wiggin

Integrity and Confidentiality Principle

Today I'm going to be talking about the Integrity and Confidentiality Principle in GDPR, also known as the Security Principle.

While all principles are important, it is worth noting from the outset that this is the principle where the largest data protection fines have been issued as it's related to keeping data secure and preventing personal data breaches.

The wording of the Principle states that: "personal data shall be 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."

There are two things that require further discussion under this text: (i) what does appropriate mean? And (ii) what does organisational and technical measures mean?

Appropriate means that businesses should have a level of security that is 'appropriate' to the risks presented by its processing. The ICO states that a business should consider the state of the art and costs of implementation, as well as the nature, scope, context and purpose of your processing. Ultimately, the greater the sensitivity of the personal data being processed, the greater the security required will be.

Technical measures, as the name suggests, relate to your IT security, your hardware security, and the presence of proper data loss prevention software. In all likelihood, you will need to work closely with your IT or Tech department to understand the measures that are in place and whether they are satisfactory. These measures should also be stress-tested from time-to-time to identify any weaknesses.

Organisational measures relate more to policies issued to staff to help make them aware of phishing attacks, proper password protection and so on, as well as training. Appropriate access restrictions should also be in place.

As mentioned, the highest fines issued under data protection relate to the Security Principle and so it is important to understand exactly what measures are in place and whether these are appropriate or if they could be improved. It is also important to remember that if the worst happens and you do suffer a personal data breach, you will not automatically be fined if you are able to demonstrate that the measures you had in place were appropriate.