

GDPR - Keeping personal data safe and secure

Submitted by: PR Artistry Limited

Thursday, 12 March 2020

Protecting personal data is at the heart of the General Data Protection Regulation (GDPR) but there remains confusion between gaining permissions to hold and process this data, and protecting it from theft or compromise. Guy Lloyd at CySure explains how understanding and protecting personal data is core to GDPR compliance.

Almost 2 years on from the introduction of the EU General Data Protection Regulation (GDPR) many business owners still lack knowledge about the consequences of not adequately protecting personal data. GDPR isn't an optional requirement, it is enshrined in UK law in the Data Protection Act 2018. This lack of understanding of the legal necessity to protect personal data is proving costly to business. Since the introduction of GDPR, EU data protection authorities have fined organisations a total of €114 million (i).

Securing personal data

If a company isn't already compliant with GDPR, the time to act is now. A key principle of GDPR is a business must process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle' described in the regulation. But what does this mean in practice? All businesses, regardless of size, must be able to demonstrate:

- They have undertaken an analysis of the risks presented by processing data
- Implemented appropriate levels of security to safeguard the data
- Have an information security policy and taken steps to implement it
- As stated ICO guidance - have put in place basic technical controls, such as those specified by established frameworks like Cyber Essentials (ii).

In summary, a business must have appropriate security to prevent the personal data it holds being accidentally or deliberately compromised. Additionally, any measures taken must ensure the 'confidentiality, integrity and availability' of the company's systems and services and the personal data it processes within them.

Get certified with Cyber Essentials

Unless there is awareness of the potential risks then it is almost impossible to create a strategy for minimising those risks. In the UK, Cyber Essentials is a government and industry backed scheme to help all organisations protect themselves against common cyber-attacks. In collaboration with Information Assurance for Small and Medium Enterprises (IAMSE) they set out basic technical controls for organisations to use which is annually assessed.

Certification provides a practical framework for an organisation to assess its current cyber hygiene levels. It also lays the foundation to developing policies and procedures to mitigate against threats that can impact business operations.

Being fully Cyber Essentials compliant is said to mitigate 80% (iii) of the risks faced by businesses such as phishing, malware infections, social engineering attacks and hacking. It aims to provide businesses with a strong base from which to reduce the risk from the most prevalent cyber-threats.

Simplify the path to Certification

Businesses need to get proactive in protecting their data and that of their customers and suppliers. It is not a matter of eventually getting around to it – it's a legal requirement and failure to comply comes with a hefty fine!

Becoming GDPR compliant can seem a daunting task initially but there are affordable solutions to support businesses through the process. For example, CySure works with iCaaS GDPR Management which provides easy to use software and comprehensive online training to ensure responsible data handling practices.

Using an online security compliance management solution that incorporates GDPR and Cyber Essentials is a simple and cost-effective way to achieve compliance.

The benefit to this is that the system delivers a staged approach to compliance and certification, guided by a virtual online security officer (VOSO). Using a system that has the security components of GDPR mapped out into a set of discrete actions becomes a manageable way of meeting and maintaining compliance. The outcome is that GDPR becomes ingrained in business practice. The benefit is that it demonstrates to customers and suppliers a commitment and diligence towards keeping personal data safe and secure.

Guy Lloyd is a Director at CySure

(i) DLA Piper

(<https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/>)

(ii) ICO

(<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/>)

(iii) NCSC (<https://www.ncsc.gov.uk/section/products-services/cyber-essentials>)

About iCaaS

iCaaS GDPR Management is an advanced cloud-based solution to strengthen data compliance. It builds trust and protects client reputation. Comprehensive online training is available to ensure responsible data handling practices supported by simple, easy to use software. iCaaS helps businesses achieve, manage and maintain full GDPR compliance and the intuitive software helps save time and money whilst instilling confidence within customer base that they are being responsible with their data.

For more information please visit iCaaS (<http://www.myicaas.com>)

About CySure

CySure is a cyber security company founded by experts with extensive experience in operational and risk management. The company has offices in London (UK) and California (USA) and CySure's flagship solution – Virtual Online Security Officer (VOSO) is an information security management system (ISMS) that incorporates GDPR, US NIST and UK CE cyber security standards to guide organisations through complex,

emerging safety procedures and protocols, improve their online security and reduce the risk of cyber threats.

For more information please visit CySure (<http://www.cysure.net>)

Press contact: Mary Phillips/Andreina West

PR Artistry Limited

T: +44 (0)1491 845553

E: mary@pra-ltd.co.uk