GDPR - the most common misconception and 4 things every business should know

Submitted by: PR Artistry Limited
Thursday, 25 October 2018

Joe Collinwood at CySure addresses misunderstanding surrounding cookies and consent in terms of GDPR

The EU General Data Protection Regulation (GDPR) came into force on 25 May 2018 with great fanfare, and rightly so. It is the most significant change to data protection legislation in Europe for over two decades and puts individuals back in the driving seat of how their data is used. However, there continues to be a lot of confusion within the business community on the steps that need to be taken to ensure compliance. Consequently, many businesses are suffering from 'GDPR fatigue' caused by over exposure to security and legal rules.

GDPR applies to even small business
GDPR is designed to govern how every organisation treats the personal data it collects. The size and location of the business is irrelevant, if an organisation holds personal information on individuals in the EU, as consumers or employees, then the regulation applies. In practice, this means that the principles guiding how data should be collected, processed, shared and stored apply to virtually every business within the EU, as well as those beyond Europe with customers the European Union. There's no exemption for small businesses or sole traders.

For small and medium sized enterprises (SMEs) compliance can often be unclear as many companies have relied on their IT person, an outsourcer or external legal services to advise and implement data privacy measures. This has left some business owners unsure of what actions are needed to meet the requirements of the legislation.

Cookies and consent - 4 things every business should know
There is a common misconception that GDPR is purely about consent and whilst this is a critical obligation, it is by no means the only area of focus. Small businesses that have an online presence must obtain clear and unambiguous consent before collecting and processing personal data.

Some businesses may believe they are GDPR compliant by having a cookie consent and privacy policy on their website, however GDPR requires organisations to meet a more comprehensive set of privacy obligations, such as;

• Data minimisation – businesses should only collect personal information which is directly relevant and necessary to accomplish a specified purpose. If you don't need it, don't collect it! Companies should also periodically review the data they hold ensuring the deletion of anything not needed

• Integrity and confidentiality – businesses must ensure they have appropriate security measures in place to protect the personal data held. This extends to ensuring that any personnel that have access to personal data have a legitimate need to do so and receive regular cyber security training

• Data protection by design – organisations are obligated to consider data protection and privacy issues upfront in everything they do. In essence, this means integrating or 'baking in' data protection

into processing activities and business practices, from the design stage right through the lifecycle

• Breach notification – there is a duty on all organisations to report certain types of personal data breaches to the relevant supervisory authority. Organisations should prioritise developing a robust detection, investigation and internal reporting procedure before a breach happens. Certain types of personal data breaches must be reported within 72 hours of becoming aware of the breach, so it is essential that processes are in place.

The importance of certification
Certification is a way of demonstrating that an organisation's method of processing personal data complies with GDPR requirements. Organisations concerned about meeting compliance regulations could benefit from undertaking a certification route, such as Cyber Essentials or the IASME Governance standard, guided by a virtual online security officer (VOSO) as part of a wider information security management system.
Obtaining certification for data processing can help SMEs to:

• Have a competitive advantage
• Be more transparent and accountable
• Create effective safeguards to mitigate the risk around data processing and the rights and freedoms of individuals
• Improve standards by establishing best practice
• Mitigate against enforcement action.

The benefit of certification via an information security management system (ISMS) is that SMEs can take advantage of the expertise of online cyber security consultants at a fraction of the cost of a full time in-house security specialist or a team of consultants. The process can be broken down into a set of discrete actions providing an easy to follow, staged approach to compliance. By taking away much of the time consuming administrative burden, a Virtual Online Security Officer frees up management to focus on policies, procedures and employee training to create an aware and compliant culture.

The processes necessary for GDPR compliance can deliver many commercial advantages, after all data is the lifeblood of any organisation. By taking a proactive stance towards GDPR, SMEs can take control of their data and engage with customers and prospects on a deeper and more personalised level. SMEs that treat GDPR as a box ticking exercise are missing the wider opportunity to demonstrate trust and confidence with their target audience – their customers.

Joe Collinwood is CEO of Cysure.net

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.

CySure also supplies organisations with cyber insurance to supplement their security strategy and offset crippling forensic and remediation costs in the event of a cyber breach.

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