Top tips for GDPR compliance.

Morrisons SOLICITORS

This advice note by Morrisons Solicitors' GDPR team will assist you in complying with the General Data Protection Regulation (GDPR) in force from 25 May 2018.

The GDPR updates the protection of individuals' personal data for the digital age and although an EU regulation, will remain in force in the UK irrespective of Brexit. It will be underpinned in the UK by a new Data Protection Act. All organisations will need to be up to speed with these new requirements and take practical steps to implement the changes.

Some key definitions

Controller determines the purpose and means of the processing of personal data and will have most obligations under GDPR. Businesses will be data controllers.

Processor processes personal data on behalf of the controller. GDPR imposes specific obligations on the processor for which they can liable. A business may process some personal data and may also have an agreement with a third party who will process other data on its behalf e.g. outsourced payroll or IT.

Information Commissioner's Office (ICO) is the UK data protection authority providing guidance on data protection on its website. The ICO will also be responsible for investigating complaints of GDPR non compliance and be able to take enforcement action for GDPR breaches. The **European Data Protection Board** will ensure EU GDPR consistency in interpretation and be involved in co-ordinated enforcement.

Personal data is 'any information relating to an identified or identifiable natural person' known as a **data subject**.

The fines for non- compliance with GDPR are hefty; up to 20 million Euros or 4% of global annual turnover. Here is our guidance on key issues you need to consider for GDPR compliance:

Decide whether you need a Data Protection Officer

Some businesses will voluntarily appoint a DPO or Data Protection Manager reporting to the Board to be the first point of contact for data protection matters and have the necessary expertise. S/he will monitor compliance with GDPR and assist the controller with implementation of effective policies.

You are required to have a Data Protection Officer where you are a public authority (except for courts acting in their judicial capacity), or carry out large scale systematic monitoring of individuals (e.g. online behaviour tracking) or large scale processing of special categories of data (e.g. health data) or data relating to criminal convictions or offences.

Review your personal data processing arrangements

Enlist key employees such as department heads, HR, marketing and finance to review and identify the categories of personal data you are processing in your business, where the personal data comes from, the purposes for which these categories are processed (and by who) and with whom you share personal data. Consider how long you need the data for those purposes and ensure it is retained for no longer than necessary. To ensure your procedures are kept up to date we recommend that you carry out a review of your personal data on a regular basis such as every 12 – 18 months.

Identify the lawful reason(s) for processing the data

Before processing data you must identify the correct legal basis for doing so and disclose this to the data subject. Otherwise, from 25 May you will be acting unlawfully. There are six legal grounds and the first four are most likely to be relevant in the employment context:

- **Performance of a contract:** processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. This is likely to be a common basis for employers. Examples include paying employees or providing them with benefits.
- **Compliance with a legal obligation:** processing is necessary for you to comply with UK or EU law (not including contractual obligations). You do not need to specify the particular law to the individual. An example will include giving salary details to HMRC.
- **Legitimate interests:** this is the most flexible basis for processing. It will be applicable where the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. An example would be fraud prevention.
- **Consent:** the individual has consented to you processing their personal data for a specific purpose. Use this as a last resort in the employment context. The ICO considers it will be difficult to obtain freely given genuine consent given the unequal relationship between employers and employees and of course it can be withdrawn at any time which could present practical difficulties for employers. There are strict rules for obtaining valid consent. An example of its use could be where you require one-off consent e.g. to provide an employee's salary details to a bank in support of their mortgage application.
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Processing 'special categories of data' is prohibited unless you identify the lawful basis as above *and* comply with one of the other ten additional conditions *and* have measures in place to protect the individual's rights. The special categories of data (similar to sensitive personal data under the Data Protection Act 1998) are data concerning a person's health, revealing their racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning a person's sex life or sexual orientation, or genetic data or biometric data for the purpose of uniquely identifying an individual such as facial recognition or fingerprints. There are separate and specific rules for processing criminal offence data and for children's personal data. If you are processing one or more special categories of data or criminal offence or children's personal data we suggest you take advice to ensure you are legally compliant.

Decide whether you need to carry out a Data Privacy Impact Assessment (DPIA) for any high risk changes in processing

A DPIA is a procedure to identify the impact of data processing activities on the protection of personal data. GDPR requires a Privacy Impact Assessment to be carried out prior to the processing where it is likely to result in a high risk to the rights and freedoms of the data subject, so that any DPIA recommendations can be incorporated in the processing. We advise that you undertake DPIAs for any existing such high risks that will continue after 25 May 2018. The DPIA must be documented and retained for the lifetime of the system or project.

Review and update your documentation and practices

Marketing emails: You will need to review to whom you are sending marketing emails to consider whether you can legitimately continue to send marketing emails to them – the consent obtained must have been of the standard required by GDPR. If you are not sure, you may need to write to the individuals in order to refresh consents if consent is the lawful basis for processing. Alternatively, you

may want to rely on the legitimate interests lawful basis. and the “soft opt in” which you *may* be able to rely on if you have always given individuals the choice of opting out in every message sent.

Going forward it will be vital to put in place mechanisms and wording which either obtains consent in compliance with the new GDPR standards or is in line with the requirements of the soft opt in. This can be done in a way that is appropriate for your business.

Privacy Notice: One of your highest priorities is to put in place or revise your Privacy Notice which notifies individuals about the personal data you propose to hold relating to them, how they can expect it to be used and for what purpose. We suggest that you have a separate Privacy Notice for your employees, workers and contractors; for job candidates and; for customers, suppliers, referrers and other parties. You need to give much more detail in a your GDPR compliant privacy notice than was required under the Data Protection Act 1998. Failure to include the required information for individuals external to your business will be very easy for the regulator, your competitors and most importantly the data subjects to see. Depending on your business requirements you may also need a separate policy dealing with your retention and erasure of personal data.

Data Protection Policy or Privacy Standard: To demonstrate your compliance with GDPR and comply with its provisions, as a minimum you will require a Data Protection Policy or Privacy Standard setting out the principles and conditions that your staff must satisfy when processing personal data in the course of its operations and activities, including customer, supplier and employee data. Your policy may also set out a procedure for notifying security breaches or you may prefer to have this dealt with separately to ensure staff are aware.

Contracts of employment and consultancy agreements: It is very likely that any data protection clause in these contracts by which the individual gives consent to your processing their personal data, is unlawful and will need to be updated.

Employment policies: Any other such policies referring to data protection will need to be updated. Following recent case law, employers can be vicariously liable for deliberate unauthorised breaches by their employees, even if the employer is not at fault. Accordingly it is very important that you minimise the risk of your employees breaching GDPR requirements by revising your disciplinary procedure to set out that breach of your Data Protection Policy could lead to disciplinary proceedings up to dismissal and may also be an offence under GDPR. You should also implement regular data protection training.

Contracts with third parties: You will need to have written agreements with certain specific clauses where necessary to comply with GDPR and to protect your business with third parties including: (i) those who are processing personal data on your behalf (ii) if your business is a data processor for its clients, and (iii) if your business is sharing personal data with other data controllers, for example, in some commercial collaborations.

Insurance cover: Given the potential size of the awards check your insurance cover. Some policies will offer access to technical providers at preferential rates.

How we can help you

We assist businesses using a step by step data protection review and assistance package which can be tailored to the needs, size and budget of your business.

If you would like our assistance ensuring your data protection practices, policies and procedures are GDPR compliant, contact J**oanne Kavanagh, Head of Employment** on the employment aspects at: joanne.kavanagh@morrlaw.com and for all other GDPR queries: **John Andrews, Head of Corporate and Commercial** at: john.andrews@morrlaw.com.