No Deal Brexit – the impact on GDPR

There has been much speculation in the media about the difficulties that importers and exporters will face if there is a No Deal Brexit. The flow of personal data between the UK and the other members of the EU has received much less coverage.

A back up of emails and attachments has much less dramatic impact than the prospect of lorry parks on the M27, but the question of the lawful transfer of data is an issue that must be addressed. It appears that it will be relatively straightforward for the transfer of data from the UK but there will be complications in transfers from the EEA to the UK.

Anyone who hopes that Brexit will result in a significant change to the UK's data protection laws, at least in the medium term, is likely to be disappointed. The European Union (Withdrawal) Act 2018 will have the effect of putting the General Data Protection Regulations onto the UK statute book on the day that the UK leaves the EU. GDPR will still apply to all data processing within the UK as well as the UK domestic legislation.

At present data may lawfully be transferred to any other country within the European Economic Area: the current EU member states, Norway, Liechtenstein and Iceland. Any other country is regarded as a "third country" and data may be transferred to it only if:

- The European Commission has made an adequacy decision: in effect, if the EC has approved the country's data protection regime.
- The two parties have adopted a set of binding corporate rules approved by the "lead authority". The lead authority depends upon the situation of the part of the company best able to deal with data protection compliance. The approval of binding corporate rules can be a lengthy process and in practice, only large multi nationals that regularly need to share data are likely to consider binding corporate rules.
- The two parties use the standard contract clauses published by the Commission in their documentation to provide data protection safeguards.
- One of the exceptions or derogations set out in Article 49 of GDPR applies.

Tel: 0344 967 0793 | Email: info@LA-Law.com | www.lesteraldridge.com

Transfers from the UK

Transfers from the UK to EEA member countries will be permitted under the UK version of GDPR and are the most straightforward issue in a post Brexit world. In addition, the UK government has stated that it will recognise declarations of adequacy in relation to other countries made by the EC prior to the exit date. It appears that in due course the list of "adequate" countries may diverge if the UK chooses to recognise other countries as "adequate"; trade deals are likely to be easier where there is a declaration of adequacy.

The use of standard contractual clauses is likely to remain the best way to authorise the transfer of data to a country that is not deemed adequate. The UK government will recognise the standard contractual clauses approved by the European Commission.

The UK will recognise binding corporate rules authorised before Brexit even if the lead authority is in an EU state. It is not clear however whether the Commission will recognise binding corporate rules authorised by the ICO in the UK.

Transfer to the UK from the EEA

On Brexit, the UK will become a third country. It will not automatically be covered by an adequacy decision despite its data protection regime being based upon GDPR. The Commission will have to consider whether to make an adequacy decision and some estimates are that it will take at least 18 months.

In the meantime, transfers from a data controller in the EEA to a data controller in the UK will have to be authorised by one of the safeguards set out in the GDPR. In practice, this is likely to mean the widespread use of the standard contractual clauses. Businesses should start to look at any contracts or arrangements that require the exchange of data with counterparts in the EEA and review the documentation to be ready to amend it by the inclusion of the standard contractual clauses.

It will still of course be possible to use one of the derogations. The derogations are quite limited and must be interpreted restrictively. It is clear that they can be used only for occasional and limited transfers. The derogations may be summarised as:

- The explicit consent of the data subject, after having been warned about the dangers of a transfer to a country without an adequacy decision or appropriate safeguards.
- The transfer is necessary for the performance of a contract with the data subject or to take pre-contract steps at the request of the data subject.
- The transfer is necessary for important reasons of public interest.

Tel: 0344 967 0793 | Email: info@LA-Law.com | www.lesteraldridge.com

- The transfer is necessary in connection with legal claims
- The transfer is necessary in the vital interests of a data subject who is unable to give his or her consent.
- The transfer is from a public register.

If none of the derogations apply, there is a further exception where there are compelling legitimate interests on the part of the data controller. The data controller must carry out an assessment of the risks and the transfer must be reported to the ICO: in short, it is clear that it must be a truly exceptional situation.

Parallel Worlds/Nightmares?

As if the data protection regime does not have enough complexities, Brexit raises the possibility of dual jurisdiction. Article 3(2) of GDPR provides that GDPR applies to the processing of the personal data of data subjects who are in the EU by a controller outside the EU – e.g. in the UK. If a UK company processes data about data subjects in the EU, it will have to comply with both UK and EU law.

It remains to be seen how far the two regimes will diverge over time. In the meantime, the ICO will cease to be a supervisory authority for the purposes of GDPR although it will remain the supervisory authority for UK based data controllers. Organisations operating in multiple jurisdictions across the EU have previously been able to opt for a supervisory authority in one jurisdiction. It appears that after Brexit, organisations operating in the UK and in EU will have to register with the ICO and with its counterpart in another EU jurisdiction.

Article 27 of GDPR requires a data controller based outside the EU who processes personal data in relation to the sale of goods or services to data subjects in the EU must appoint a representative in one of the Member States where the goods or services are sold. UK businesses selling into the EU will have to comply with this requirement after Brexit. The UK government intends to mirror Article 27 and require EU businesses similarly to appoint a representative in the UK.

The UK government is apparently seeking close co-operation between the ICO and the EU data protection authorities but in the absence of any legal instrument, it is difficult to see how the enforcement powers of the ICO and its EU counterparts will be co-ordinated.

And finally – this article was written on Tuesday 3rd September. Between starting to write it and completing it, the government lost its majority. By the time it is published, it may be well and truly out of date!

Tel: 0344 967 0793 | Email: info@LA-Law.com | www.lesteraldridge.com