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

Data Protection Act

Please note: The following information has not been updated since the Data Protection Act 2018 became law. Although there may be some subtle differences between the guidance in this document and guidance reflecting the new law – we still consider the information useful to those in the media. This guidance will be updated soon to reflect the changes.

Contents

Introduction

1. The Data Protection Act 1998 (the DPA) is based around eight principles of good information handling. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

2. An overview of the main provisions of the DPA can be found in The Guide to Data Protection.

3. This is part of a series of guidance, which goes into more detail than the Guide, to help data controllers to fully understand their obligations and promote good practice.

4. As information systems and business models become more complex, a number of organisations may be working together in an initiative that involves processing personal data.

5. We are producing this guidance because of the increasing difficulty organisations can face in determining whether they or the organisations they are working with have data protection responsibility.

6. In data protection terms, these organisations must act as either data controllers or data processors.

7. This guidance will explain the difference between a data controller and a data processor, what their roles and responsibilities are and the governance issues that have to be addressed to ensure data protection compliance.

Overview

- 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.

- 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.

Section 1 - What is the difference between a data controller and a data processor?

What the DPA says

8. The DPA draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. It is the data controller that must exercise control over the processing and carry data protection responsibility for it. This distinction is also a feature of Directive 94/46/EC, on which the UK's DPA is based.

9. Section 1(1) says that:

> **"data controller"** means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed
>
> **"data processor"**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
>
> **"processing"**, in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—
>
> a) organisation, adaptation or alteration of the information or data,
> b) retrieval, consultation or use of the information or data,
> c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

> d) alignment, combination, blocking, erasure or destruction of the information or data

10. The definition of processing can be useful in determining the sort of activities an organisation can engage in and what decisions it can take within its role as a data processor. The definition of 'processing' suggests that a data processor's activities must be limited to the more 'technical' aspects of an operation, such as data storage, retrieval or erasure. Activities such as interpretation, the exercise of professional judgement or significant decision-making in relation to personal data must be carried out by a data controller. This is not a hard and fast distinction and some aspects of 'processing', for example 'holding' personal data, could be common to the controller and the processor.

Processing required by law

11. Section 1(4) of the DPA says that:

> Where personal data are processed only for purposes for which they are required by or under any enactment to be processed, the person on whom the obligation to process the data is imposed by or under that enactment is for the purposes of this Act the data controller.

12. This means that where an organisation is required by law to process personal data, it must retain data controller responsibility for the processing. It cannot negate its responsibility by 'handing over' responsibility for the processing to another data controller or data processor. Although it could use either type of organisation to carry out certain aspects of the processing for it, overall responsibility remains with the organisation with the statutory responsibility to carry out the processing.

Why is it important to distinguish between data controllers and data processors?

13. If all parties are working well together to make sure that compliance issues such as giving subject access or keeping personal data secure are addressed, then the question of data protection responsibility may seem academic. However, the distinction between a data controller and data processor can have significant real-world consequences. For example, if there is a data breach it is essential for both the organisations involved and the ICO to be able to determine where responsibility lies.

14. This can be difficult, and there is evidence of confusion on the part of some organisations as to their respective roles and therefore their data protection responsibilities. It is important that the various organisations involved in a data processing activity establish their roles and responsibilities at an early stage, particularly before the processing commences. This will help to ensure that there are no gaps in organisations' responsibilities – such gaps could result in subject access requests going unanswered, for example.

How do you determine whether an organisation is a data controller or a data processor?

15. The data controller determines the purposes for which and the manner in which personal data is processed. It can do this either on its own or jointly or in common with other organisations. This means that the data controller exercises overall control over the 'why' and the 'how' of a data processing activity. The definition provides flexibility, for example it can allow one data controller to mainly, but not exclusively, control the purpose of the processing with another data controller. It can also allow another data controller to have some say in determining the purpose whilst being mainly responsible for controlling the manner of the processing. Many business relationships work this way.

16. To determine whether you are a data controller you need to ascertain which organisation 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.

17. These are all decisions that can only be taken by the data controller as part of its overall control of the data processing operation.

18. Within the terms of the agreement with the data controller, and its contract, a data processor may 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.

19. These lists are not exhaustive, but illustrate the differences between the controller's and the processor's roles. They illustrate that a processor has the freedom to use its technical knowledge to decide how to carry out certain activities on the data controller's behalf. However, it cannot take any of the over-arching decisions, for example what the personal data will be used for or what the content of the data is. Such decisions must only be taken by the data controller.

Why can it be difficult to determine where data protection responsibility lies?

20. The DPA's definition of data processor can be difficult to translate into the complexity of modern business relationships. In practice there is a scale of responsibility in terms of how organisations work together to process personal data. The key

is to determine the degree of independence that each party has in determining how and in what manner the data is processed as well as the degree of control over the content of personal data.

21. At one extreme, one party will determine what personal data is to be processed and will provide very detailed processing instructions which the other party must follow. The party following the instructions is tightly constrained in what it can do with the data and has no say at all over its content or how it is processed. In this relationship the party providing the detailed instructions (the client) is clearly the data controller and the party following the instructions (the service provider) is the data processor. For example, the client may provide precise instructions to the service provider about how to store the personal data, including what sort of servers should be used, what encryption products should be deployed and what sort of physical security should be in place. This type of arrangement is relatively rare but is sometimes found in government, for example where contractors are handling high-security information and arrangements for its protection are set out in great detail.

22. However, it is far more common for a data controller to allow its processor a considerable degree of discretion over how the processing takes place using its own expertise. For example, a bank hires an IT services firm to store archived data on its behalf. The bank will still control how and why the data is used and determine its retention period. In reality the IT services firm will use a great deal of its own technical expertise and professional judgement to decide how best to store the data in a safe and accessible way. However, despite this freedom to take technical decisions, the IT firm is still not a data controller in respect of the bank's data. This is because the bank retains exclusive control over the purpose for which the data is processed and the content of the data, if not exclusively over the manner in which the processing takes place. A key consideration is who exercises control over the content of the personal data.

Data processors who are also data controllers

23. A data processor usually also has its own data controller responsibilities for personal data which is not being processed on behalf of its data controller client. In our original example, the IT services firm will have its own data controller responsibilities for its employees' records or those of its clients

and suppliers, but not for the data processing it carries out when it is storing personal data for the bank. An organisation cannot be both data controller and processor for the same data processing activity; it must be one or the other.

24. This means that in order to establish which organisation has data protection responsibility for which data, it is necessary to look at the processing in question, as well as the organisations involved. It is also important that, as far as is practicable, systems and procedures distinguish between the organisation's 'own' data and the data it processes on behalf of the other data controller.

Sub-contractors, professional advisers and consultants

25. There can be a tendency for the 'main' data controller organisation to deem its sub-contractor, professional adviser or consultant to be its data processor. Sometimes this can be written into a contract. However, the fact that an organisation contracts or employs another organisation to provide a service to it does not mean that the other organisation becomes its data processor in every case. Whether an organisation is a data controller or data processor will depend on their role and responsibilities in relation to the processing.

26. Organisations often use a professional or business service to obtain specialist assistance, for example:

    - a lawyer to provide legal advice;
    - an accountant to provide accountancy services;
    - a doctor to provide a medical report on an individual in connection with an insurance claim;
    - a recruitment agency to recruit specialist staff for an engineering firm; or
    - a counselling service to assist traumatised individuals employed by the emergency services.

27. In these cases, the client will not have sole data controller responsibility even though they initiated the work by asking for advice or commissioning a report. Responsibility also lies with the professional service provider itself because it determines what information to obtain and process in order to do the work and because it is answerable itself for the content. The use of a lawyer provides a good illustration of why providers of professional services are not usually just data processors. A client receives legal advice and, regardless of whether or not

he chooses to follow the advice, would not ask the lawyer to make amendments to the original advice – the lawyer controls the detailed content of the advice. Lawyers would also have their own professional responsibilities in terms of record keeping, the confidentiality of communications and so forth. Again, this points towards lawyers and similar professional service providers being data controllers in their own right.

28. Organisations that are data processors may use a sub-contractor to deliver their services. In our original example, the IT services firm might want to contract out part of its storage solution to a cloud provider. Although it is not a requirement of the DPA, it is good practice for the data processor to seek the consent of its data controller prior to sub-contracting out any of its services. The written contract between the controller and the processor should stipulate whether the sub-contracting of services is allowed. The fact that a data processor sub-contracts out its services does not make it a data controller in its own right, provided that overall control of the processing remains with the original data controller.

Examples

Market research company

29. A bank contracts a market research company to carry out some 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.

30. The research company is processing personal data on the bank's behalf, but it is also determining the information that is collected (what to ask the bank's customers) and the manner in which the processing (the survey) will be carried out. It has the freedom to decide such matters as which customers to select for interview, what form the interview should take, what information to collect from customers and how to present the results. This means that the market research company is a data controller in its own right in respect of the processing of personal data done to carry out the survey, even though the bank retains overall control of the data in terms of commissioning the research and determining the purpose the data will be used for.

Payment services

31. An online retailer works in co-operation with a third-party payment company to process customers' transactions. The payment company is not the retailer's data processor, even though there is a contract in place between the two companies that covers areas such as service standards and financial arrangements. This is because the payment company:

    - decides which information it needs from customers in order to process their payments correctly;
    - exercises control over the other purposes the customer's data is used for, for example direct marketing;
    - has legal requirements of its own to meet, for example relating to the use and retention of payment card data; and
    - has its own terms and conditions that apply directly to the retailer's customers.

32. Therefore the payment service is a data controller in its own right and will have full data protection responsibility for the processing it carries out.

Mail delivery services

33. 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.

34. A mail delivery service will not generally process personal data, even if it does physically hold the personal data contained in a letter sent using its services. Processing personal data, including holding it, implies a degree of access to or ability to control or use the data itself, not just physical possession of the letters or parcels that contain the data. The term 'holding', as used in the definition of 'processing', implies considerably more than simply being in possession of a physical object that contains personal data.

35. This means that the mail delivery service is neither a data controller nor a data processor for the clients that use its services because:

    - it is a mere conduit between the sender of the mail and its recipient;

- it does not exercise any control over the purpose for which the personal data in the items of mail entrusted to it is used; and
- it has no control over the content of the personal data entrusted to it.

36. This makes sense in practice because it would be unreasonable to expect a mail delivery service that has no control over the content of the mail items it delivers to comply with the data protection principles. For example it would not be able to ensure that personal data in its possession is accurate, up to date or held only for so long as it necessary. It cannot have data protection responsibility for personal data contained in an item of mail. It is merely responsible for the security of the letter or parcel in a physical sense.

37. The fact that the delivery service does not act as a controller for the mail it has been asked to deliver – even if the content is personal data - means that the ICO cannot take any action against the delivery service. Also the fact that the delivery service is not a data processor means there is no need for clients using its services to put a data controller – data processor contract in place.

38. The data controller that chooses to use a delivery service to transfer personal data is the party responsible for the data. If a delivery service loses a parcel containing highly sensitive personal data, it is the data controller that sent the data that will be responsible for the loss. It was the data controller that chose to use the delivery service. If it was vital that the personal data was delivered securely, the data controller should have used secure delivery rather than an ordinary postal service.

39. However, the delivery service will be a data controller in its own right in respect of any data it holds to arrange delivery or tracking for example, such as individual senders' and recipients' names and addresses and in respect of its own staff records and so forth.

Solicitors

40. The owner of a small engineering firm has evidence that a former salesman stole a client list just before he resigned and is using it to promote a rival company. The firm's owner consults solicitors to find out whether she can secure the return of the list and prevent its use by the rival firm.

41. She knows the service she requires but has little understanding of the process the solicitors will adopt or how they will process the personal data she has provided about her ex-employee. Once she hands over the personal data to the solicitors, they take on data controller responsibility for the data and process it for their own purposes, even though they are acting on behalf of their client.

42. The solicitors process this personal data for the broad purpose of providing legal services in accordance with their professional obligations. They will use the information the firm has provided and will collect any other information they need in order to carry out the instructions. The solicitors determine the manner in which the personal data obtained from the firm will be processed. The solicitors therefore act as the data controller in relation to the personal data processed in connection with the client's instructions.

43. As the client and the solicitors are both data controllers in relation to this data, they each have their own data controller responsibilities – for example in relation to requests for access to the data and in terms of keeping the data secure.

Accountants

44. A firm uses an accountant to do its books. When acting for his client, the accountant is a data controller in relation to the personal data in the accounts. This is because accountants and similar providers of professional services work under a range of professional obligations which oblige them to take responsibility for the personal data they process. For example if the accountant detects malpractice whilst doing the firm's accounts he may, depending on its nature, be required under his monitoring obligations to report the malpractice to the police or other authorities. In doing so an accountant would not be acting on the client's instructions but in accordance with its own professional obligations and therefore as a data controller in his own right.

45. Where specialist service providers are processing data in accordance with their own professional obligations they will always be acting as the data controller and cannot agree to hand over or share data controller obligations with the client in this context.

IT services

46. 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.

47. However, despite these instructions, the vehicle-tracking company is a data controller in its own right. This is because it has sufficient freedom to use its expertise to decide which information to collect about cars (and their drivers) and how to analyse this. It is entirely in control of its own data collection – the operation of the vehicle-tracking software is a trade secret and the hire company does not even know what information is collected. Although the hire company determines the overall purpose of the tracking (the recovery of its cars), the fact that the tracking company has such a degree of freedom to decide which information to collect and how, means it is a data controller in its own right.

Cloud providers

48. 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.

49. Although the cloud provider provides a range of services and uses a great deal of its own technical expertise to do this, it is still only a data processor. A key consideration is that the conditions of the contract mean the cloud provider has no scope to use the data for any of its own purposes. In addition, the cloud provider does not collect any information itself. All the personal data it holds in connection with its provision of the service is provided by the local authority. See our guidance on cloud computing for more information about this.

Statutory bodies

50. 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.

51. The larger authority processes personal data about complainants in the same way as the first authority had done. As the first authority has ceased to handle complaints, it might appear that the larger second authority has become the data controller in respect of the files about complainants that have to be kept as part of the service. However, despite the arrangements in place between the two authorities, the statutory obligation to provide an environmental complaints handling service must remain with the first authority. It cannot renounce its data protection responsibilities in favour of the larger authority. The larger authority can only be a data processor because data controller responsibility must remain with the body with the relevant statutory responsibility for carrying out the processing.

Section 2 – What are the governance implications for data controllers and data processors?

Governance considerations between groups of data controllers

Compliance with the data protection principles

52. When a controller discloses personal data to another controller each has full data protection responsibility because both parties will exercise control over the purposes for which and the manner in which the data is processed. Where the sharing is systemic, large-scale or particularly risky, then both parties should sign up to a **data sharing agreement**, covering for example how the data can be used and whether it can be further disclosed. In other cases, where the sharing is a 'one off', is small scale and low-risk, then a more informal approach can be adopted. See our Data Sharing Code of Practice for more information about this.

53. A data sharing agreement could provide for the controller that holds most of the personal data to be responsible for the practical elements of compliance. For example, if a number of organisations – each data controllers in their own right – are working together in a child protection initiative it would be acceptable for one of the organisations to take responsibility for giving individuals subject access to the personal data held by all the organisations involved.

Enforcement issues

54. If there is an agreement in place about who will deal with the various aspects of compliance, for example dealing with subject access requests, then the ICO will only seek to take action against the data controller with responsibility for that aspect of compliance. However, the ICO may find that the other data controllers have failed in their obligations if:

- the allocation of responsibilities is unreasonable;
- the other data controllers are at fault for the non-compliance; or
- one of the other data controllers received the subject access request but failed to pass it to the controller responsible for handling requests.

55. Where a data controller provides personal data to another data controller, the second controller takes its own responsibility for any compliance failure on its behalf. For example, where a client instructs a solicitor in good faith, it would be unfair for the client to be held liable if the solicitor fails to process the personal data in accordance with the data protection principles. The client is unlikely to have any practical control over the data in question and indeed may have very little knowledge of what personal data the specialist is holding in connection with the service commissioned. This is reflected in the ICO's approach to enforcement.

Governance considerations between data controllers and data processors

Written contracts

56. Under the DPA all the legal responsibility for compliance falls directly on the data controller and not on the data processor. The DPA requires that when a controller discloses personal data

to a processor they should have a written contract in place rather than a data sharing agreement. This is because even after disclosure, only the controller will exercise control over both the purposes for which and the manner in which the personal data is processed. The controller issues contractual instructions to the processor saying what the processor can or cannot do with the data, with the contract requiring the processor to only act on its instructions.

57. The controller also has a duty to ensure the processor's security arrangements are at least equivalent to the security the controller would be required to have in place if it was processing the data itself.

> The DPA's interpretation of the seventh data protection principle (security) requires that:
>
> Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh (security) principle—
>
> (a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
>
> (b) take reasonable steps to ensure compliance with those measures.
>
> Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless—
>
> (a) the processing is carried out under a contract—
>
> (i) which is made or evidenced in writing, and
>
> (ii) under which the data processor is to act only on instructions from the data controller, and
>
> (b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

58. The controller must also take reasonable steps to ensure security is maintained, for example by regular auditing of the processor's security arrangements.

Transfers of personal data to data processors overseas

59. The DPA places restrictions on the transfer of personal data outside the European Economic Area. The provision of personal data from a data controller to a data processor is still a transfer for the purposes of the 8th data protection principle. This means that the data controller must ensure that any personal data transferred overseas remains adequately protected. The most obvious way to ensure that this is the case is through provisions included in the written contract that must exist anyway between the data controller and its processor. See our guidance on international transfers for more information about this.

Contracting out compliance tasks

60. Even though the data controller must remain exclusively responsible for overall compliance with the DPA, it can still contract out certain tasks related to this to its data processor. The most obvious example is where a controller uses a processor to store its personal data but then receives a request for subject access to the data. The controller can:

- require the data processor to provide it with the requested data so that the controller can deal with the request itself; or
- issue instructions to the processor so that the processor can deal with the request on the controller's behalf.

61. The latter option is only feasible if it is a routine subject access request. The controller will need to specify to the processor how to handle the request, for example by stipulating if there are any categories of information that it should withhold.

62. If the subject access request is less routine and involves working through the requested information to decide on a case by case basis whether a particular exemption applies, then the request can only be handled by the data controller itself. This is due to the degree of expertise and judgement that may be needed to apply the subject access exemptions correctly.

Enforcement issues

63. The distinction between a data controller and a data processor is particularly important in the context of enforcement action taken under the DPA. It is clear that the DPA makes the data controller legally responsible for the processing of personal data it undertakes itself and that is undertaken on its behalf by a data processor. No action can be taken under the DPA against a data processor itself. This is intended to ensure that data controllers put the necessary measures in place to protect their data processing operation from any vulnerability that may arise from their use of a data processor, such as a weakening of security.

64. The ICO cannot even take action directly against a processor who is entirely responsible for a data breach, for example by failing to deliver the security standards the controller has required it to put into place. However, in these cases the ICO may decide not to take any enforcement action against the controller if it believes it has done all it can to protect the personal data it is responsible for and to ensure the reliability of its processor, for example through a written contract. However, whilst the ICO cannot take action against the processor, the data controller could take its own civil action against its data processor, for example for breach of contract.

Data processors who take on data controller responsibilities

65. A data processor will have access to the personal data held by the controller or controllers it provides its services to but it cannot have any of its own data controller responsibilities for that data. However, in certain situations this may change and it will become a data controller in its own right if only to a limited extent.

66. If a data processor is directly served with a warrant requiring it to provide certain personal data to a law enforcement agency it will take on its own data controller responsibilities such as deciding if and how to comply with the request, which data to provide or withhold and what format to supply it in. This means that the ICO could take enforcement action against it directly, for example, if it disclosed excessive personal data in response to the warrant.

67. If a data processor breaks the agreement with its data controller, for example by using the data for its own

unauthorised purposes, then it will also take on its own data controller responsibilities. This includes the duty under the first data protection principle to process, including to obtain, personal data fairly and lawfully. Where a data processor takes the personal data the controller has entrusted it with but breaks the terms of its contract by using the data for its own purposes, it is likely to be in breach of the first principle and the ICO could take enforcement action against it. Where an organisation acting as a data processor obtains personal data without the consent of the data controller it could also commit a criminal offence under section 55 of the DPA.

More information

69. Additional guidance is available on our guidance pages if you need further information on other parts of the DPA.

70. This guidance has been developed drawing on ICO experience. Because of this it may provide more detail on issues that are often referred to the Information Commissioner than on those we rarely see. The guidance will be reviewed and considered from time to time in line with new decisions of the Information Commissioner, Tribunals and courts.

71. It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

72. If you need any more information about this or any other aspect of data protection, please contact us, or visit our website at www.ico.org.uk.