

DATA PROTECTION/DATA DISCLOSURE NEW EU REGULATIONS – THE GDPR

It was being reported at the beginning of April that companies had abandoned plans to comply with the EU General Data Protection Regulation because of Brexit. Apparently, a significant proportion of UK companies believe that the GDPR will not apply to the UK outside of the EU. Unfortunately, they are wrong and the GDPR will be preserved by the Great Repeal bill. On the bright side, there are still 12 months left before May 2018 to prepare...

The GDPR is of course particularly significant in relation to HR because of the volume of personal data on employees which is processed by employers.

The headlines of the **GDPR** include:

- a significant increase in the possible level of fines for breach;
- a right to data portability;
- a right to have one's data erased;
- requirements to notify data breaches to the information commissioner and to data subjects;
- privacy impact assessments;
- data protection officers.

However, some of the more mundane requirements may require the most work for HR.

To highlight a few:

- the GDPR is generally more input-based than output-based – this means that there will be an increased focus on the documentation of data privacy policies and procedures;
- information notices will need to be reviewed against the requirements of the GDPR. A compliant notice will require significantly more information to be provided than is normal practice, such as details of the basis upon which data is processed, retention periods, data subject rights, the right to complain to the information commissioner and information on international transfers (including access to relevant agreements);
- reliance on consent will need to be reviewed and in most cases abandoned. The issue is not new but there is renewed focus on the imbalance of power between employer and employee. Consent will only be appropriate where the data subject has a genuine choice, and processing can stop without them suffering a detriment. The difficulty in maintaining reliance on consent will be what is done when consent is withdrawn and knock-on effects, such as the ability to require erasure where processing is based on one's consent and such consent is withdrawn.

The right of access to personal data is often an issue for employers and frequently used by employees as a means of gaining early disclosure in litigation or simply putting the employer to work. The basic right remains the same but some things will change, and probably not for the better:

- the default time period reduces to one month;
- we lose the provision allowing data controllers to ask for location information in order to find the personal data which the data subject is looking for;
- instead, push back will need to be on the basis of the proportionality of EU derived legislation, or a new provision allowing for more time to answer and/or refusal where a request is manifestly unfounded (although interpretation of that phrase by the information commissioner or the courts will need to be awaited).

The advice, for now, is to accept that GDPR is not a problem for which Brexit is the solution, and take advantage of the next 12 months to start bringing compliance up to standard.

Philip Bartlett

Partner, Simmons & Simmons LLP
philip.bartlett@simmons-simmons.com