Data controllers and data processors: what the difference is and what the governance implications are

Iain Bourne
Group Manager, Policy Delivery
Why new guidance?

- The existing guidance was fine but maybe lawyer and accountant-centric
- Policy advice request analysis showed a need for new processor scenarios to be covered
- Requests from enforcement / audit showed need for more advice on governance issues
- External confusion about whether organisations are controllers or processors: complex business relationships
The problems we’re trying to solve

- Organisations thinking they’re data controllers when they’re data processors
- Organisations thinking they’re data processors when they’re data controllers
- Organisations deeming other data controllers to be their data processors when they’re not
- Particular confusion in some areas – eg mail delivery services
- Tension between what the law says and how modern business relationships work
Overview 1

It is essential for organisations involved in the processing of personal data to be able to determine whether they are acting as a data controller or as a data processor in respect of the processing. This is particularly important in situations such as a data breach where it will be necessary to determine which organisation has data protection responsibility.
Overview 2

The data controller must exercise overall control over the purpose for which, and the manner in which, personal data are processed. However, in reality a data processor can itself exercise some control over the manner of processing – e.g. over the technical aspects of how a particular service is delivered.
The fact that one organisation provides a service to another organisation does not necessarily mean that it is acting as a data processor. It could be a data controller in its own right, depending on the degree of control it exercises over the processing operation.
A data controller decides:

- to collect the personal data in the first place and the legal basis for doing so;
- which items of personal data to collect, ie the content of the data;
- the purpose or purposes the data are to be used for;
- which individuals to collect data about;
- whether to disclose the data, and if so, who to;
- whether subject access and other individuals’ rights apply ie the application of exemptions; and
- how long to retain the data or whether to make non-routine amendments to the data.
A data processor can decide:

- what IT systems or other methods to use to collect personal data;
- how to store the personal data;
- the detail of the security surrounding the personal data;
- the means used to transfer the personal data from one organisation to another;
- the means used to retrieve personal data about certain individuals;
- the method for ensuring a retention schedule is adhered to; and
- the means used to delete or dispose of the data.
What’s in it 1?

• What is the difference between a controller and a processor: what the law says
• Processing required by law – ie statutory duty
• Why is it important to distinguish between data controllers and data processors?
• How do you determine whether an organisation is a data controller or a data processor: practical tests
What is in it 2?

- Why can it be difficult to tell the difference between controller and processor?
- Enforcement issues – eg where there’s a data breach
- Sub-contractors, professional advisors, consultants
- When processors take on controller responsibility
- Examples
Examples

• Market research companies
• Payment services
• Mail delivery services
• Solicitors
• Accountants
• IT services
• Cloud providers
• Statutory bodies
Keep in touch

Subscribe to our e-newsletter at www.ico.gov.uk or find us on...

facebook

Twitter

www.twitter.com/iconews

YouTube

LinkedIn