WHAT DOES THE GDPR MEAN FOR HR PROFESSIONALS?

BRODIES LLP

The General Data Protection Regualtion

An introduction

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 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.

> 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

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.

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

Organisations must build appropriate privacy requirements into day to day operations.

Breach notifications

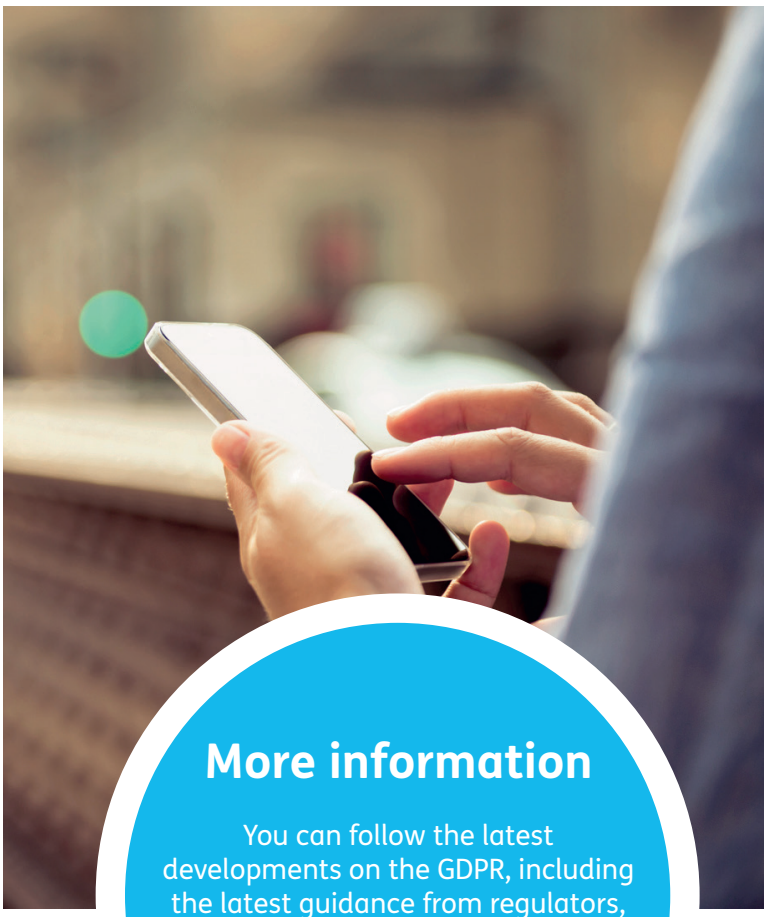
New express obligations to notify privacy regulators and affected individuals in the event of certain data privacy breaches.

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).



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:
techblog.brodies.com

How will this affect me?

HR departments process large amounts of personal data – not just in relation to employees, but also job applicants and former employees. That information may be held on systems within an organisation or processed by third parties, for example third party payroll processing and cloud hosted HR systems.

The information held will include special category personal data, such as medical information and trade union membership.

The requirement under GDPR to provide individuals with more information in relation to their data subject rights is likely to lead to increased awareness of those rights, such as the right to make a subject access request (DSAR).

At the same time, the rules on DSARs are being tightened up, with organisations given less time to respond.

Specific issues:

Recruitment

Do you provide applicants with an appropriate privacy notice explaining how their personal data will be used? Do you ensure that the personal data collected at each stage of the recruitment process is proportionate and necessary? Do you have clear arrangements with recruitment agencies?

Background checks

Are these proportionate and only carried out once a job offer has been made?

Legal basis for processing

Do you ask for consent when you have another legal basis for processing (eg the processing is necessary for you to comply with law or a duty on you as an employer)? Is your employee monitoring lawful?

Privacy notice

Do you carry out a privacy impact assessment prior to any new project?

Policies and processes

Have you reviewed your data policies and processes for handling personal data?

Privacy assessments

Do you carry out a privacy impact assessment prior to any new project?

Third party data processors

Have you reviewed your contracts with third parties to ensure that they comply with the requirements of GDPR?

Subject access requests

Do you have sufficient resource to deal with a likely increase in data subject access requests? Can you use technology to simplify findings and identify information that may be disclosable?

Data minimisation

The scope of a subject access request can be reduced by minimising the amount of personal data you hold. Do you have a records retention policy in place? Are HR personnel and line managers aware that records they retain may be disclosable?

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;
- identify your status under the GDPR;
- review your processes and systems for dealing with data subjects rights, as well as responses to FOI requests;
- 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; and
- ensure that new technology and systems are GDPR ready.

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

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:
techblog.brodies.com

BRODIES LLP

brodies.com