GDPR Certification is coming...

By Lisa Rix - 31 July 2019

Want a certificate for all your hard work on GDPR?

Later this year "certification" will come into effect as a way for both controllers and processors to demonstrate compliance with GDPR. If a company can show compliance with a particular "certification scheme", then it will be issued with a certificate, seal or mark which the company can display to demonstrate its compliance.

How will certification work?

- "Certification schemes" will be established. Certification schemes will be a set of criteria or standards which companies can follow to demonstrate compliance with either a specific or general rule of GDPR (for example, on secure storage or personal data either generally or in specific locations/circumstances). Certification schemes will be created by companies putting forward suggestions to the Information Commissioner's Office ("ICO"), for approval and publishing.
- Those certification schemes will then be 'delivered' by accredited certification bodies. These bodies will have the powers to run certification schemes once a body has been approved by UKAS, the UK's national accreditation body, applying accreditation requirements issued by the ICO.
- Companies can then apply to an accrediting certification body for "certification" to show that they complies with a particular certification scheme.
- Certification is valid for a maximum of three years, subject to periodic reviews (certifications can be withdrawn if companies no longer meet the certification criteria).

Do I have to get certified?

No. Signing up to a certification scheme is voluntary. However, if there is an approved certification scheme that covers your processing activity, you may wish to consider working towards it, as:

1. it can help you demonstrate compliance to the ICO, the public, and your customers;
2. this may be an important part of public relations in your sector if your company works in IT security or handles a lot of special category

personal data; and
3. it will be considered as a mitigating factor if the ICO imposes a fine.

However, whilst certification will be considered as a mitigating factor when the ICO imposes a fine, non-compliance with a certification scheme could also be a reason for issuing a fine.

Does being certified mean that I am GDPR compliant?

Certification can help you demonstrate compliance with GDPR, but does not reduce your data protection responsibilities.

When is certification coming in?

- At this time, there are no approved certification schemes or accredited certification bodies for issuing GDPR certificates, as we are still awaiting the final publication of the European Data Protection Boards' ("EDPB") certification and accreditation guidelines and annexes, and the ICO is awaiting approval of its draft additional accreditation requirements from the EDPB.
- It is expected that by Autumn 2019, the ICO will issue the accreditation requirements for accrediting certification bodies and certification schemes will start being published. Businesses will then be able to decide whether to apply for certification.
- We will provide updates as we find out more...

