

Client Alert: ICO GDPR Draft Guidance on Contracts & Liabilities between Data Controllers & Data Processors

Date : September 27, 2017

The UK data protection regulator, the Information Commissioner's Office (ICO), recently published draft guidance on contracts and liabilities between data controllers and data processors under the EU General Data Protection Regulation (GDPR).

The draft guidance seeks to explain to data controllers what they must include in contracts and sets out what responsibilities and liabilities data processors have under GDPR. It is mainly just a summary of what GDPR says about these issues, with some degree of explanation, and some practical examples, along with two checklists, one for data controller and data processor contracts and the other for data processors' responsibilities and liabilities.

This material is useful by way of setting out the basics but does not address these complicated issues in detail.

This draft guidance nevertheless does act as a timely reminder that businesses would do well to consider now revising their existing contracts that will be affected by GDPR, if they haven't already done so.

It is also worth highlighting that a key new issue under GDPR is that data processors have direct responsibilities and liabilities in their own right, i.e. outside and beyond the contractual terms in contracts between them and data controllers. This includes liability subject to corrective measures, fines and compensation requirements for non-compliance with GDPR obligations (i.e. specifically concerning data processors) or where data processors act against a data controller's instructions. This said, as the guidance also points out, data controllers are ultimately responsible for ensuring that data is processed in a compliant fashion even where they appoint a data processor to process it on the data controller's behalf, and data controllers only avoid liability if they can demonstrate that they are "in no way responsible for the event giving rise to the damage" resulting from data processed (by a data processor on their behalf) in a non-complaint way; a data controller may be able to claim back all or part of any compensation paid from a data processor to the extent that the data processor is liable.

GDPR Navigator (for more information on this and a link see the end) has some information which helps establish who a data controller and who a data processor is in any given situation and helps work out how to structure the relationship. The resources include:

1. a Guidance Note on accountability and audit;
2. a Guidance Note on appointing processors;
3. a Guidance Note on determining who is the data controller and data processor;
4. a comprehensive glossary of data protection terms;
5. a Guidance Note on fine determination;
6. a 35 minute film on key aspects of GDPR;
7. a 10 minute film on the information security aspects of GDPR, including responsibilities on data processors;
and
8. a 25 minute film on data protection impact assessments.

The ICO consultation closes on 10 October 2017.

The ICO also indicates in the draft guidance that it will also issue at some point separate GDPR-related guidance on: security matters; data subjects' rights; breaches, including breach notification; Data Protection Impact Assessments; high-risk processing; Data Protection Officers; appointing a representative in the EU (where a data controller or data processor is based outside the EU); investigative and corrective powers, penalties and damages; and, record-keeping.

We have written previously on GDPR including our FAQs, which can be found [here](#). We have developed the GDPR Navigator[™] subscription service to help business get ready to deal with GDPR compliance requirements – for more

about this please see [here](#).

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

[Jonathan Armstrong](#), Cordery, Lexis House, 30
Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com



[André Bywater](#), Cordery, Lexis House, 30
Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com

Farringd

