Data Protection

What is Data Protection?

The Data Protection Act came into force in 2018 and intends to:

- strengthen the data protection offered to individuals regarding their personal information. Personal information is defined as information that relates to an identified or identifiable individual e.g. this could be a name, IP address, etc.;
- standardise data privacy laws;
- empower all UK citizens when it comes to data privacy;
- change the way organisations approach data privacy.

The regulation applies to all organisations that offer goods and services or monitor the behaviour of UK citizens in any way.

Quickfire Guide

Quickfire Guide

Who Does GDPR Apply To?

Data protection applies to both controllers and processers of data.

A **controller of data** determines the purposes and means of processing personal data and has legal requirements under the regulations e.g. to maintain records of personal data and processing activities.

A **processor of data** is responsible for processing personal data on behalf of a controller and ensure processors comply with data protection requirements.

Data protection includes an accountability principle i.e. businesses must demonstrate compliance that includes any data processing supply chain the business might have. As a result, data protection is a matter for the entire organisation – not just for procurement.

Data protection sets out seven key principles for your approach to processing personal data:

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality (security);
- Accountability;

The Information Commissioner's Office (ICO) has issued specific guidance on GDPR and who is affected by it. You should refer to this guidance for more detailed information.

For contracts awarded after 25th May 2018

For contracts awarded after 25 May 2018, you should ensure:

- you undertake sufficient due diligence of your own suppliers to ensure they can implement the appropriate technical and organisational measures to comply with data protection i.e. provide guarantees of their ability to comply with the regulations;
- terms and conditions are updated;
- for relevant contracts i.e. which include data processing activities, apply the guidance at Annex B to all stages of the procurement and relevant documentation.

Please refer to the Scottish Government GDPR Policy Note for further information or to the buyer undertaking the tender process.