

Preparing for the General Data Protection Regulation (GDPR) – Steps to take now

Awareness - You should make sure that decision makers and key people in your branch are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

Information you hold - You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

Communicating privacy information - You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

Individuals' rights - You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

Subject access requests - You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

Lawful basis for processing personal data - You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

Consent - You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

Children - You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

Data breaches - You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Data Protection by Design and Data Protection Impact Assessments - You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

Data Protection Officers - You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your branch's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.