HR Made Simple Guidance for Managers

The General Data Protection Regulation – "GDPR"

Introduction

The General Data Protection Regulation (GDPR) is in effect from 25th May 2018. It is designed to ensure that data protection law keeps pace with changes in technology and further strengthens the rights of data subjects. Many of the concepts and principles are the same as the Data Protection Act (DPA) 1998, but there are new elements and significant enhancements.

Note: This guidance relates to how the GDPR affects employee data only. It does not cover customer data or marketing activities. Further guidance should be sought from legal or data protection specialists on processing this type of data.

Data protection principles

GDPR requires that personal data must be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

What to do to ensure compliance with the GDPR

1. Awareness and responsibility

It is important to ensure that decision makers and key people within the organisation are aware of the GDPR and its requirements. Organisations need to appoint a Data Protection Officer if they are:

- a public authority, or
- they carry out regular and systematic monitoring of individuals on a large scale, or
- they carry out the large-scale processing of special categories of data such as health records

If you do not need to appoint a Data Protection Officer, you still need to designate someone to take responsibility for data protection compliance within the organisation.

2. Carry out a data audit

This needs to include what data you hold, where it came from, who you share it with and how long you keep the data for. You will also need to establish and document your legal basis from processing the data. Under both the DPA and GDPR you must have a valid reason for processing personal data, and the reasons you can use are specified in the legislation. It is important that you get this right first time, as it can't be changed retrospectively if there's a problem. For employee data it will often be for the purposes of entering into an employment contract, but sometimes other bases may apply such as consent for sensitive medical information. The "lawful bases for processing" data are:

- **Consent:** the data subject has given clear, unambiguous, specific and explicit consent
- **Contract:** the processing is necessary for you to enter into a contract with an individual (including an employment contract)
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations)
- **Vital interests:** to protect someone's life
- **Public task:** the processing is necessary to perform a task in the public interest and has a clear basis in law
- **Legitimate interests:** 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

Special categories of data such as medical information or union membership (this was known as sensitive personal data under the DPA) need to have a "condition for processing" as well as a "lawful basis for processing". These are:

- **Consent:** the data subject has given explicit consent to the processing of those personal data for one or more specified purposes
- **Legal obligation:** processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law

- **Vital interests:** processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- **Legitimate interests:** processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- **Public data:** processing relates to personal data which are manifestly made public by the data subject
- **Legal claims:** processing is necessary for the establishment, exercise or defence of legal claims
- **Public interest:** processing is necessary for reasons of substantial public interest
- **Medical:** processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee or medical diagnosis
- **Public health:** processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health
- **Archiving and research:** processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

3. Communicate privacy information

Under the DPA you had to give people certain information when you collected their data, such as who you are and how you intend to use the information. Under the GDPR there are some additional things that you need to tell people. This is normally done through a "privacy notice", so existing notices will need to be updated and if you don't have one already you will need to create one. The privacy notice must include:

- Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer (if applicable)
- Purpose of the processing and the lawful basis for the processing
- The legitimate interests of the controller or third party, where applicable
- Any recipient or categories of recipients of the personal data
- Details of transfers to third country and safeguards
- Retention period or criteria used to determine the retention period
- The existence of each of data subject's rights
- The right to withdraw consent at any time, where relevant
- The right to lodge a complaint with a supervisory authority
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
- The existence of automated decision making (if applicable), including profiling and information about how decisions are made, the significance and the consequences

The privacy notice needs to go out when the information is collected, so a copy will need to go to all new employees and existing employees need to be sent a copy of the updated notice once it is created. Existing data protection policies will also need to be updated and communicated to employees.

4. Review processes for dealing with requests from candidates, employees and former employees - "data subjects"

Individuals' rights under the GDPR are broadly similar to their rights under DPA, but with some significant enhancements. Data subjects have the right to request that data is rectified if it is inaccurate, and if you have passed the data to a third party you also have to inform the third party of the rectification. They can also request that their data be erased, and requests for erasure can be refused in certain circumstances. There is a new right to data portability, but this is unlikely to apply to employee data, nor is the right to request not to be subject to automatic decision making, so this is not covered in detail in this guide.

As with the DPA, under the GDPR individuals have the right to access all the data you hold on them, including emails, texts etc, in which they are mentioned by name. The time limit for responding to such as request has been reduced from 40 days to one month. The ability to charge £10 for such a request has also been removed, although if a request is "manifestly unfounded or excessive" it may be refused or a reasonable charge for collating the information made. It is important that organisations have a process in place for responding to such requests within the time limits, and it may be useful whilst preparing for GDPR to make sure that information is held in one place to make handling such requests easier.

5. Review processes for obtaining consent

The way of obtaining consent from data subjects has been tightened up under the GDPR, and existing consent may not be valid under the new rules. For most types of employee data, consent is unlikely to be an appropriate basis for processing and, therefore, is not required. However, where consent is gained for data such as medical reports, consent forms will need to be reviewed to ensure that consent is freely given, specific, informed and unambiguous. Employers need to take particular

care when relying on consent, as an employer-employee relationship is not seen as an equal one and, therefore, the task of establishing that consent is freely given is likely to be more onerous.

6. **Review processes for preventing and handling data breaches**
The GDPR introduces significantly tougher financial penalties for breaches of the legislation, and tighter regulations on the reporting of data breaches. It is, therefore, another important step to introduce procedures on how to prevent and handle data breaches and ensure that these are understood by employees. If a data breach is likely to result in a risk to the rights and freedoms of individuals this is reportable to the ICO within 72 hours of the organisation becoming aware of the breach. Where there is high risk to those rights and freedoms, the organisation also has to directly contact the individuals concerned.

   A breach may be a successful hack of your internal systems but could also include the loss of a memory stick or documents, the theft of an unencrypted laptop or the sending of a confidential email to the wrong recipient. The requirements for data to be held securely have not been significantly altered by GDPR, this requirement was already in place under the DPA and measures must be taken by organisations to ensure the security of employee data. This means reviewing your IT system security, but also putting simple measures in place such as ensuring that all emailed files containing personal data are password protected and the password sent on a separate email and instructing employees not to leave documents or laptops in their cars overnight.

   The regulations make "data protection by design and default" an express legal requirement – this basically means you have to make sure you are taking all reasonable measures to keep data safe. If you have a data breach and it is found that an employee was holding, for example, an unprotected spreadsheet containing salary information on an unencrypted laptop using an unsecure internet connection, this would give an impression to the Information Commissioner that the business has not taken basic steps to ensure data security.

7. **Review processes for data minimisation and accuracy**
Check your process for the removal of data or create one if it doesn't exist. If your privacy notice states that, for example, all data relating to disciplinary records will be removed six months after an employee leaves your employment, then you will need to have processes in place to make sure this happens. This has the additional benefit of freeing up disk and file space. If your employee files are held by Kealey HR, we will inform you of our standard retention periods and remove leaver data in line with these. If you wish to retain any files for longer than our standard retention periods these will be returned to you.

   There is also a requirement to ensure that data is accurate. This is most effectively done by contacting employees to ask them to review their personal information and make sure it is still up to date. We would recommend this is carried out at least once every twelve months.

8. **Review contracts with third party providers**
The GDPR, like the DPA, applies to 'controllers' and 'processors' of personal data. Employers are the controllers of personal data relating to their employees, and they may pass this data on to processors such as their HR or payroll provider. Additional care will need to be taken and guidance sought if employee data is being transferred outside of the EU.

   Where you have suppliers who process employee data on your behalf, it is a requirement that a written contract is in place. **Contracts must include as a minimum the following terms, requiring the processor to:**
   - only act on the written instructions of the controller
   - ensure that people processing the data are subject to a duty of confidence
   - take appropriate measures to ensure the security of processing
   - only engage sub-processors with the prior consent of the controller and under a written contract
   - assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR
   - assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments
   - delete or return all personal data to the controller as requested at the end of the contract
   - submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their GDPR obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state

Further Information

The Information Commissioner's Office guide to the GDPR can be found at:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

If you have any questions about the content of this guide, please speak directly to your HR contact.