Brodies has a market leading data protection and information law team. Together we have produced this guide to highlight what the GDPR means for HR and what you should be doing now to prepare.

The General Data Protection Regulation comes into effect in May 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. Businesses 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.

**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).

### 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 (e.g., 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 provide employees with a clear and transparent privacy notice explaining how their personal data is used and explaining their rights as a data subject?
- **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 should I 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 your recruitment processes and template documentation.
- Review your employee privacy notices to ensure they meet the new requirements.
- Review your processes and systems for dealing with data subjects rights and monitoring employees.
- Implement data governance policies and measures and training to ensure your HR department operates in accordance with the requirements of the GDPR.
- Review your contracts with recruitment agencies and employment businesses.
- Review your supply chain arrangements with data processors, such as IT and outsourced service providers.
- Review the data you hold and your data retention policies and practices.

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

Information on data protection and the GDPR is also available on Workbox: [https://bresourcefull.brodies.com](https://bresourcefull.brodies.com)

Key contacts

Please get in touch if you would like to discuss how the GDPR will impact on your organisation; how Brodies can assist with your preparations; or to find out more about our information law team’s GDPR self-assessment tool.