

Insights

THE DATA & BREXIT DIGEST – DRAFTING TIPS FOR CONTRACTS AND POLICIES

28 January 2021

Introduction

With the UK now unambiguously out of the EU, the EU General Data Protection Regulation (2016/679) (“**EU GDPR**”) has been replaced by the United Kingdom General Data Protection Regulation (“**UK GDPR**”). In this third instalment of our Data & Brexit Digest, we highlight some practical implications of Brexit for data protection contractual drafting and policies.

What should you consider in terms of contractual and policy drafting?

Contracts

- Statutory references: Standard terms and conditions and other contractual documents should be updated to include the correct statutory references. Where an agreement has a cross-border element, this will involve considering the extent to which the UK GDPR, the EU GDPR and/or other data protection laws may apply to each party, and how this should be reflected in the drafting. This should take account of the specific circumstances, such as the location of the parties and the nature of any services being provided.
- Liability: Statutory references and references to a particular “data protection authority” may prove to be significant in the event that liability arises under the contract; if these are tied to the EU GDPR, will they provide the redress intended in the event of a fine being issued in future under the UK GDPR, for example? Limitations on liability and indemnities are another area for consideration.
- Future amendments and flexibility: The UK government is currently consulting on its National Data Strategy, with the consultation document suggesting that UK data protection law is likely to be amended in the coming year. Similarly, the UK’s data protection authority, the ICO, has indicated there will be a consultation on new UK standard contractual clauses for data transfers. Parties to an agreement may wish to signal a mutual willingness for flexibility in this area, e.g. an acknowledgment that, in the event of a material change to relevant legislation, certain aspects of a data protection clause may need to be revisited.

Policies

- Privacy policies and notices: Organisations should ensure that privacy policies (whether directed at website users, clients, employees, recruits or other third parties) are updated to reflect the UK's move to the UK GDPR. In particular, any information regarding international transfers is likely to require revision. Following the end of the Brexit transition period, EEA member states became "third countries" for the purposes of the UK GDPR, triggering a need to update references to transfers out of the "EEA".
- Data security breach response plans: The ICO can no longer serve as the "lead authority" for companies that fall within the jurisdictional scope of the EU GDPR, just as EU data protection authorities are not capable of enforcing the UK GDPR. Companies should consider what this change may mean, particularly in the event of a cross-border data security incident. This increases the likelihood that multiple personal data breach reports will need to be made where a single report to an organisation's lead authority may have sufficed in the past.
- Internal documentation: Organisations subject to both the UK GDPR and EU GDPR may wish to maintain separate Article 30 records of processing activities ("**ROPAs**"). Each ROPA, whether drafted pursuant to the UK GDPR or EU GDPR, must detail any transfers of personal data to "third countries" (a term that will encompass different jurisdictions in each case).

Some changes are more obvious than others, such as updating references to the UK GDPR; however, other implications can be more subtle and also potentially far-reaching, particularly in a contractual context. This briefing is not legal advice. Please feel free to contact any team member if you would like to discuss any of the issues covered in this instalment.

The UK's data protection regime looks set for a period of change in 2021, notwithstanding the significant impact already brought about by Brexit. Businesses will need to be alert to these regulatory changes and monitor developments carefully. In our next instalment, we look at GDPR representatives required under Article 27.

Previous Editions of the Data & Brexit Digest

- Personal Data and the UK-EU Trade and Cooperation Agreement: UK gets special "third country" status for up to 6 months
- What is the source of the UK's post Brexit Data Protection Law and how should you reference it?

RELATED PRACTICE AREAS

- Data Privacy & Security

- General Data Protection Regulation
- Brexit

MEET THE TEAM



Kate Brimsted

Co-Author, London

kate.brimsted@bclplaw.com

[+44 \(0\) 20 3400 3207](tel:+442034003207)



Geraldine Scali

Co-Author, London

geraldine.scali@bclplaw.com

[+44 \(0\) 20 3400 4483](tel:+442034004483)



Anna Blest

Co-Author, London

anna.blest@bclplaw.com

[+44 \(0\) 20 3400 4475](tel:+442034004475)

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.