Accountability

The General Data Protection Regulation (GDPR) integrates accountability as a principle which requires that organisations put in place appropriate technical and organisational measures and be able to demonstrate what they did and its effectiveness when requested. Organisations, and not data protection authorities, must demonstrate that they are compliant with the law.

Such measures include:

Adequate documentation on what personal data is processed

How, to what purpose, and how long data will be processed for

Documented processes and procedures aimed at tackling data protection issues at an early state when building information systems or responding to a data breach

The presence of a Data Protection Officer (if required) who is integrated in the organisation planning and operations etc.

Make an inventory of all personal data you hold and examine it under the following headings:

- Why are you holding it?
- How did you obtain it?
- Why was it originally gathered?
- How long will you retain it?
- How secure is it, both in terms of encryption and accessibility?
- Do you ever share it with third parties and on what basis might you do so?

This is the **first step** towards compliance with the GDPR's accountability principle, which requires organisations to demonstrate (and, in most cases, document) the ways in which they comply with data protection principles when transacting business. The inventory will also enable organisations to amend incorrect data or track third-party disclosures in the future, which is something that they may be required to do.

ARC
Awareness raising campaign for SMEs

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

An Coimisiún um Chosaint Sonraí
Data Protection Commission