

# General Data Protection Regulation (GDPR) Preparation Checklist

The European Commission requires that European Union members must implement new General Data Protection Regulation (GDPR) privacy rules by 2018. The goals are to harmonise data protection law across the member states, and increase protection for citizens. This will impact any business (regardless of location) that is marketing to European Union member states.

Here's a checklist of steps (drawn from the United Kingdom's [Information Commissioner's Office](#)) you can take now to prepare.

- 1. Awareness.** Make sure that your executives and stakeholders understand what's changing and the effect it will have on your organization's operations and liabilities
- 2. Data.** Have a thorough plan to document and categorise the personal data you have, where it came from, and who you share it with. You will be required to be accountable.
- 3. Privacy notices.** Review your privacy notices and align them with new GDPR requirements.
- 4. Individuals' rights.** People have enhanced rights, such as the right to be forgotten, and new rights, such as data portability. Check your procedures, processes, and data formats to ensure you can meet the new terms.
- 5. Subject access requests.** You will have shorter timeframes to respond, and in most cases you will not be able to charge for access. Update your procedures to meet the new terms.
- 6. Legal basis for processing personal data.** You will need to document your legal basis for processing personal data, in your privacy notice and other places.
- 7. Consent.** Review how you obtain and record consent; you will be required to document it. It must be a positive indication; it cannot be inferred. Make sure you have an audit trail.
- 8. Children.** There will be new safeguards for children's data. Put systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.
- 9. Data breaches.** New breach notification rules and new fines will affect many organisations. Make sure you know how you will detect, report, and investigate personal data breaches.
- 10. Privacy by Design.** A privacy by design and data minimisation approach will become an express legal requirement. Plan now how you will meet the new terms.
- 11. Data Protection Officers.** Your organisation may need to designate a Data Protection Officer. Know who will take responsibility for compliance, and how their role will be positioned.
- 12. International.** If your organisation operates internationally, determine which data protection supervisory authority you come under. If you have multiple sites where decisions about data processing are made, this may be a complex answer.

[Read the European Commission's press release listing the benefits of the GDPR Protection Regulation](#)

In April 2016 the Council of the European Union published what may be the final text of the [General Data Protection Regulation](#).