Data protection and GDPR

Companies have been required to comply with the data protection legislation for some time. Currently the Data Protection Act 1998 sets out what is required. The UK is required to implement the EU General Data Protection Regulations and from 25 May 2018 there will be new legislation and rules that will need to be followed.

All organisations have different needs for data. The impact of GDPR will therefore be dependent upon your use of data. Your organisation, if it is a Data Controller, should already be registered with the Information Commissioner's Office (ICO). Within this registration you will have already identified the categories of data you hold and for what purposes the data is used. This should be reviewed as a first step.

For RBA client's we will mostly be concerned with how data is used in relation to employment. If you use financial data, credit information, housing information, or you market through the collection of analytics, you may need to seek separate specialist advice in those specific areas. How you secure electronic data is another topic that is generating much current discussion in the light of GDPR but outside the scope of this document.

The general advice at this stage is for organisations to carry out an impact assessment in advance of May 2018 in order to consider:

- the existing use of data
- the policies in regard to data use and controls
- how data is stored and secured and how long it is retained for
- whether in the light of the new regulations changes need to be made.

The DPA and the EU directive give individuals rights concerning the processing of personal data. The DPA applies to personal data in a computerised format as part of an accessible record or held manually as part of the relevant filing system. Employers are therefore a data controller as all employers need to gather and process data in relation to their employees.

In simple terms data protection law means that those who decide how and why personal data is used must comply with certain principles. The eight DPA principles to specify that data must be:

1. fairly and lawfully processed,
2. processed for limited purposes,
3. adequate, relevant and not excessive,
4. accurate,
5. not kept for longer than is necessary,
6. processed in line with an individual's rights,

7. secure,
8. not transferred to countries outside the European economic area (EEA) without adequate protection.

The Information Commissioner is the enforcing body and can issue "undertakings", enforcement notices, and civil penalties potentially up to £500,000 for a breach of one or more of the principles.

Specific guidance for employers is available from the IOC Office. There are codes of practice in relation to:
1) recruitment and selection
2) employment records
3) monitoring at work
4) information about workers health

A review of current practices would do well to take note of the relevant codes for employers set out on the ICO web site at https://ico.org.uk/for-organisations/

So what are the main changes in the new regulations?

The new regulations are designed to address developments in the use of data over recent years and to counterbalance some of the abuses of data usage. There have been a number of high-profile cases where organisations such as Uber failed to prevent millions of users' data been retrieved from their systems. Marketing data has been sold and passed between suppliers and increasing use of web-based analytics has led to a European-wide fresh look at whether individuals are protected.

There many different areas to the data protection regulations. In August 2017 the Information Commissioner issued updated guidance on preparing for GDP in the document "12 steps to GDPR compliance". (https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf)

The 12 steps are:

1) **Awareness:** start preparing before May 2018
2) **Information you hold:** GDPR requires organisations to maintain records of processing activities and the legal basis for doing so. This should include how long records are retained for.
3) **Communicating privacy information**: review privacy notices
4) **Individual rights**: and the right to be informed, right of access, rights of rectification, right to erasure, right to restrict processing, rights to data portability, right to object, and right not to be subjected to automated decision-making and profiling.
5) **Subject access requests**: have a policy and procedure to respond to a request within the new one-month deadline.
6) **Lawful basis for processing personal data:** organisations must review the legal basis used for processing personal data to ensure this is still relevant and within the GDPR compliance.

7) **Consent:** where consent is relied upon ensure that it is freely given and not abused or used for other purposes
8) **Children**: under the new regulations children's data is specifically protected for the first time.
9) **Data breaches**: there will be a duty for organisations to report a data breach, specific rules apply, and these include in some cases informing individuals about the breach.
10) **Data protection by design and data protection impact assessments**: where the processing of data is likely to result in a high risk to individuals, rolling out a new technology, large-scale data processing or some form of automated profiling.
11) **Data protection officers (DPO's):** organisations should evaluate whether they require to appoint a DPO under the GDP.
12) **International:** operating in more than one geographical area it is suggested that there is a European lead. Considerations will also have to be given as before to the transfer of data outside the EEA.

For employers, preparing to address the new legislation will likely start with a review of your exiting policy, if you have one, and then considering who in your organisation should be taking the lead. This may take you to the 11th step, the appointment of a Data Protection Officer and whether or not this role is already in place. An outline DPA policy, together with the role of the DPO is available for clients looking to review this area.

Consent

The new regulations consider the issue of "consent". Is an individual freely giving of their consent for data to be used? What are they consenting to and how do they know how the data will be used?

Many employers will have a clause within their employment contracts that states that the employee is agreeing to the processing of data by entering into the employment contract. In future, such a clause is likely not to be considered as free consent as the employee has little option but to sign acceptance for work. This is similar to the old practice of gaining consent to opt out of the Working Time Regulations by excepting an employment contract, such a clause no longer to be taken as a valid opt out.

In the case of working time, a separate signed consent is now obtained. However, consent is only one way that data can be lawfully obtained and processed. Consent is generally not the basis for processing data within the employment relationship, the data is needed by the employer and necessary for the employment relationship.

The employer can process data where it is needed:

- for the performance of the employment contract
- to comply with legal obligations
- to protect the vital interests of the employee or any other natural person (including the employee's dependents or family) and/or

- because of the legitimate interests of the company (provided that such processing is proportionate to the interests and fundamental rights and freedoms of the employee or data subject)

In some areas there are overriding reasons were an employer will be expressly permitted to hold and process data, such as in relation to the payment of HMRC, the retention of accident information, insurance claims, legal proceedings and immigration status etc. In other areas such as obtaining a medical report the employer will have to follow specific processes in order to obtain and process "personal sensitive data".

Monitoring and investigation - Proportionate Means
Therefore, the vast majority of data in the employment relationship is included within the headings above. However, the key lies within the phrase "providing that such processing is proportionate". For employers, much of the justification for the use of data will hinge on the employer being able to show that their use of data was a "proportionate means" of achieving a legitimate end.

An employer may need to specifically evidence this, e.g. who in the organisation sanctioned the search through an employee's email account? What was the search instruction? What was the legitimate purpose? What steps were taken to ensure the search was not excessive or overly intrusive etc?

Within the employment context, typically data is only problematic where it is identified within a disciplinary or grievance context. Often this falls within emails, telephone recordings, CCTV surveillance or private investigations. All of the above are unlikely to be areas where the employee will be freely giving of their consent!

The employer will of necessity need to obtain and use this information, but care will need to be taken in how this is done and what purpose the data is used for. Good policies on the use of computer equipment, email and social media are important in support or the employer's aims and showing fairness, objectivity and proportionality along the way. Again, for clients, suggested wording is available for use within the employee handbook.

Subject Access Requests.
Employers are often faced with requests by employees to see their "personal file". This request is a "Subject Access Request" has been around for some time. The employer was able to charge £10 for the request, however under the new regulations the request can be made free of any charge. Whereas previously a request had to be provided within 40 days, future requests will have to be supplied within reasonable time and no more than one month from the date of request.

Retention of records
Data should only be held for as long as necessary. It is suggested that some thought is given to when data is cleansed from the system or archived into an anonymised form.

Recruitment data may have a shelf life of perhaps 6 months, HMRC and accounting data is usually kept for the last six years. Some health records and documents from legal claims and

settlements may need to be held for many more years. The rationale however should be considered and documented.
As guide http://www.robbryanassociates.org.uk/wp-content/uploads/2017/12/Retention-of-records-table.pdf may assist you.

Links:

ICO website for organisations: https://ico.org.uk/for-organisations/
ICO '12 steps' guidance: https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf
RBA sample data protection policy: http://www.robbryanassociates.org.uk/wp-content/uploads/2017/12/Data-Protection-Policy.docx
Retention of records guidance: http://www.robbryanassociates.org.uk/wp-content/uploads/2017/12/Retention-of-HR-records.pdf