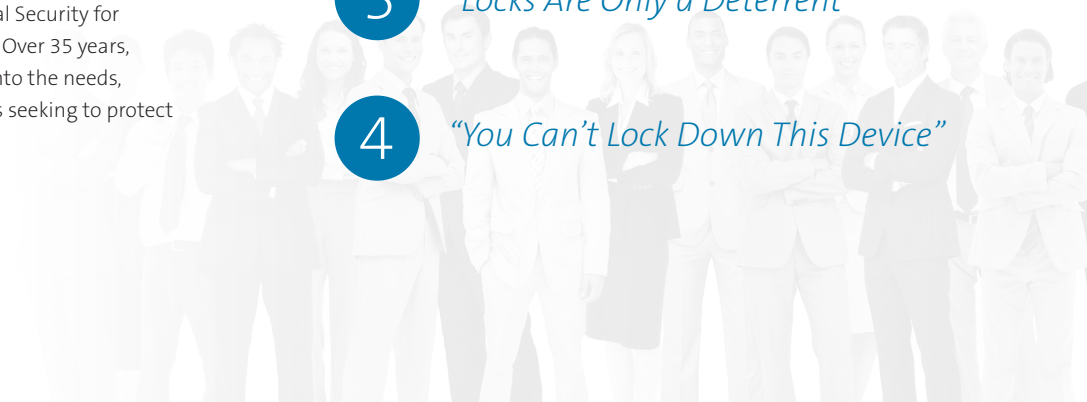
User Co-Operation is Critical to GDPR Compliance

If we can conclude that physical security remains vital to information security, then the question is: what can organisations do about it?

Kensington is the World's Leader in Physical Security for IT hardware, originator of the Laptop Lock, Over 35 years, Kensington has gained valuable insights into the needs, wants and challenges facing organisations seeking to protect themselves and comply with the GDPR.

These insights have led us to believe that there are four main objections and barriers to effective physical security in organisations:

1. *"We Operate In a Secure Environment"*
2. *"We Use Encryption & Cloud Storage"*
3. *"Locks Are Only a Deterrent"*
4. *"You Can't Lock Down This Device"*



Overcoming Barriers to GDPR Compliance

WHY A PHYSICAL SECURITY POLICY IS INTEGRAL TO **GDPR COMPLIANCE**

"We Operate In a Secure Environment"

CCTV, employee passes and security personnel can create a heightened sense of security and lower perceived risk. 58% of laptops are stolen from the office and 85% of IT managers suspect internal theft.[8] Data is at risk as soon as the laptop has been taken, especially as only 3%[9] are ever recovered. Laptop locks prevent opportunistic theft and the time and cost investments associated with tracking the offender and replacing the laptop, let alone the potential penalties under GDPR.

"We Use Encryption and Use Cloud Storage"

Encryption is not a solution when faced with a stolen device containing non-backed up data. Even when users are not storing data on their hard drives, the productivity loss experienced by an employee without their primary computing device is worth protecting against. Take a walk around your building. How easy would it be for a courier to take a device? 49% of SME's take 2 to 4 days to replace a lost or stolen laptop.[8]

"Locks Are Only a Deterrent"

Laptop locks are primarily designed to protect against opportunistic theft. But they are also very effective at preventing theft. IDC reported that, of IT Managers that have suffered laptop theft, 52% state that the thefts would have been prevented by a lock.[8]

Overcoming Barriers to GDPR Compliance

"You Can't Lock Down This Device"

With the move to thinner form factors, today's computing devices may not incorporate the industry-standard Kensington Security Slot™. However, it is a misconception to believe that such devices cannot be physically secured. Even devices without a security slot can be locked down to prevent opportunistic theft. Kensington offers a full range of solutions for a diverse array of devices:

MicroSaver® 2.0 and ClickSafe® 2.0

For devices using the standard Kensington Security Slot™ as used on 90% of business devices.

Kensington Security Slot™ on laptop and desktop

MicroSaver® 2.0 lock attaches directly to Security Slot

ClickSafe® 2.0 lock attaching via ClickSafe Anchor

N17 for Dell 2017 Devices

For devices using the Wedge Security Slot as used on Dell Latitude 2017 models (later) and selected other devices.

Wedge Security Slot

Laptop anchored to fixed object

NanoSaver™ Keyed Laptop Lock

For devices using the Kensington Nano Security Slot™, used on ultra-thin devices

Kensington Nano Security Slot™

NanoSaver™ Keyed Laptop Lock

Microsoft Surface™ Locking Solutions

Device-specific locks for the Surface™ Pro, Surface™ Book and Surface™ Studio

Keyed Lock for Surface™ Pro

Locking Kit for Surface™ Studio

Locking Bracket for 13.5" Surface™ Book

Laptop Locking Station 2.0

For devices without a security slot including the Surface™ Laptop and MacBook Pro®

Laptop Locking Station with MacBook Pro®

Find the ideal locking solution for your laptop or device by visiting:
kensington.com/securityselector

6 Key GDPR Points to Consider

1. Consider appointing a Data Protection Officer

This officer must be fully commensurate with the organisation's responsibilities regarding GDPR and have a thorough understanding of what data within your organisation counts as 'personal', where it's kept, who has access to it, how to spot breaches when they occur and who to report this to. **The Data Protection Officer doesn't have to be an employee - you can outsource this function.**

2. Assess Your Systems

Review all contracts, technology support, procedures and tools that relate to the processing, handling, storing and deleting of data to enable you to identify any weaknesses or gaps that require changes to be made.

3. Develop a Strategy

Construct a new strategy that will ensure full compliance with the GDPR. This strategy may encompass new investment in technology, revise staff procedures and responsibility for data processing and create new roles within the organisation.

WHY A PHYSICAL SECURITY POLICY IS INTEGRAL TO **GDPR COMPLIANCE**

6 Key GDPR Points to Consider

4. Implement New Organisation Policy

The next step towards GDPR compliance is to put your plan into action throughout all levels of the organisation. Invest and introduce new technologies and systems required in the workplace and publish an informative data handling and processing guide.

5. Employee Engagement

Launch your new data compliance policy to all staff; provide training, information and guides to employees so they are educated and aware of the changes taking place and their responsibility in ensuring that the company meets the requirements of the GDPR.

6. Review and improve

After launching your GDPR compliance plan, now is the time to review and improve before the regulations come into effect. Identifying any necessary improvements well in advance of the GDPR's deadline, once May 2018 arrives your organisation will have successfully and efficiently adapted to the changes and be completely compliant.

Solutions

Laptop and device locks are a direct response to the need for organisations to encourage employee compliance with a physical hardware security policy and reduce the risks of potential security breaches. Additional solutions can further help lower this risk in and outside of the office environment.

SecureTrek™ Luggage

The SecureTrek™ range of rollers, cases and backpacks have the ability to be anchored in locations where theft is a concern, such as airports, hotels and trade shows.

Privacy Screens

'Visual hacking' is easy, happens quickly and often goes unnoticed.[10] A privacy screen reduces the viewing angle and reduces this risk.

USB Port Blockers

System administrators can physically prevent users from connecting USB devices, reducing the risk of unauthorised data copying or conversely uploading malware to a system.

Cabinets

A fast and simple way of charging, syncing and securing multiple tablets and ultra-thin laptops.

VeriMark™ Fingerprint Key

Provides a simple, fast and secure biometric Windows Hello™ logon and works with services requiring two-factor authentication, protecting against unauthorised access and enhancing online security.

Sources

1. Kensington IT Security & Laptop Theft Survey, August 2016
2. 2016 Data Breaches - Privacy Rights Clearinghouse
3. Breach Level Index, September 2017
4. Kensington IT Security & Laptop Theft Survey, August 2016
5. Information Commisioner's Office - https://ico.org.uk/action-weve-taken/data-security-incident-trends
6. Financial Services Breach Report, Bitglass, 2016
7. Verizon Data Breach Investigations Report 2016
8. IDC Executive Brief 2010 - Laptop Theft: The Internal and External Threat
9. IDC White Paper 2007 - The Threat of Theft and Loss of Laptops for the SME
10. Ponemon Institute Visual Hacking Experiment, 2015

Kensington®

kensington.com

FOR MORE INFORMATION CONTACT:

Maddie Neale
UK B2B Sales Manager
maddie.neale@kensington.com
Mobile: +44 (0)7740 061 887

Keith Ward
Key Account Manager
keith.ward@kensington.com
Mobile: +44 (0)7740 061 887

Paul Greenfield
Business Development Manager
paul.greenfield@kensington.com
+44 (0)7734 596 276

Scott Houchin
Key Account Manager
scott.houchin@kensington.com
Mobile: +44(0)7557 268 013

The Professionals' Choice™