Why CE Certification?

It is a requirement of GDPR that personally identifiable information is:

Source ICO/EU GDPR - 7th Principle (regulation)

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

https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to €20 million, or 4% of your total worldwide annual turnover, whichever is higher.

IASME Self Assessment Questionnaire

38. Which security accreditations are held by the public cloud providers used by your organisation?

64. Where you disclose personal data to a supplier/provider does the contract explicitly impose the obligation to maintain appropriate technical and organisational measures to protect personal data in line with relevant legislation?

90. Do the contracts with all your suppliers ensure that they meet the requirements of your security policy around handling data and keeping information secure?

132. How do you ensure that all your suppliers (including cloud providers and sub-contractors) follow information security procedures that are certified to be the same as, or more comprehensive than, the information security procedures followed by your own organisation for the data involved in that contract?

An example of such certification would be an independent audit of the whole business to ISO27001, the IASME Governance standard or Cyber Essentials.

Why do I need to do this?

In the event of a complaint to the ICO or a report of a data breach (which is a legal requirement) you as a controller or processor will need to demonstrate that you ensured appropriate security was in place. That extends to suppliers and contractors to your business.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

Whenever a controller uses a processor it needs to have a written contract in place. The contract is important so that both parties understand their responsibilities and liabilities.

The GDPR sets out what needs to be included in the contract. In the future, standard contract clauses may be provided by the European Commission or the ICO, and may form part of certification schemes. However at the moment no standard clauses have been drafted.

Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor which adheres to an approved code of conduct or certification scheme may help controllers to satisfy this requirement – though again, no such schemes are currently available.

Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

- The GDPR makes written contracts between controllers and processors a general requirement, rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures) under the DPA.
- The GDPR envisages that adherence by a processor to an approved code of conduct or certification scheme may be used to help controllers demonstrate that they have chosen a suitable processor. Standard contractual clauses may form part of such a code or scheme, though again, no schemes are currently available.
- The GDPR gives processors responsibilities and liabilities in their own right, and processors as well as controllers may now be liable to pay damages or be subject to fines or other penalties.

CySure

CySure Limited

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

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