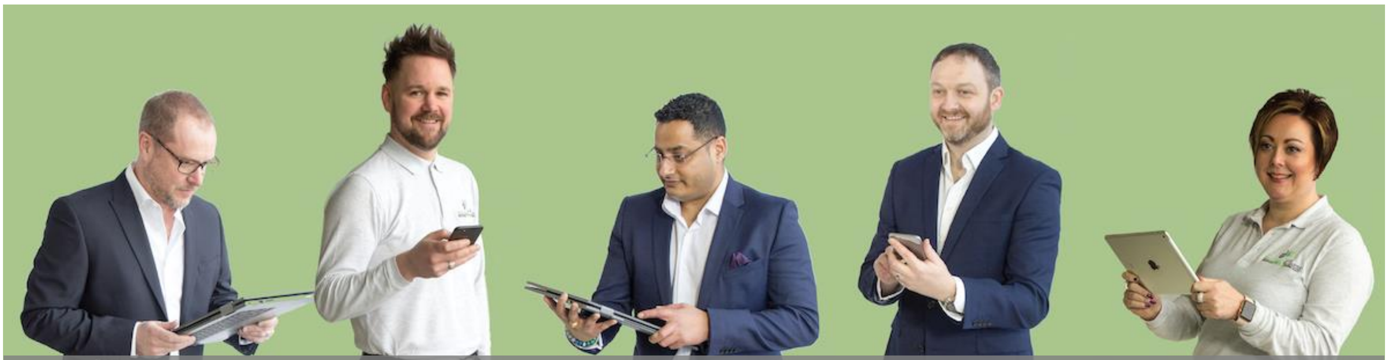

Does ISO 27001 : 2013 cover the requirements of the General Data Protection Regulation?

Both the ISO 27001 framework and the GDPR requirements cover data security within a business and share many common themes.

However, implementing the new ISO 27001 Management System does not necessarily mean that your EMS Vendor will have fulfilled their responsibilities as a supplier of software handling personal data in accordance with the GDPR

What is the General Data Protection Regulation (GDPR)?

The GDPR is a set of laws and guidelines covering the handling of personal information. This regulation is being introduced in May 2018 by the European Union and will affect companies - both inside and outside of the EU - that collect, hold, use or process the personal information of EU citizens. Failure to comply with the GDPR could result in fines of up to 4% of annual global turnover.

GDPR principles

The regulation is split into six guiding principles which cover the general aims of the framework. They consider why personal information is collected, how long it is stored for, and the way in which it is stored.

Data subject rights

A person – called a data subject in the regulation – has a number of rights when it comes to companies storing, accessing or using their personal information. These rights take into account special cases such as sensitive information and records held on children. The GDPR sets out these rights and describes your responsibilities as an organisation to uphold them.

Your obligations

It is an important part of the regulation that you can prove your adherence to it. You should also be able to deal with any issues – such as breaches of information security – appropriately and according to the steps specified in the regulation.

Companies that regularly process large amounts of personal data, or handle special data categories such as criminal convictions, must assign a Data Protection Officer (DPO). The DPO will be responsible for proving and ensuring that your organisation complies with data protection law and practices

Does ISO 27001 satisfy the GDPR requirements?

The following information is provided for guidance and is based on a fully integrated, well-managed ISO 27001 Management System that already incorporates controls and processes for handling personal information.

To determine how well your Management System covers GDPR, we would always recommend a gap analysis be performed.

The principles

Principle	Elector8	ISO 27001
Lawful, fair and transparent processing	Full Data Audit	Partial coverage
Data should be used as specified	Full Data Audit	Partial coverage
Data should be limited to what is necessary for the specified use	Redacted Data	Partial coverage
Data should be accurate	Always Accurate	Partial coverage
Data that can identify individuals for no longer than necessary	Auto Cleansing	Partial coverage
Data should be protected at all times	Encrypted at transit and rest	Full coverage

Data subject's right

Right	Elector8	ISO 27001
The right to be informed	Right Click and Communicate	Partial coverage
The right to object	2 Way comms	Partial coverage
The right to erasure	Included	Partial coverage
The right to restrict processing	Included	Partial coverage
The right of access		No coverage
The right to data portability	Quick Extracts	Partial coverage
The right to rectification	Easy to amend	Partial coverage
Rights regarding automated decisions/profiling		No coverage

Other obligations

Obligation	Elector8	ISO 27001
Information security breach notification	Full Data Audit	Full coverage
Restrictions on gathering children's data	Covered	Partial coverage
Specific and informed consent to gather data	Full Data Audit	Partial coverage
Assignment of a Data Protection Officer	Held in EMS	Partial coverage
Protection of data that is accessible by suppliers	You hold the Encryption Key	Full coverage
Performing risk assessments	In Built	Full coverage
Performing a Data Protection Impact Assessment	In Built	Partial coverage

What next?

If you are concerned about your data handling processes and would like to align your systems with the requirements of the GDPR, you should consider our GDPR Readiness Assessment.

During the Readiness Assessment you will benefit from training, a Data Protection Impact Assessment (DPIA), a Gap Analysis, and guidance on Data Mapping