ICO Updated Brexit Data Protection Guidance & Resources

Date : January 31, 2020

Introduction

The UK is now leaving the EU, to be followed by a transition period until the end of December 2020 (i.e. with a deal for that period of time). The UK's Information Commissioner's Office (ICO) has provided an update about what this means in terms of data protection and related issues, which can be found here: https://ico.org.uk/for-organisations/data-protection-and-brexit/

What's the main issue?

During the transition period it will for the most part be business as usual for data protection but at this stage it is impossible to say what the data protection landscape will look like at the end of the transition period. Organisations will need to plan ahead and start preparing in order to be ready for the changes to come.

What are the particular issues?

The ICO has set out what it sees as the main issues in a set of FAQs. Aspects of particular note are as follows:

- **What happens at the end of the transition period?** Whilst this will depend on the negotiations during the transition period '[t]he default position is the same as for a no-deal Brexit: the GDPR will be brought into UK law as the 'UK GDPR', but there may be time for further developments about how we deal with particular issues such as UK-EU transfers';
- **Do we need a European representative during the transition period?** 'No, during the transition period you do not need to appoint a representative in the EEA. However, you may need to appoint a representative from the end of the transition period if you are offering goods or services to individuals in the EEA or monitoring the behavior of individuals in the EEA';
- **Will the GDPR still apply when the UK leaves the EU?** GDPR will no longer apply to the UK after the end of the transition period but the UK intends to incorporate GDPR into UK data protection law from the end of the transition period, 'so in practice there will be little change to the core data protection principles, rights and obligations found in the GDPR'. But bear in mind that:
    - 'if you operate inside the UK, you will need to comply with UK data protection law';
    - 'the EU version of the GDPR may also still apply directly to you if you operate in Europe, offer goods or services to individuals in Europe, or monitor the behaviour of individuals in Europe';
    - 'GDPR will still apply to any organisations in Europe who send you data, so you may need to help them decide how to transfer personal data to the UK in line with the GDPR'; and,
    - 'The ICO will not be the regulator for any European-specific activities caught by the EU version of the GDPR, although we hope to continue working closely with European supervisory authorities';
- **What role will the ICO have?** The ICO will continue to be the UK's data protection regulator as regards the UK's data protection legislation. Further, '[d]uring the transition period the ICO will engage in the co-operation and consistency mechanism under GDPR and continue to be a lead supervisory authority. The UK government will continue to work towards maintaining close working relationships between the ICO and the EU supervisory authorities once the UK has left the EU';
- **Is the ICO's GDPR guidance still relevant?** 'Yes. We expect UK data protection law to be aligned with the GDPR, so you should continue to use our existing guidance. Following the approach in our guidance will help you comply now and after the end of the transitional period';
- **Can we still transfer data to and from Europe?** The UK government's position is that data transfers *from* the UK *to* the EEA 'will not be restricted. But, from the end of the transition period, GDPR transfer rules will apply to any data coming from the EEA into the UK';
- **Does PECR still apply?** 'Yes. The current PECR rules cover marketing, cookies and electronic communications. They derive from EU law but are set out in UK law. They will continue to apply after we exit the EU. The EU is replacing the current e-privacy law with a new e-privacy Regulation (ePR). The new ePR is not yet agreed.'

- **Do the Network and Systems Regulations (NIS) still apply?** Yes. The NIS rules cover network and information systems and include security requirements and mandatory 'incident' notification obligations. The NIS regime derives from EU law and has been implemented into UK law and will continue to apply after the UK has left the EU. Further, '[i]f you are a UK-based digital service provider offering services in the EU, from the end of the transition period you may need to appoint a representative in one of the EU member states in which you offer services. You will need to comply with the local NIS rules in that member state. If you also offer services in the UK, you will also need to continue to comply with the UK rules regarding your UK services'.

The FAQs can be found here: https://ico.org.uk/media/for-organisations/documents/brexit/2617110/information-rights-and-brexit-faqs-v2_3.pdf.

The FAQs make no mention of the fact that the EU will need to adopt a so-called 'adequacy decision' concerning the UK – this cannot be expected to be automatic, in particular because of the UK's surveillance legislation that is viewed in some quarters as not complying with data protection rules.

There is also some uncertainty as to how in reality the ICO will play its role in the co-operation and consistency mechanism under GDPR and continue to be a lead supervisory authority during the transition period.

Note that although the FAQs are an update on the current situation the ICO's guidance materials remain focused on a no-deal situation (which could of course still happen after the transition period).

Finally, bear in mind that at the end of the day the ICO's guidance and resources are simply that – the ICO could depart from them, a court might disagree with them, they might be subject to challenge from pressure groups, and the EU organisms might also take a different view of them.

What is the takeaway?

The takeaway for what to do during the transition period is to have a plan and put it in place:

1. Be proactive – do not leave this until the last-minute and instead review your current compliance measures on a prioritized basis;
2. Looking at data transfer arrangements should be a key priority (standard contractual clauses/model clauses, Binding Corporate Rules etc.) – approach the businesses, vendors etc. with whom your data transfers are taking place for discussions about future arrangements between you;
3. Consider the official Representative obligations and start drafting the relevant documentation to be able to make this work in practice;
4. Follow closely how the ICO's role actually plays out in the co-operation and consistency mechanism and how it continues to act a lead supervisory authority, and determine who your lead supervisory authority might be after the end of the transition period; and,
5. Follow the eventual changes made to UK data protection rules and determine if and how they might affect your business.

We report about data protection issues here: http://www.corderycompliance.com/category/data-protection-privacy/.

For more about GDPR please also see our GDPR FAQs which can be found here: http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/

and our Data Protection Glossary which can be found here: http://www.corderycompliance.com/?s=glossary.

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. GDPR Navigator includes:

- Detailed guidance on the security aspects of GDPR in paper and on film;
- A template data breach log;

- A template data breach plan; and,
- A template data breach reporting form.For more information please contact André Bywater or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

For information about our Breach Navigator tool please see here: https://www.corderycompliance.com/solutions/breach-navigator/

For more information please contact André Bywater or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

André Bywater

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com

Jonathan Armstrong

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com

Image used courtesy of the ICO