Putting the R(etention) in GDPR

By Deborah Margolis - 28 February 2018

As the General Data Protection Regulation ('**GDPR**') fast-approaches (we are now under three months away!) many HR departments will be looking at their current processes to assess whether they will meet the requirements of GDPR after 25 May 2018, when GDPR comes into force.

Why are we even talking about retention of records?

At face value, the existing data protection principle under the Data Protection Act 1998 ('**DPA**') that data "*should not be kept for any longer than is necessary*" has been translated into GDPR. However, the question of retention of HR records has come to greater prominence for three reasons:

- The maximum penalties for non-compliance under GDPR will be €20 million or 4% of worldwide annual turnover, whichever is higher. By way of comparison, under the DPA, the maximum penalties are £500,000. As a result, data protection has become much more of a prominent issue for businesses and HR departments are taking the opportunity in the run up to GDPR to review their current practices.
- Under GDPR, privacy notices require data controllers (for our purposes, employers) to tell data subjects (their employees) how long their data will be kept for, or if that isn't possible the criteria which will be used to determine that period. This therefore means that timeframes for retention need to be addressed properly, whereas, under the Data Protection Act, there was less of a focus on specific retention periods and making data subjects aware of these.
- The new Data Protection Bill (as currently drafted, but not yet passed at the time of writing) will require employers that process sensitive personal data (this is likely to cover most employers) to put in place a retention policy to set out for how long this sensitive personal data will be retained.

Thinking about retention periods

Our top tips to employers who are thinking about retention periods is as follows:

- **Break it down**: divide up the data you hold on employees (and prospective employees) into smaller categories of data, for example, recruitment, performance information/appraisals, pay, contact details, next of kin, maternity/paternity documentation etc.
- **Don't forget the statutory retention periods**: don't get carried away with over-zealous retention periods! The statutory retention periods set out the mandatory minimum periods for which certain categories of data *must* be held. For example, maternity records must be kept for at least three years after the end of the tax year in which the maternity pay period ended.
- **Consider how long you need to retain data:** for example, think about your business or any regulatory requirements. Do you have any internal reporting requirements for which you will need to retain certain information?
- **Think about the more sensitive categories of information**: there are some categories (for example criminal record checks on recruitment) for which, depending on the nature of your business, you may not need to keep the record itself, and only the fact that a satisfactory background check has been completed.
- **Don't forget about unsuccessful candidates**: it is best practice not to retain information relating to unsuccessful candidates. The Information Commissioner's Office recommends that if you do intend to keep details of unsuccessful candidates that they should be made aware of this and given the opportunity to have their details removed.
- **Document everything**: ensure that your decision making is well documented and you have an policy to record your retention periods and internal processes for ensuring that the policy is implemented.
- **Training and implementation**: put staff training in place in order to ensure that the retention policy is adhered to.

If you have any questions surrounding the implementation of GDPR please get in touch with your normal GQ contact.