GDPR - ACCOUNTABILITY AND DOCUMENTING INFORMATION YOU HOLD

Under the new General Data Protection Regulation (GDPR) which comes into force on May 25th 2018 there are new provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance.

You are expected to put into place comprehensive but proportionate governance measures. You must be able to demonstrate compliance with the Regulation and compliance with the principle of accountability. Good practice tools that the ICO has championed for a long time such as privacy impact assessments (PIA) and privacy by design are now legally required in certain circumstances.

Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this means that we have to record all our processing activities where personal data is involved, these records will have to be produced to the ICO on request.

Within your organisation, and as part of the Information Governance Toolkit (IGT) compliance you already hold Data Flow Maps and an Information Asset Register. Previously you have reviewed these annually in line with the IGT, however to comply with the GDPR these need to be updated on an on-going basis and should always be up to date and accurate.

When a PIA is carried out at the start of a new project or process it includes questions around data flows and information assets and prompts the project to ensure that any new flows are mapped and that any new information assets are allocated an owner and added to the register.

These should then be reported on a regular basis to the IG Steering Group or equivalent and the SIRO. The SIRO will ultimately be responsible for ensuring compliance.

Remember: the ICO can request to see these records at any time and will be enabled to fine up to €20,000,000 for a breach in compliance

Actions that need to be taken:

- Ensure SIRO is aware of the new accountability provisions
- Brief Information Asset Owners (IAOs) emphasising the need for the register to be up to date and accurate at all times and that new assets must be reported to the IG Steering group (or equivalent) on a regular basis and to the SIRO
- Ensure IAOs understand their new responsibilities
- Allocate an IAO to be responsible for data flow mapping
- There should be a comprehensive and up to date list of all who contribute towards the data flow map
- Anyone listing a data flow should be made aware of their new responsibilities of ensuring that any new flows are added to the mapping and that these are reported to the IG Steering group (or equivalent) and the IAO