THE ICO'S ACCOUNTABILITY FRAMEWORK: HOW DO YOU FARE IN THE DATA PROTECTION COMPLIANCE CHECK-UP?

01 / 11 / 2021

In January this year I wrote a short blog about the accountability principle. In the blog I discussed the importance of this principle and the checklist produced by the ICO to assist data controllers when considering data protection risks. The ICO recommends that data controllers should visit the checklist on a regular basis.

The ICO has recently published an 'Accountability Framework' to assist data controllers in their compliance with the accountability principle.

What is it?

The ICO advises organisations to conduct regular data protection reviews of their data processing. The accountability framework provides an ideal platform for organisations to conduct a review using the framework's ten categories.

In the words of the ICO the framework will assist organisations in creating or improving their privacy management programme by checking existing practices against the ICO's expectations. It will help organisations to understand ways to demonstrate compliance and record and report on their progress. It will also help to increase senior management engagement and privacy awareness across an organisation.

The Framework is more detailed than the accountability checklist.

The regulator's expectations

The ICO explain the framework in some detail and also what their expectations are. ICO expectations are important because where organisations do not follow ICO guidance or ignore it their data protection risk is increased.

For example, when the ICO investigate a data security breach or poor data protection compliance they review the overall compliance of the organisation and consider the breach or non-compliance in terms of mitigating and aggravating factors.

Failure to comply with ICO guidance is considered an aggravating factor and often described by the ICO as the "intentional or negligent character of the infringement."

10 categories of compliance

The Accountability Framework covers a lot of ground. For example the ten categories are as follows:

1. Leadership and oversight.
2. Policies and procedures.
3. Training and awareness.
4. Individual's rights.
5. Transparency.
6. Records of processing and lawful basis.
7. Contracts and data sharing.
8. Risks and data protection impact assessments (DPIAs).
9. Records management and security.
10. Breach response and monitoring.

Categories in detail

The ICO explains each of the 10 categories in greater detail informing organisations about what they should consider. For example in the leadership and oversight category they suggest that organisations should consider:

- Organisational structure,
- Whether to appoint a DPO,
- Appropriate reporting,
- Operational roles,
- Group to provide oversight and direction,
- Operational group meetings.

In the Records of processing and lawful basis:

- Data mapping,
- Records of processing activities (ROPA),
- ROPA requirements,
- Good practice for ROPAs
- Documenting your lawful basis,
- Lawful basis transparency,
- Consent requirements,
- Reviewing consent,
- Risk based age checks and parental/guardian consent
- Legitimate interest Assessment (LIA).

In the Transparency category:

- Privacy notice content,
- Timely privacy information,
- Effective privacy information,
- Automated decision making and profiling,
- Staff awareness,
- Privacy Information review,
- Tools supporting transparency and control.

In the Breach response and monitoring category:

- Detecting, managing and recording incidents and breaches,

Privacy - Terms

- Assessing and reporting breaches,
- Notifying individuals,
- Reviewing and monitoring,
- External audit or compliance check,
- Internal audit programme,
- Performance and compliance information,
- Use of management information.

In the other six categories (Policies and procedures, Training and awareness, Individual rights, Records of processing and lawful basis, contracts and data sharing, risks and data protection impact assessments) there are a further 46 sub headings within those categories. In total there are 77 sub headings within the 10 categories.

Useful framework

Within each of the 77 sub headings there is a short explanation of what the ICO expects.

This is a much more comprehensive explanation by the regulator and emphasises the importance they attach to this principle. It is expected that data protection officers will be aware of the expectations and fashion their organisations compliance based on the requirements.

The ICO expects organisations to take note and act upon their guidance and codes of practice. The ICO also expects organisations to conduct regular data protection compliance reviews.

The 77 sub headings of the Accountability Framework provide the perfect opportunity for a compliance review.

This site uses cookies: Find out more. Accept