HYPERTEC
MAKING IT PERFORM

EU Data Protection Compliance

EU Data Protection Law Reform

The law around Data Protection is changing. Since the EU Data Protection Regulation was first introduced in 1995, technology has evolved dramatically. Mobile devices are now an essential tool in business communication and efficiency. However, this means that sensitive data is now being moved and accessed outside of the office. As a result, new policy reforms have been implemented to protect confidential data.

Article 30 of the new reform addresses the security of processing data:

1a. Having regard to the state of the art and the cost of implementation, such a security policy shall include:

(a) the ability to ensure that the integrity of the personal data is validated;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data.

(c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident.

Simply put, organisations are required to implement an appropriate security strategy to protect personal data.

Hypertec can help you stay compliant with the new 2015 Data Protection Legislation reform.

Hypertec has 3 dedicated **Security Categories:** IT Security, Physical Security and Security.

IT Security




View All ▶ GO

Our IT Security Category addresses a number of IT Concerns Including:

- Data Accessibility
- Data Encryption
- Authentication & Access Control
- Data Recovery

Who Needs to Comply?

"Today European companies have to adhere to stricter standards than companies established outside the EU but also doing business on our Single Market. With the reform, companies based outside of Europe will have to apply the same rules. We are creating a level-playing field."

At the moment, when a business is established in one Member State, only the Data Protection Authority of that Member State is competent, even if the business is processing data across Europe. The proposals aim to correct this anomaly.

How To Comply

The best way to comply with the change in legislation is to implement a data protection strategy which includes **data encryption.**

Best practice would be to implement state of the art technical controls which renders personal **data unintelligible to unauthorised users.** Therefore if encrypted data becomes lost or stolen, it is essentially worthless.

Non Compliant Data Breaches

If a company fails to comply with the new legislation change then Article 79* stipulates that the supervisory authority can impose at least one of the following sanctions:

(a) A warning in writing in the case of a first and/or non-intentional non-compliance.

(b) regular periodic data protection audits.

(c) **A fine up to EUR 100,000,000 or up to 5% of the annual worldwide turnover** in the case of an enterprise, whichever is higher.

Read the Reforms ▶ GO

*EU Data Protection Regulation Proposals Whitepaper - SOPHOS.
*Edward J Correia - crn.com

Physical Security




View All ▶ GO

Our Physical Security Category addresses a number of IT Concerns Including:

- Data Leakage
- Device Protection
- Visual Hacking
- Anti - Theft

Data Security




View All ▶ GO

Our Security Category addresses a number of IT Concerns Including:

- Shredding Compliance
- PED/POS Security
- Media Destruction
- Screen Protection

01488 686 844
Info@hypertec.co.uk