GENERAL DATA PROTECTION REGULATION

HR professionals' guide - making sure you're ready

December 2017

The GDPR comes into force in May 2018. With less than six months to go, many organisations are well on the way to ensuring they are ready for the new regime. This guide is a handy reminder of the key issues for HR and gives you a checklist to help benchmark your progress towards GDPR HR compliance.

Key changes – a reminder

1 Consent

- → Employers will no longer be able to include general catch-all consent clauses in employment contracts.
- → Affirmative action will be needed: pre-ticked boxes or inactivity won't be valid consent.

2 Subject Access Requests

- → Employers must respond to requests within one month, with a possibility to extend this period for complex requests.
- → If a request is 'manifestly unfounded or excessive', you can charge a fee or refuse to respond, but you will need to be able to justify your decision.

3 Privacy Notices

- → Privacy notices need to be more detailed – employees must be given details including the purpose of processing, the legal justification for it and an explanation of their rights.
- → The information you provide must be concise, transparent, easily understandable and given in plain language.

4 Incident/breach response

- → Employers must notify the regulator of personal data breaches without undue delay, ideally within 72 hours – the notification must set out what happened, the number of individuals affected and the likely consequences and steps taken.
- → Employees must be notified if the breach poses a high risk to their rights and freedoms.

5 Penalties

- → Penalties for non-compliance will be more severe. The maximum fine for serious breaches is the greater of 4% of worldwide turnover or €20million. Smaller offences could result in fines of the greater of 2% of worldwide turnover or €10million.

BLP

What should you be doing now?

- **Data audit:** Gather information on what employee data you hold, where it came from and who you share it with. Ensure this is fed in to your company's wider GDPR audit.
- **Assess legal justifications:** For each of category data held, review the legal basis for processing data.
- **Incident response procedure:** Make sure there is a system in place for reporting breaches and for escalating where appropriate. Employees should have a clear procedure to follow in the event of a data breach. Make clear that data breaches by staff can result in disciplinary sanctions.
- **SAR preparation:** Update processes to take account of the more onerous changes to SAR response rules and ensure requests are handled within the new timeframes.
- **Update privacy notices:** Account for the additional information that will need to be provided to employees.
- **Consent:** Review how you seek consent to data processing and make any necessary changes to employment contracts and other employment documentation**.**
- **Training:** Give you staff practical training on the GDPR, so that they understand the impact on their day-to-day work.
- **Data Protection Officer:** If your company is involved in regular monitoring or large-scale processing of sensitive data, you will need to appoint a data protection officer.

Get in touch

Please don't hesitate to contact us if you would like to discuss anything covered or raised in this guidance note.

Rebecca Harding-Hill
Partner, Employment
T: +44 (0)20 3400 4104
rebecca.harding-hill@blplaw.com

Jackie Thomas
Senior Associate
Employment
T: +44 (0)20 3400 4776
jackie.thomas@blplaw.com

Rosie Kynman
Associate
Employment
T: +44 (0)20 3400 4080
rosie.kynman@blplaw.com