Data Protection Act

Data Controller or Data Processor?

information commissioner
Barrantagh Fysseree

The Data Protection Act 2002 (DPA) imposes certain obligations on "data controllers". These include the requirement to maintain an entry in the register of data controllers and compliance with the data protection principles and the rights of individuals.

What is a "Data Controller"?

A data controller is the legal person (which includes a company, an organisation or an individual such as a sole trader or private practitioner) *"who either alone, or jointly, determines the purpose for and manner in which personal data is, or will be, processed"*.

"Processing" includes obtaining, holding, or recording data or carrying out operations such as disclosure, retrieval, consultation, organisation and ultimately erasure or destruction of the data.

A Data Controller exercises overall control and determines, among other things, what personal information is necessary to fulfil the purpose, how that personal information is to be processed, to whom it may be disclosed and how it is stored.

> *A company is a data controller for any personal data it processes about its employees, and for any images of people, employees or the public, recorded by CCTV cameras.*

If a data controller is required by law to process personal data, it must retain its responsibility as data controller. For example, whilst a corporate service provider may undertake the anti money-laundering reporting function on behalf of its client companies, each client company remains responsible for that processing as the data controller.

What is a "Data Processor"?

A data controller may engage a third party to undertake certain aspects of the processing necessary for fulfilling its purpose(s).

"[A]ny person (other than an employee of the data controller) who processes the data on behalf of the data controller" is a "data processor", for example, a third party undertaking a payroll function, advertising campaign, or data destruction.

Note that the definition explicitly excludes employees of the data controller – this may be their job title, but it is not their legal status under the DPA.

A data processor will be contractually obliged to ensure it processes personal data only in accordance with the data controller's instructions, including complying with the provisions of the DPA.

The data processor often has the freedom to use its technical knowledge to decide how to carry out certain activities on the data controller's behalf, but it cannot take overarching decisions and the data controller remains legally responsible for any personal data processed by its data processor. This includes, in particular, the security of the personal data.

Specialist service providers, for example, accountants, advocates, recruitment agencies or counselling services, will process personal data in accordance with their own professional obligations and will always be acting as a data controller in their own right. They cannot agree to hand over or share data controller obligations with the client in the context of engagement for that service.

Does a data processor need to have an entry in the register of data controllers?

A data processor will not be required to notify the Information Commissioner of its processing and have an entry in the register of data controllers if the **only** processing it undertakes is as a data processor.

However, it is likely that a data processor will also be a data controller in its own right: for example it is likely to process the personal data of its own staff. It may also process personal data for other purposes, such as having CCTV on the premises, and therefore be required to have an entry in the register of data controllers.

Further guidance on the notification requirement is available in the "Registration" section of our website.

Other guidance

The UK's Information Commissioner has published guidance on its website, www.ico.org.uk

The Article 29 Working Party on Data Protection has issued an Opinion on the differences between data controllers and data processors, *"Opinion 1/2010 on the concepts of "controller" and "processor""*. This can be found by following the link to the Article 29 Working Party from the Useful Links page on our website.

Data controllers and data processors: what's the difference?

A bank contracts a market research company to carry out research. The bank's brief specifies its budget and that it requires a satisfaction survey of its main retail services based on the views of a sample of its customers across the UK. The bank leaves it to the research company to determine sample sizes, interview methods and presentation of results.

The research company is a **data controller**, as it determines the methodology for processing personal data.

An online retailer works in co-operation with a third-party payment company to process customers' transactions.

The payment company is a **data controller** for the personal data processed for the payments - the payment company provides that specific service on behalf of the online retailer. The online retailer has no say in how that processing is undertaken by the payment company.

A firm uses an advocate to represent it.

The advocate is a **data controller** for the personal data processed to provide legal advice or represent the firm. The advocate provides advice, and the firm decides whether to follow it or not – the firm cannot ask the advocate to make amendments to the original advice – the advocate controls the detailed content of the advice. The advocate is also bound by professional and legal obligations with regard to record-keeping and confidentiality of communications etc.

A car hire company contracts a vehicle-tracking company to install devices in its cars and monitor them so that cars can be recovered if they go missing. They specify that the tracking company should track all the company's cars and send back the location data to the hire company six hours after the end of the hire period, if the car has not been returned.

The vehicle-tracking company is a **data controller**, determines how the personal data is processed, and sends a report based on that personal data to the car hire company. The car hire company has no say in how the vehicle-tracking system works.

A local authority uses a cloud provider to store data about its housing stock and residents, rather than holding the data on its own IT system. The cloud provider is also contracted to delete certain data after a particular period and to grant members of the public access to their own records via a secure online portal. It also hosts a residents' discussion forum.

The cloud provider is a **data processor** acting on the instructions of the local authority. A contract is in place which includes terms regarding deletion and the right of access to personal data. The local authority exercises overall control over the purpose for which, and the manner in which, personal data are processed.

A regulatory authority is required by an enactment to carry out certain functions, including the handling of complaints from members of the public who have environmental concerns. Given the large number of complaints it receives, the authority decides to outsource its complaints handling to a much larger regulatory authority with better logistical capacity. The first regulatory authority will no longer provide these services itself and will second most of its staff to the larger authority. The two authorities put an agreement in place saying that, in effect, all data protection compliance responsibilities have passed over to the larger authority.

The larger authority provider is a **data processor** acting on the instruction of the regulatory authority. The regulatory authority exercises overall control over the purpose for which, and the manner in which, personal data are processed.

A courier service is contracted by a local hospital to deliver envelopes containing patients' medical records to other health service institutions. The courier service is in physical possession of the mail but may not open it to access any personal data or other content.

The mail delivery service is neither a data controller or data processor for the service provided as it does not process any personal data. If, however, electronic signatures are required or it maintains a database of the recipients' details, then it will be a data controller in its own right for that personal data. It will never be a data processor in the context of that service.