BRODIES LLP

# WHAT DOES THE GDPR MEAN FOR...**PUBLIC AUTHORITIES?**

The General Data Protection Regulation comes into effect in mid-2018 and will introduce a number of substantive changes to data protection laws across Europe. The changes are likely to be supplemented by new rules in relation to electronic marketing and online tracking.

The GDPR will require all organisations to review how they collect, hold and process personal information and how they communicate with individuals. Organisations will need to adopt new measures and update their internal processes to demonstrate their compliance with the GDPR. The new rules will be backed up by enhanced enforcement powers.

## Changes include:

### Consent
There is a new requirement for 'clear affirmative action' and an end to pre-ticked boxes and bundled consents.

### Transparency
Organisations must provide much more information to individuals.

### Lawful Processing
There are stricter rules on processing data for new purposes.

### New access rights
Greater rights are given to individuals, including rights of erasure, protection against profiling, and a right of data portability.

### Privacy by design and default
Existing good practice recommendations must be hard-wired into day to day operations.

### Breach notifications
New express obligations to notify privacy regulators and affected individuals in the event of certain data privacy breaches.

### Accountability
Organisations will have to demonstrate compliance to regulators on an ongoing basis and maintain records.

### Sanctions
The power for regulators to issue fines for up to €20m or 4% of worldwide turnover, (including substantial fines for administrative breaches).

*We always get excellent service from them. They always understand what we're looking for, they communicate in plain English, stick to timelines and always deliver.*

Data Protection & Information Law, Chambers & Partners 2016

## How will this affect me?

Public authorities regularly handle personal data in relation to the delivery of public services. Such processing will frequently involve sensitive (or special category) personal data, to which even stricter rules apply. Public authorities also have all the responsibilities that private sector firms do: they are employers, they operate IT systems and engage in marketing. GDPR may have an impact on freedom of information laws.

GDPR changes the basis on which public authorities can process personal data for these functions. The UK Data Protection Bill proposes that an organisation will be a public authority under GDPR if it is a public authority under freedom of information laws. It is important that public authorities understand whether processing is being carried out in relation to tasks carried out in the public interest or in the exercise of official authority or for other purposes, as different rules apply. The Data Protection Bill clarifies that public authorities can rely upon the legitimate interests condition in certain circumstances.

## Specific issues:

- **Data collection** – do your privacy notices, client engagement and processes for collecting personal information meet the new rules on transparency and consent?
- **Status** – bodies that perform a quasi-public role or also carry out commercial activities will need to understand what their status is under the GDPR.
- **Legal basis** – public authorities will need to review their reliance on consent or legitimate interests and identify whether and the extent to which those legal bases can be relied upon going forward.
- **Data collection** – do you clearly explain to data subjects how their data will be used? How do you communicate your privacy notice when data is provided by a third party (eg another public authority)?
- **Policies and processes** – are your policies for handling and retaining personal data and data subject requests adequate?
- **Contracts** – if you use third parties to handle personal data on your behalf (for example providers of IT systems or marketing agencies), do your contracts comply with the requirements of GDPR?
- **Data sharing** – if personal information is shared with third parties, is that being done on a fair, lawful basis, bearing in mond that many public authorities currently rely on legitimate interests?
- **Freedom of information** – what impact will GDPR have on freedom of information requests?
- **Breach reporting** – do you have internal processes in place to deal with data breaches and ensure that they are reported to the ICO? Do your staff know what to do if they suspect a data breach has occurred?

## What do I need to be doing?

- Identify **your team** and **plan your strategy** for compliance.
- Create an **information asset register** – what personal information and where, why how and with whom do you process it.
- Review the **legal basis** for your data processing activities.
- Review your **data collection forms** and **privacy notices** to ensure they meet the new requirements.
- Review your **processes and systems** for dealing with data subjects rights, including new rights in relation to erasure of data and data portability and your use of profiling.
- Implement **data governance** policies and measures and **training** to ensure your organisation operates in accordance with the requirements of the GDPR.
- Review your **supply chain arrangements** with data processors.
- Ensure that new technology and systems are **GDPR ready**.

### More information

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

## Key contacts


**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