BRODIES LLP

PREPARING FOR THE GDPR - **BASIC STEPS**

The General Data Protection Regulation comes into force on 25 May 2018. Whilst regulatory guidance begins to emerge, there are some basic steps that you can take to start preparing your organisation for the GDPR.

Our Top 5 recommendations

- Resource
- Data mapping
- Data minimisation
- Review processing justifications
- Contract reviews

Resource

Prepare your team and strategy for dealing with your GDPR project.

- Organisations should be thinking now about how they are going to resource privacy compliance:
  - Who will be in the project team?
  - Does it have the necessary budget and support from senior management?
- Specialist resource may be required – legal /compliance or IT functions may not have the required skills, bandwidth or cross-departmental reach.
- Data protection officers – identify whether you are required to appoint a DPO or whether it would be good practice to do so. DPOs are likely to be in high demand, which means that recruitment and retention will be a key issue.

Data mapping

Understand what data you hold and why.

- Your strategy for GDPR compliance should be based on a clear picture of the personal data that your organisation holds - for example, understanding where it comes from, what it is used for (and why) and where it goes.
- Construct a data map or register to:
  - assess compliance (or non-compliance) with current data protection law.
  - create a gap analysis between what is done now and GDPR.
  - prioritise key areas for action.
- Completing a data mapping exercise will take time and resource. Don't leave it too late.
- Remember, data mapping may provide the opportunity to fundamentally re-engineer data structures, which may in turn deliver greater efficiencies and reduce risk.

Data minimisation

Think about what you can do to reduce the amount of data that you collect and process – not just personal data, but data generally.

- Personal data collected should be:
  - limited to what is necessary for the purposes for which they are obtained (what the GDPR calls 'data minimisation').
  - kept for no longer than is necessary for the purposes for which they are retained (which the GDPR calls 'storage limitation').
- Compliance with the requirements for data minimisation and storage limitation will reduce the amount of data held, the costs of data storage and the administrative burden of complying with data subject rights and demonstrating GDPR compliance.
- In advance of the GDPR, organisations should review the data that they hold and cleanse their databases in line with the data minimisation principles and ensure that the data held is accurate.
- Understanding the concepts of data minimisation and storage limitation will help organisations adopt the GDPR's requirements for data protection by design and default.

Review processing justifications

Ensure that you have a lawful basis upon which to process personal data.

- Under GDPR, there are a number of areas where the justifications for processing personal data are tightened:
  - Consent – consent must be unambiguous, pre-ticked boxes are expressly prohibited and it must be as easy to withdraw consent as it is to give it in the first place.
  - Legitimate interests – when relying upon legitimate interests, data controllers must clearly set these out in their privacy notices.
  - Data relating to children - in particular in relation to online services, where age verification and parental consent will be required. Notices for services aimed at children must also be child-friendly.
- Public authorities will no longer be able to rely upon legitimate interests or (in most cases) consent as a basis for processing.
- Existing consents can only be relied upon if they comply with the requirements for consent under the GDPR. If the basis on which you've obtained consent will become invalid then you will need to devise a strategy to refresh that consent or find another justification for the processing.

Contract reviews

Consider what steps you need to take to ensure that your contracts are up to date.

- The GDPR imposes a number of specific requirements in relation to contracts between controllers and processors.
- Processing contracts that remain in effect after GDPR comes into force should comply with the requirements of the GDPR. Consider which contracts should be reviewed – for example, material data processing arrangements or data sharing arrangements with third parties and identify whether any amendments are required – either prior to GDPR or at the next break/renewal, depending on the risks identified.
- Adopting a good contract management solution such as Brodies' BOrganised - brodies.com/borganised - will be highly desirable.
- Contracts for the procurement of technology solutions which host, or are used, to process personal data will also need to be reviewed. New technology should be 'GDPR ready' and designed to simplify compliance with subject access requests and other data subject rights such as data portability.
- Develop new contractual styles based around the requirements of GDPR.

More information

You can follow the latest developments on the GDPR, including the latest guidance from regulators, on our GDPR microsite: **brodies.com/GDPR** or our blog: **http://techblog.brodies.com**

Key contacts

To discuss how the GDPR will impact on your organisation, or how Brodies can assist you with your preparations, please get in touch with a member of Brodies' data protection and information law team.

Grant Campbell
PARTNER
+44 (0)131 656 0115
grant.campbell@brodies.com

Martin Sloan
PARTNER
+44 (0)131 656 0132
martin.sloan@brodies.com

Christine O'Neill
PARTNER
+44 (0)131 656 0286
christine.oneill@brodies.com

Charles Livingstone
PARTNER
+44 (0)131 656 0273
charles.livingstone@brodies.com