BDBF
EMPLOYMENT LAW

Monument Place, 24 Monument Street, London EC3R 8AJ +44 (0)20 3828 0350 www.bdbf.co.uk

Quick Tips for Preparing for the General Data Protection Regulation (GDPR)

1. **Don't Panic.** GDPR will come into force on 25th May 2018. It's a big change but it builds on the existing UK data protection regime. So, if you have the basics such as a data protection policy in place, then you will be building from solid foundations.

2. **But do take it seriously.** One of the major changes under GDPR is the potential consequences of non-compliance. Under GDPR, fines can be imposed up to the higher of €20 million or 4% of a company's global turnover. While the worst sanctions will be reserved for very serious breaches, the stakes are certainly higher.

3. **Get to grips with your data processing.** Your priority should be to assess in detail how you deal with employee data. Conduct an audit or "data-map" showing what kinds of data you have, what you do with it (including how you store it and when you delete it), how you protect it, how that data gets transferred between data systems, and where and to whom the data is sent.

4. **Identify your lawful basis for processing.** Once you have the 'how', you need the 'why'. You will need to identify which of the six legally permitted reasons (listed here) you are relying on for each type of employee data processing that you perform. The most likely justifications for employment data processing are:

    a. to comply with a contract

    b. to satisfy a legal obligation, or;

    c. for the purposes of the employer's legitimate interests (unless the potential harm to the employee overrides the interests in processing that data).

    In very limited and specific cases, you may be able to rely on employee consent. Good records should be kept of the lawful reasons identified for processing particular classes of data, as it is a requirement under GDPR that you are able to demonstrate (not just achieve) compliance.

> **" While the worst sanctions will be reserved for very serious non-compliance, the stakes are certainly higher. "**

5. **Be wary of relying on employee consent.** Under GDPR, obtaining an employee's consent will not normally be sufficient or appropriate to justify data processing. The regulatory authorities believe that, in an employment context, consent is unlikely to be genuine and freely given. You should not seek consent where another legitimate basis for processing applies (which will normally be the case). Where you do rely on consent, it should be "unbundled", so that employees can agree (or not) to specific activities individually, and they must be told of their right to withdraw consent at any time by a simple method. Employment contracts should be amended accordingly.

6. **Check for – and fix - other weaknesses.** A lawful basis for processing is a necessary pre-condition for processing, but is not enough by itself to comply with GDPR. There are other requirements about how data is processed, and you must check that you satisfy these. Take care also with the arrangements that you have with other parties who might process data on your behalf or fulfil contracts with you, e.g. payroll providers, insurance brokers, consultants and reference/background checkers. Transfers to countries outside the EU need special arrangements.

7. **Be transparent with employees.** Staff should be told clearly which data of theirs is being processed, in what ways, for how long, and for what reasons. The best means of doing that is to draft a GDPR-compliant data protection policy or privacy notice setting out all the details that employers are required to give their staff, and provide details of the 'responsible person' to whom they can address any queries. The policy should also set out what rights they have in relation to their data, including the right to withdraw consent and/or make a complaint to the Information Commissioner's Office.

8. **Consider appointing a data protection officer.** If you systematically process personal data on a large scale, you may be legally required to appoint an appropriately qualified data protection officer (DPO). If you are not obliged to appoint a DPO (and decide not to do so voluntarily), then you should still designate a manager who will have specific responsibility for ensuring the company's continued compliance with GDPR, without formally becoming DPO.

9. **Prepare for requests. Data subjects**, including employees, have a right to request what you do or do not do with their data, including making a Data Subject Access Request (DSAR). Essentially, this requires you to provide copies of all the personal data on them that you hold (with limited exceptions) within 30 days. DSARs are often used as a tool in an employment dispute. Meeting the deadline can be extremely challenging, and you will need to plan in advance how you will comply.

> **" Training on data protection should be offered to all staff. "**

10. **Offer training.** Training on data protection should be offered to all staff. There are a host of good reasons for offering this training, not least that it helps to satisfy the requirement that staff are kept in the loop on data protection issues. It also ensures that they understand how to deal appropriately with any personal data they may come across in their jobs and what to do in the event of a data breach.

At BDBF we provide expert employment law advice to the directors, HR advisers and in-house counsel of businesses. For strictly confidential legal advice and representation, please call us on +44 (0)20 3828 0350 or email us at info@bdbf.co.uk