The Parks Medical Centre

May 2018

GDPR - The General Data Protection Regulation

The GDPR (General Data Protection Regulation) came into force on 25 May 2018. The regulation replaced the current Data Protection Act. Both employers and their employees have new responsibilities to consider to help ensure compliance. After Britain leaves the European Union, a new UK Data Protection Act will ensure that the GDPR principles remain in UK law.

Organisations must have a valid reason for having personal data and the data should not be held for any longer than necessary. The Information Commissioner's Office (ICO) has published an overview of the regulation and has a **checklist of 12 steps [PDF, 539kb]** that can help employers ensure they are GDPR compliant.

What is GDPR?

The GDPR (General Data Protection Regulation) is concerned with respecting the rights of individuals when processing their personal information. This can be achieved by being open and honest with employees about the use of information about them and by following good data handling procedures. The regulation is mandatory and all organisations that hold or process personal data must comply.

The regulation contains 6 principles.

- Personal data should be processed fairly, lawfully and in a transparent manner.
- Data should be obtained for specified and lawful purposes and not further processed in a manner that is incompatible with those purposes.
- The data should be adequate, relevant and not excessive.
- The data should be accurate and where necessary kept up to date.
- Data should not be kept for longer than necessary.
- Data should be kept secure.

All staff have a responsibility to ensure that their activities comply with the data protection principles. Line managers have responsibility for the type of personal data they collect and

how they use it. Staff should not disclose personal data outside the organisation's procedures, or use personal data held on others for their own purposes.

If companies and their staff are already complying with the Data Protection Act 1998 they will be well on their way to being compliant with the new regulation.

Who does GDPR apply to?

The GDPR applies to any organisation that handles personal data.

An individual who holds data about another individual on a personal level, for example a family members telephone number stored in a phone, will not need to consider GDPR for that particular data.

What is personal data?

Personal data is data that relates to an identified or identifiable individual and is:

- processed electronically
- kept in a filing system
- part of an accessible record, for example an education record
- held by a public authority.

This includes data that does not name an individual but could potentially identify them. For example a payroll or staff number. Employers should ensure staff are aware that any personal data they have in their possession will also be subject to the regulation. For example, if a manager has a written copy of contact details for their team or an employee keeps customer names and numbers on post it notes on their desk.

An organisation must have a lawful basis for handling any personal data. The **ICO has an interactive tool** to assist in identifying whether such a basis exists.

For further information, go to the **ICO website**.

Monitoring employees

If employers are monitoring their staff, for example to detect crime, they are required to make their workers aware of the nature and reason for the monitoring. This is applicable whether the monitoring is taking place using CCTV, accessing a worker's email or telephone calls or in any other way. For further information, go to the **ICO website**.

How long can information be kept?

Information must not be kept for longer than is necessary.

While there is no set period of time set out within the GDPR, some records must be kept for a certain period of time in accordance with other legislation. For example, HMRC require payroll **records to be kept for three years** from the end of the tax year that they relate to.

How can employers comply with the regulation?

To ensure its compliance to the GDPR, an organisation must:

- have a clear retention policy for handling personal data and ensure it is not held for longer than is necessary
- have a legal basis for acquiring and/or using any personal data (for more information on legal bases please see the **ICO website**)
- ensure that all staff are aware of the retention policy and follow it
- respond to subject access requests (sometimes called personal data requests) within one month
- if there is a personal data breach that is likely to result in a risk to the rights and freedom of an individual, inform the ICO within 72 hours and, if the risk is deemed to be high, also inform the individual concerned.

Some employers will also be required to appoint a Data Protection Officer who can help embed, communicate and monitor the organisation's GDPR data protection policy. For more information on Data Protection Officers and when one may be required, see the **ICO website**.

A worker's right to request their personal data

Workers have a right to access information that an employer may hold on them. This could include information regarding any grievances or disciplinary action, or information obtained through monitoring processes.

If a worker wants to see their personal data, they should speak to their employer. Most requests for personal data can be provided quickly and easily.

If the employer is unable or unwilling to agree to the request, a worker could make a **Subject Access Request**. A subject access request should be in writing and include:

- full name, address and contact details
- any information used by the organisation to identify the worker (account numbers, unique ID's etc.)
- details of the specific information required and any relevant dates.

Arrangements should already be in place to deal with Subject Access Requests as a 40 day time limit is currently stipulated under the Data Protection Act. This time limit shortens to one month under the GDPR.

While the Data Protection Regulation allowed an employer to charge a fee for Subject Access Requests, fees may only be required under GDPR if the requests are "manifestly unfounded or excessive".

If an employer refuses a request they must inform the individual within one month:

- why they have refused the request
- that the individual has the right to complain to the supervisory authority and to a judicial remedy.