CySure

Virtual Online Security Officer

Manage your business safely and avoid cyber threats

Confusion in the business community

There is a lot of confusion in the business community regarding what needs to be done to be GDPR compliant. This has resulted in many companies suffering "GDPR fatigue" caused by over-exposure to security rules with little understanding of what they are required to do. There are good reasons as organizations have relied on their IT department/outsourcer to have implemented appropriate security measures while being advised by their legal counsellors who are mainly focused on protecting the rights of the subject whose personal data they are collecting. Companies that say they are GDPR compliant are in the main referring to the processing of explicit consent from a subject by way of data privacy/data protection and cookie statements to:

- Capture, process and store a subject's personal data.
- Parental consent if the subject is a child.
- Justification for obtaining personal information.
- Provide access or data portability requests to a subject's personal data.
- Correcting of inaccurate records, deleting records or suspending the processing of records.
- Confirming whether you are a data controller or a data processor.

Legal obligation to protect the data

However organizations forget that they have a legal obligation to protect the data they have collected. Organizations need to understand that while GDPR has superseded the Data Protection Act the act enshrines the GDPR into UK law, and supplements the GDPR by filling in the sections of the Regulation relating to data security.

The act places an obligation on data controllers to have "appropriate security measures" in place to prevent "unauthorized access to, or unauthorized alteration, disclosure or destruction of the data and against accidental loss or destruction." The GDPR requires that "Taking into account the state of the art, the costs

of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and processor shall implement appropriate technical and operational measures to ensure the level of security appropriate to the risk….account shall be taken in particular of the risks that are presented by processing …which could lead to physical, material or non-material damage."

What are the specific security requirements

So, what are the specific security requirements that an organization should implement? The ICO recommends Cyber Essentials as a good place to start, ideally the Plus version. It covers the minimum infrastructure security requirements.

Those being: -

- Firewalls
- Secure configuration
- Password- based authentication
- User access control
- Malware protections
- Patch management

Minimal organizational measures

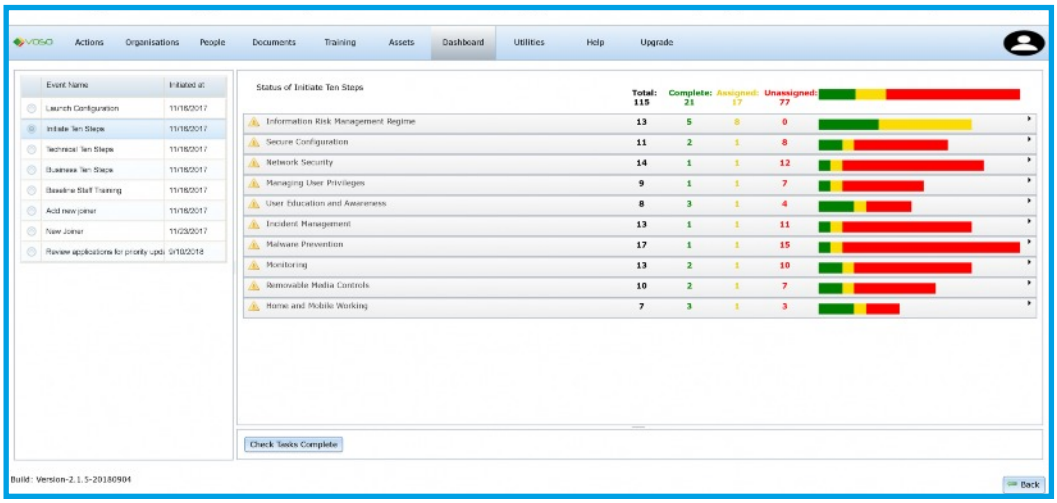
The next stage is the minimal organizational measures under GDPR covering governance. No matter what technical or physical controls are in place, people are the biggest risk. IASME provides an affordable standard to follow with a governance process to ensure that security is elevated from IT to involve senior management and leadership who set the standard for the rest of the workforce. An example would be the continual vetting and training of staff, contractors, vendors and suppliers. The monitoring of operations to ensure that policies are being adhered to and that risks are continually assessed and mitigated. For example organizations must have procedures in place to manage staff turnover. "New joiners" to ensure that all staff are aware of their responsibilities and "leavers" to ensure the quick removal of access permissions and the retrieval of data.

Meeting compliance regulations

Organizations concerned about meeting compliance regulations will benefit from undertaking a CE, CE Plus, IASME certification route guided by a virtual online security officer (VOSO) as part of an information security management system. Certification through CE and IASME indicates that data controls have been subject to audit against a recognized standard. The benefit of this approach 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 VOSO frees up management to focus on policies, procedures and employee training to create an aware and compliant culture.

Appropriate security measures

Having cookie consents on your website does not mean a company is GDPR compliant unless it knows that it has implemented the appropriate security measures to prevent unauthorized disclosure as part of GDPR. Following a phased, certification process, an organization's workforce can clearly understand what their roles and responsibilities in ensuring compliance. They will know that everyone from the senior executive down plays an important role in protecting their company and their client's personal data. By doing so they ensure their organization avoids the business disruption and penalties for failing to comply which in turn protects their jobs and income.



CySure provides a virtual cyber security officer that tells you what you should be doing and when, to protect your online equipment and stored data.

CySure Limited

2, Printer's Yard, 90A The Broadway, Wimbledon, London, SW19 1RD

D : +44 (0) 20 8412 1106 | W: www.cysure.net