Privacy and GDPR

Legal Speedread (Latest Update 16.5.17)

The GDPR applies to 'controllers' and 'processors'. The definitions are broadly the same as under the Data Protection Act (DPA) – i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf. The controller and processor may be the same legal entity or person. Processors maintain records of personal data and processing activities and have significantly more legal liability if they are responsible for a breach under the GDPR.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

Fair Processing

In order to process (use) information compliantly under the current Data Protection Act and the new GDPR data should be:

- used fairly and lawfully.
- used for limited, specifically stated purposes.
- used in a way that is adequate, relevant and not excessive.
- accurate.
- kept for no longer than is absolutely necessary.
- handled according to people's data protection rights.
- kept safe and secure.

You must have a legitimate and lawful reason for controlling and processing data. The conditions remain the same under the GDPR:

- The individual whom the personal data is about has **consented to the processing**.
- **The processing is necessary:**
  - **in relation to a contract which the individual has entered into; or**
  - **because the individual has asked for something to be done so they can enter into a contract**.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.

- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions
- The processing is in accordance with the "**legitimate interests**" pursued by the controller or third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. This cannot be relied on by public bodies.

Consent

Excerpt from the ICO's Overview of the GDPR:

"The GDPR has references to both 'consent' and 'explicit consent'. The difference between the two is not clear given that both forms of consent have to be freely given, specific, informed and an unambiguous indication of the individual's wishes.

Consent under the GDPR requires some form of clear affirmative action. Silence, pre-ticked boxes or inactivity does not constitute consent. Consent must be verifiable. This means that some form of record must be kept of how and when consent was given.

Individuals have a right to withdraw consent at any time.

Remember that you can rely on alternative legal bases to consent – for example, where processing is necessary for the purposes of your organisation's or a third party's legitimate interests."

If you are relying on implied consent to hold and process data currently, this will not be sufficient under the GDPR. You must obtain explicit consent, find an alternative legal basis or cease processing/holding the data.

The condition receiving the most attention from recruiters is legitimate business interest but there is a scarcity of precedent on how this can be used and has to be considered in light of an individual's right to know that there data is held and processed by you.

Individuals' Rights under the GDPR

Individuals have the right to:

- transparency of use of their data (to be kept informed)
- access their data – within a maximum of a month of request (a Subject Access Request)
- correct their data (you must also tell third parties if you have disclosed inaccurate data to them)
- have their data deleted where there is no "compelling" reason to process it (the right to be forgotten)
- block or suppress processing of their data
- obtain and reuse their personal data across different services – to obtain a copy or their data in a commonly used format (data portability)
- object to processing based on "legitimate interests" or direct marketing (including profiling) – see basis for processing below

Note the law has already changed in this area as ECJ decisions provide individuals with enhanced rights to be forgotten. For example, this has altered Google's approach to delivering search results.

Data Protection Officer

Duties:
To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

The DPO must report to your board and must operate independently.

A DPO does not need specific qualifications, however they will certainly be in a better position to undertake the role if they attend external training courses or have data protection accreditation.