



ICO issues further guidance on roles of data controller and data processor

The ICO has issued new guidance for organisations as to when they will be a data controller or a data processor given the continuing confusion over the roles. The distinction is important because only data controllers have to comply with the Data Protection Act 1998 (DPA).

Under the DPA the data controller is the organisation that determines the purposes for which and the manner in which personal data is processed. It has overall control over the why and how of the processing. A data processor is any organisation processing data on behalf of a data controller.

When trying to decide whether an organisation is a data controller or data processor the ICO suggests ascertaining who makes certain decisions including whether to collect data and the legal basis for doing so, which data to collect, the purposes of collection, which individuals to collect data from, whether to disclose the data and who to, whether subject access rights apply and how long to retain the data. These are all decisions that a data controller would take.

The guidance states that the decisions that are more likely to be made by a data processor relate more to the technical aspects of the processing including what IT systems or methods are used to collect data, how the data is stored, security measures, the means of transfer of the data from and to other organisations, the means used to retrieve data if necessary, the method for ensuring a retention schedule is complied with and the means of deletion and destruction of data.

However, the ICO recognises that modern business relationships are complex and in every business relationship the responsibilities of the parties will vary. It suggests that the key is to determine the degree of independence and degree of control that an organisation has over the processing activities.

The guidance provides several examples of applying these factors to common business relationships including employing a market research company (a data controller), an agreement with a third party payment company (a data controller),

appointment of professional services firms (data controllers) and the outsourcing of data storage (a processor).

Having established the status of the parties, the guidance gives recommendations as to the governing of such relationships to ensure compliance with the DPA. The key message is that whatever the parties' status, organisations should have a written agreement in place clearly setting out each party's responsibilities and obligations in relation to processing the data. Key points to cover in the agreement are how the data can be used, whether the data can be disclosed, security requirements, use of sub-contractors, assistance with subject access requests and transfers overseas.

The guidance also reminds organisations that even where they are a data processor for their customers during the supply of services, they will also be a data controller in respect of their own business activities, for example the processing of data about their own employees.

The full guidance can be found here: http://ico.org.uk/news/current_topics/~media/documents/library/Data_Protection/Detailed_specialist_guides/data-controllers-and-data-processors-dp-guidance.pdf

Contacts

If you have any queries, please contact:



Andrew Dunlop
Partner

+44 (0)117 902 2786
andrew.dunlop@burgess-salmon.com



Chris O'Connell
Associate

+44 (0)117 307 6885
chris.o'connell@burgess-salmon.com