
DaraIT
GDPR Security
Solutions
November 2017

Introduction

The General Data Protection Regulation (GDPR) was approved by the EU Parliament in April 2016. The goal of GDPR is to give private citizens better controls over their personal data and the ability to hold businesses to account for misusing their data.

The UK Parliament has since created a new piece of legislation that will adopt the requirements and tenants of GDPR from May 25t 2018 and will continue after Brexit. Much like the health and safety act of 1974, GDPR is good in principle but has caused a great deal of uncertainty for many businesses as the rules apply to everyone, regardless of size or revenue. Legal counsel should be sought and a business plan made to ensure compliance before the deadline. The penalties for wilfully ignoring GDPR and losing customer data starts at up to twenty million euro (Or 4% of global turnover, whichever is higher)

One crucial area of GDPR is cyber-security. Businesses will need to take proactive steps to protect the personal data of EU/UK citizens. No cyber-security solution will make a business compliant yet is vital as part of a wider plan of action for the business.

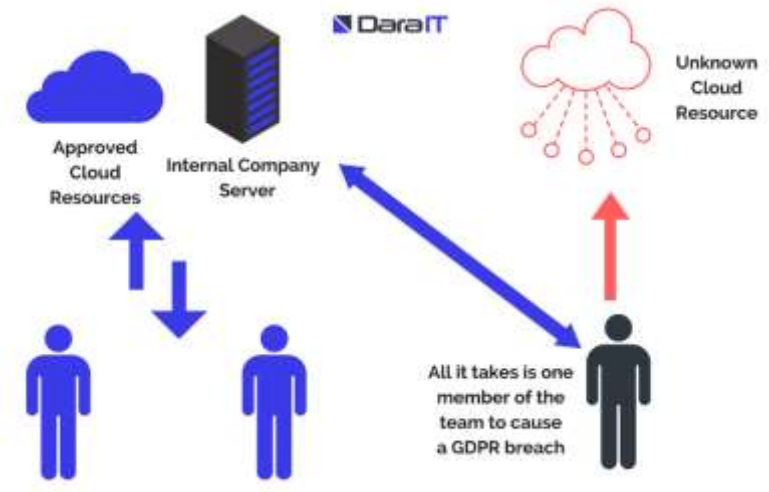
Contents:

Where Is The Data

A key test for GDPR is for a business to identify where it is storing personal data. Cloud computing has allowed companies to make use of Dropbox and other services to store data.

Sometimes this is against company policy. An employee may begin using a new online service which may be located outside of the UK and not compliant.

A staff member may have an online to-do list which contains names and contact details of their prospects. Or a calendar booking system. The issue is that this data is being held by a third party service.

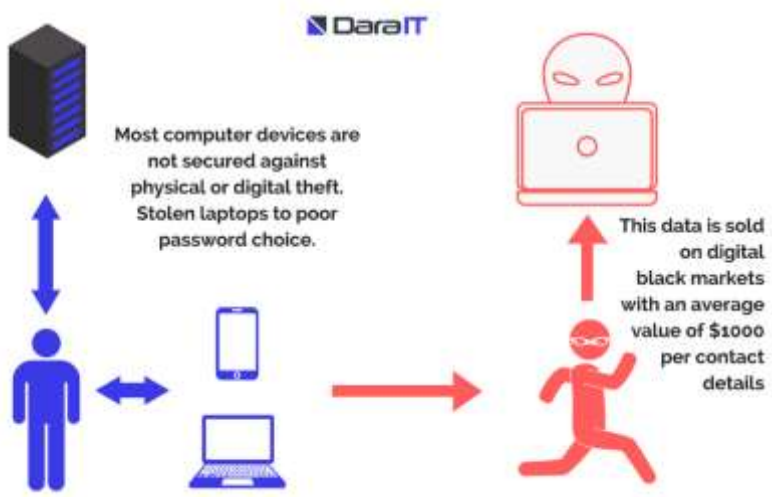


There are tools which will monitor what online services and tools your business is using on a day to day basis so that you always know where your data is held. You can also choose to block certain services from being used on company devices at all.

Do you really know that all personal data is only stored on company devices?

Who Has Access

A requirement for GDPR is defining who has access to the data and that you have sufficient controls in place to prevent unauthorised access. You also need to be ready to prove to the ICO that you have taken sufficient steps to prevent a breach of personal data.



Most IT systems in businesses are not secured against a physical intruder. Whether a break in at the office or a device stolen from a travelling employee, digital security is only part of the answer.

Viruses and malware which can grant hackers access to the business should also be accounted for in the plan for GDPR compliance, what steps have been taken? How do you know that there is not a security breach in the business currently?

The number one security breach for small to medium sized businesses comes down to phishing emails and poor password choice. An attacker does not need to break into the office when they can type "Password1" into a website to gain access to the company data or send an email with a virus which will give them unrestricted access to all files.

A requirement under GDPR is that all personal data is encrypted when sent or stored. Do you utilise encryption in your business?

Key Solutions For GDPR

You may need to apply one or all of these to meet GDPR compliance in your business

- Full Device Encryption

A computer might be protected with a password to log into it. There is a very low-tech way of bypassing this login and accessing all data. Device encryption means that even if an IT professional tries to access the data, they will be unable to.

- Hacker Detection System

Proactive monitoring for hackers and malware in the network. This means that if defences are breached, a quick response can be made to address it. Many companies are unaware of a breach for weeks or months at a time until it is far too late.

- Internet Apps Monitoring

Know and understand what third party cloud apps and websites are being used in your business. You can also take steps to explicitly block them from being used at all, reducing the likelihood of accidental breach.

- End User Cyber Awareness Training

No matter what tools you invest in, some degree of training is essential for staff. Computer security 101 is vital in 2018. Learning the red flags that make up cyber-attacks. Advanced versions are available for IT professionals who should be fully equipped to protect the business.

- Third Party Security Auditing

The value of this very much depends on the scope and purpose of the audit, along with the competency of the company you choose. The audit ensures that security best practices are being followed and will identify any weak points that need to be addressed. To avoid a conflict of interest, the company doing the audit should not be the same company that provides a security solution.

Your IT team should be able to research these topics and propose the right solution for your business. You can also speak with us at Dara IT and we can provide advice, training or implement these solutions fully.

Resources

Information Commissioner's Office Guide to GDPR: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Sophos GDPR Compliance Check Tool: https://www.sophos.com/fr-fr/lp/compliancecheck-nl.aspx

Do you offer free Wifi: https://www.itgovernance.eu/blog/en/how-the-gdpr-will-affect-wi-fi-providers/

Symantec – Six Cybersecurity habits to give up: https://medium.com/threat-intel/bad-cybersecurity-practices-c814ca6e65db

Article 32 of GDPR (Security): https://gdpr-info.eu/art-32-gdpr/

Sharing data with third parties: https://martechtoday.com/gdpr-mean-third-party-data-processors-208098

If you need help or advice on possible security solutions for your business, speak with our team on 0203 5826 695 or email security@darait.co.uk