How Brexit will affect your data protection efforts

By Lisa Rix - 28 March 2018

With Brexit due to take place in either just over two weeks (if the proposed deal is rejected) or just under a month (if the deal is approved), there is uncertainty over a whole host of issues. But one issue employers have been grappling with is the impact of Brexit on data protection laws, so we thought we would try to clear that up in this short blog post.

Generally, the General Data Protection Regulation (GDPR), which came into force in the UK on 25 May 2018, is going to be absorbed into UK law at the point the UK exits the EU. This absorption will require some technical changes so the rules work, but the intention is that there will be no immediate substantive change to the rules that most UK organisations need to follow. This could change in the future, given that the UK will be free to determine its own data protection laws as it pleases, but this is unlikely to happen any time soon. This is good news for all of those UK employers who have spent a lot of time and effort to comply with GDPR: it certainly was not a waste.

The main change for employers in the UK, upon exit, is that the UK will become a "third country" for the purposes of GDPR. Significantly this means that the rules about safeguarding data sent outside of the EEA will now apply to the UK. The UK Government has confirmed that UK businesses will continue to be able to send personal data from the UK to the EU freely after Brexit as the UK will recognise EEA states (and any other countries with an EU adequacy decision) as providing an adequate level of protection for personal data. However, the position is different for EU states sending data to the UK:

- In a "Deal" scenario, during the transition period GDPR will continue to apply in full. The EU will assess the UK for an "adequacy decision" as soon as possible after the exit in May 2019 and will try to put that adequacy decision in place by the end of the transition period (which would allow the continued free flow of personal data from the EU to the UK after that point in time).
- In a "No Deal" scenario, the UK will almost certainly not receive an adequacy decision by the point of exit in April 2019, so companies transferring personal data from the EU to the UK will likely need to rely on standard contractual clauses (SCCs) or binding corporate rules (BCRs). Companies may need to put in place these SCCs or BCRs to receive data from the EU and any existing BCRs will likely need updating to ensure the UK is considered a third country and to change their lead authority if needed. In the future, the UK and the EU will both need to approve BCRs.

The ICO has also issued a lot of helpful guidance on other steps which companies should take in relation to data protection if there is no deal, for example around lead supervisory authorities, EU and UK representatives, data breach reporting and updating privacy documentation, etc. Many of these steps are not employment-specific but will apply to all companies.