12 months since GDPR - what do employers really need to know?

By Deborah Margolis - 31 May 2019

As we sip champagne reflecting on the first anniversary of GDPR, we consider the key obligations that employers need to be aware of. In our recent webinar we looked at what employers really need to know and a couple of key practical issues for employers including responding to Data Subject Access Requests and dealing with data breaches. You will find a link to the recording of our webinar here.

In this article we have set out the four key steps that employers need to take on the road towards GDPR compliance:

1. Audit and analyse your data

Work out what data you process as a business and focus on the more unusual data, for example CCTV or fingerprint access. Employers should then consider the legal basis for which they process it. One of the key points for employers was a shift away from consent (which is generally not appropriate in the employment context) to other legal bases for processing.

2.Updating documentation

This is the main area of compliance we saw employers working on in the run up to GDPR:

- Privacy notices – employers need to put in place specific privacy notices for employees (and clients, if appropriate) to tell them what they're doing with their data.
- Employment contracts – employers will need to update their contracts for new employees. Some employers that process a large amount of personal data might want to consider adding data protection obligations into their contracts.
- Policies – employers that process "special" categories of personal data, (i.e. health, race or religion) will need to have a policy document in place to explain what data they process of this nature, how they intend to comply with GDPR and how long they will keep this data for. Employers may also want to put data protection/security policies in place to set out how their employees must comply with their data protection obligations.

3. Assessed and addressed risks

After all of the hype in the run up to GDPR, it can be easy to forget that GDPR is an ongoing obligation and not a one-time exercise.

Employers can work on assessing ongoing risks by taking the following steps:

- Privacy Impact Assessments – employers should conduct risk assessments before doing anything high risk or unusual. Employers should really be focused on anything they do that is out of the ordinary, for example automatic decision making during the recruitment process or CCTV in the workplace.
- Criminal records checks – these are less clear cut under GDPR than under the old law, but if you process employee criminal records you should think about the reason you are carrying them out and the risks involved in doing so.
- Security – security is another key focus under GDPR, but this isn't something new although there has been a renewed focus on it under GDPR because of the higher fines. Employers should be thinking about password protection and encryption and IT security, for example when transmitting personal data.
- Data breaches – employers should spend time thinking about data breaches and how they would deal with them if they ever occur. (We discuss this in more detail on the webinar).

4. Demonstrating compliance

Once you've put all of the work into complying with GDPR, it's worth documenting what you've done and ensuring ongoing compliance, for example:

- Data Protection Officer – some organisations will need to appoint a Data Protection Officer, to act as the businesses' figurehead for GDPR compliance both internally and externally.
- Pay a fee – employers will need to pay a fee to the Information Commissioner's Office depending on the organisation's size and turnover.
- Cross border issues – international businesses will need to put some thought into cross-border issues, for example how they transfer data in and out of the EU and documenting those flows.
- Keeping records – businesses will need to maintain a record of all of their processing activities (which would hopefully be a straightforward task if you've conducted the analysis at point 1 above).

For more information about what employers really need to know about GDPR please listen to a recording of our webinar here. For more assistance on your data protection compliance project, get in touch with your normal GQ|Littler contact.