Using the crime and taxation exemptions

Data Protection Act

Contents

Introduction

1. The Data Protection Act 1998 (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 fully understand their obligations and promote good practice.

4. This guidance explains how to apply the exemptions for using personal data for purposes connected to crime and taxation. There are two main parts to the exemption. The first allows data controllers processing data for the relevant purposes to withhold information that should usually be provided to individuals. The second allows data controllers to disclose personal data in ways that would otherwise breach the data protection principles, if it is necessary for the relevant purposes.

Overview

- The crime and taxation exemptions are based on the purpose for which the personal data is being processed, not on the type of organisation doing the processing. The purposes relevant to this exemption are the prevention and detection of crime, the apprehension or prosecution of offenders, and the assessment or collection of tax.

- Data controllers do not have to fulfil their obligations to tell individuals how their data is being processed or respond to a subject access request (SAR), if doing so would prejudice the crime prevention and taxation purposes.

- Data controllers can disclose personal data without applying the usual data protection principles, if the disclosure is necessary for the crime prevention and taxation purposes.

- It is the data controller making the disclosure who is responsible

for deciding whether the exemption applies in each case.

- The exemptions must be applied on a case by case basis, and should be used only when it is necessary to do so.

The crime prevention and taxation purposes

5. Section 29 can be applied to:

> S29 (1) Personal data processed for any of the following purposes:
>
> a) The prevention or detection of crime,
> b) The apprehension or prosecution of offenders, or
> c) The assessment or collection of any tax or duty or of any imposition of a similar nature.

6. The scope of the exemption should be clear from the wording of the DPA. The exemption applies to the purpose of processing, not the type of organisation using the personal data. Police forces and HMRC are an obvious example of data controllers which are likely to need to apply the exemption when necessary, but the exemption is not limited to these bodies. A non-exhaustive list of relevant activity includes:

    - Recording information, interviews and statements about reported crimes and tax investigations.
    - Calculation of tax status or liability.
    - Intelligence gathering and surveillance for crime prevention and detection.
    - Attempts to locate potential suspects or witnesses in relation to crime prevention and detection.
    - Proceedings in the courts and tribunals for criminal or tax matters.
    - Assessments of suitability for parole or prisoner reclassification.

7. Even if a data controller's main activity falls within these purposes, not all of the personal data it processes will be within the scope of the exemption.

8. Data originally obtained for crime prevention or taxation activity but no longer processed for that purpose and now processed for a different purpose cannot be exempt under s29.

9. This exemption does not apply to civil legal proceedings. In circumstances where disclosure of information is necessary for civil proceedings or is otherwise required by law, data controllers should consider applying the exemption under s35 of the DPA.

Prejudice and likelihood

10. The exemption does not apply to all information being processed for the crime prevention and taxation purposes. The test is whether applying the DPA in the usual way "would be likely to prejudice" the purposes. A data controller should be able to demonstrate why this is the case each time the exemption is applied. An organisation cannot apply the exemptions as a blanket policy, even if in practice there are types of information that would be made exempt in the majority of decisions.

R (on the application of Alan Lord) v Secretary of State for the Home Department [2003] EWHC 2073 (Admin)

A prisoner challenged the Home Office's policy of automatically withholding reports into their Category A status in response to a subject access request. The Home Office's approach was to apply s29(1) to all requests for this information by data subjects. The court held that the policy of blanket non-disclosure could not be justified under s29(1), and that the exemption required a more selected and targeted approach to non-disclosure based on the circumstances of the particular case. The judge said that:

"it is for the data controller, if he wishes to rely upon the exemption in section 29(1), to show that one of the statutory objectives is likely to be prejudiced *in the particular case* in which the question arises".

11. The first step in deciding whether the exemption applies is to identify the prejudice that might occur if the DPA was followed in the usual way. In each particular case, the data controller needs to be able to demonstrate the nature of the prejudice. The prejudice can be that a specific investigation would be

compromised by information being withheld or disclosed. There can also be prejudice against wider activities, for example if disclosing personal data would reveal methods of investigation that need to remain confidential to be effective. Any prejudice must be real, actual and of substance. If the impact on the purposes would only be trivial, the exemption will not apply.

Example

A victim of a mugging tells the police that their attacker ran off through an industrial estate car park. The owners of the car park have CCTV footage that will help to identify the attacker and show their movements. This is clearly of importance to the apprehension and prosecution of the offender. Withholding the footage from the police would have a significant impact on the investigation. The owners of the car park can rely on s29(3) to allow the disclosure of the CCTV footage.

12. The next step in assessing whether the exemption applies is to establish a causal link between the use of the data and the prejudicial effect. The data controller should be able to show in each case how applying the DPA without the exemption would lead to the identified prejudicial outcome.

Example

A police force is concerned about a rise in burglaries targeting older people. They ask a local elderly support charity to share the names and addresses of their clients, so that the police can contact them to offer crime prevention advice.

Section 29(3) is unlikely to apply to the disclosure. This is because there is not a clear causal link between making the disclosure and preventing crime. Complying with the usual requirements of the DPA would not be inconsistent with the purpose of the disclosure. The police and the charity should find a way to share the information in compliance with the principles.

13. Finally, a data controller needs to be able to demonstrate that failing to apply the exemption would be "likely" to cause the prejudice that has been identified. In R (Lord) v Secretary of

State for the Home Department, the judge said the test of likelihood requires:

"a degree of probability where there is a very significant and weighty chance to prejudice to the identified public interests".

This test recognises that a data controller should only apply the exemptions when it is necessary to do so in order to safeguard the relevant purposes. It sets a higher bar than being merely 'possible', and requires a data controller to establish a strong link between the data processing and its prejudicial effect.

Example

An insurance company is concerned about the validity of a claim and conducts a standard investigation into whether it is an attempted fraud. While the claim is still being assessed, the customer makes a subject access request for the information held about them. The company refuses to provide any information, saying that it would prejudice an ongoing attempt to detect a criminal act.

A basic assertion that releasing the information might prejudice this and future investigations is not sufficient to rely on the exemption. The company would need to demonstrate more precisely how providing the information in this case would adversely affect their ability to investigate and prevent criminally fraudulent claims.

14. The factors to take into account when considering prejudice will depend on which part of the exemption is being applied and the nature of the data.

15. It is important to remember that in cases where the exemption does not apply, this does not necessarily mean that a particular activity cannot take place. If a data controller cannot rely on the exemption, they will need to find ways to ensure that if the processing does go ahead it is fully compliant with the requirements of the data protection principles.

Withholding information from individuals

16. There are two main ways in which the DPA requires organisations to provide information to individual data subjects. The first data protection principle requires data controllers to provide fair processing information so that individuals know how their data will be used. Section 7 of the DPA allows individuals to find out if an organisation is processing their personal data and to request copies of the personal data that is held about them. Section 29 allows data controllers to withhold this information, if following the usual requirements of the DPA would be likely to prejudice the crime prevention and taxation purposes.

The first data protection principle

17. Section 29(1) allows personal data to be exempted from the first data protection principle, except to the extent to which it requires compliance with the conditions in Schedules 2 and 3.

18. The first principle requires that personal data is processed fairly and lawfully. A key component of fairness is that individuals should know who is processing data about them and the purpose of the processing. Processing activity should generally be within the reasonable expectations of an individual, should be explained in a fair processing or privacy notice, and people should not be misled about how their data is used.

19. General guidance on how to comply with the first principle is available in the Guide to data protection and the Privacy notices code of practice.

20. In the context of the crime and taxation purposes, there will clearly be circumstances where it is undesirable to provide individuals with this information. This is likely to be because it would tip them off about an ongoing investigation, or would reveal general investigation methods to the wider detriment of an organisation's work. The exemption applies "to the extent to which" compliance would be likely to prejudice the crime and taxation purposes. This means that a data controller must do as much as it can to comply with the first principle.

21. The data controller still needs to have a valid condition under Schedule 2 for processing the data, and a further condition under Schedule 3 for sensitive personal data. Any processing being done for the crime prevention and taxation purposes is

very likely to be covered by paragraph 5 of Schedule 2 and paragraph 7 of Schedule 3.

Section 7 – subject access requests

22. Section 7 of the DPA allows individuals to request copies of the personal data that is held about them by a data controller. More detailed guidance about complying with these requests is available in our Subject access code of practice.

23. Like the exemption from the first principle, the exemption from section 7 applies only to the extent that providing the data would be likely to prejudice the crime prevention and taxation purposes. A data controller must handle each request on its own merits, and still has to provide as much personal data as possible.

24. The likelihood of prejudice may reduce over time, and this is particularly important to take into account when considering the application of the exemption to subject access requests. If a subject access request is made while an investigation is ongoing, there is likely to be a strong argument in favour of at least some personal data being withheld if it would reveal sensitive information about the process. However, a request which is made after an investigation has concluded is less likely to reveal information that would prejudice the purposes.

Example

A taxpayer makes a subject access request to HMRC for personal data they hold about him related to an ongoing investigation into possible tax evasion. If disclosing the information that HMRC have collected about the taxpayer would be likely to prejudice their investigation (because it would make it difficult for them to collect evidence, for example), HMRC could refuse to grant subject access to the extent that doing so would be likely to prejudice their investigation.

If the taxpayer makes the subject access request some years later when the investigation (and any subsequent prosecution) has been completed, it is unlikely that providing some of the information would prejudice the crime and taxation purposes – in which case HMRC would need to comply with it.

Extending the exemption to other statutory functions

25. Section 29(2) states that:

> Personal data which —
>
> (a) are processed for the purpose of discharging statutory functions, and
>
> (b) consist of information obtained for such a purpose from a person who had it in his possession for any of the purposes mentioned in subsection (1),
>
> are exempt from the subject information provisions to the same extent as personal data processed for any of the purposes mentioned in that subsection.

26. This section is particularly relevant to data controllers who have obtained information from the police or HMRC as part of their statutory functions, for example the Independent Police Complaints Commission or the Information Commissioner's Office. These organisations are processing the data for their own statutory functions, not for the crime prevention and taxation purposes. The s29(2) exemption ensures that a data controller can still withhold personal data in these limited circumstances if disclosure would prejudice the crime prevention and taxation purposes for which the data was originally held.

27. This exemption also applies on a case by case basis, so a data controller cannot take a blanket approach to all information obtained from the police or tax authority. It is good practice to consult with the source of the data when considering this exemption, but the final decision on whether to withhold or disclose the information lies with the data controller.

28. Data controllers covered by s29(2) may also be able to rely on the s31 exemption covering regulatory activity.

Withholding information about risk assessment

29. Sections 29(4) and (5) state that:

> (4) Personal data in respect of which the data controller is a relevant authority and which—

(a) consist of a classification applied to the data subject as part of a system of risk assessment which is operated by that authority for either of the following purposes—

(i) the assessment or collection of any tax or duty or any imposition of a similar nature, or

(ii) the prevention or detection of crime, or apprehension or prosecution of offenders, where the offence concerned involves any unlawful claim for any payment out of, or any unlawful application of, public funds, and

(b) are processed for either of those purposes,

are exempt from section 7 to the extent to which the exemption is required in the interests of the operation of the system.

(5) In subsection (4)— "public funds" includes funds provided by any institution;

"relevant authority" means—

(a) a government department,

(b) a local authority, or

(c) any other authority administering housing benefit or council tax benefit.

30. Organisations administering tax and benefits often use risk assessment criteria to identify potentially unlawful activity. One outcome of this might be a classification or warning marker being added to an individual's personal data.

31. The exemption allows an individual's risk classification to be withheld from them if they make a subject access request. The exemption only applies if disclosure would be harmful to the ongoing use of the system. This means that disclosure would have to reveal something about the wider operation of the risk classification and would allow individuals to avoid its measures. The test used by a data controller should be similar to a prejudice test, and they must be able to show a causal link between disclosure of the data and harming the system.

32. This exemption is only available to the organisations listed in s29(5). It cannot be used by private sector bodies or by public sector organisations that are not listed.

Disclosing information to prevent or detect crime

33. Disclosure of personal data, or of the information held in the data, is a type of data processing. This means that any disclosure should usually comply with the data protection principles. Section 29(3) allows a data controller to disclose personal data to a third party where the disclosure is made for any of the crime prevention or taxation purposes listed in 29(1) if applying specific provisions in the DPA would be likely to prejudice the purposes by preventing the disclosure.

34. The definition of "disclosure" under DPA s1(2)(b) includes disclosing the information contained in the data. This means that providing copies of data is not the only way to make a disclosure. For example, verbally disclosing or confirming personal data or allowing someone to view CCTV footage is still 'processing' under the DPA.

35. This exemption also applies on a case by case basis. This means that each time a request for disclosure is received, a data controller needs to decide whether or not to comply with the request based on the circumstances of the particular case. Responsibility for applying the exemption lies with the data controller making the disclosure, not the person requesting the information. The disclosing party needs to be satisfied that the disclosure is for the crime prevention or taxation purposes and that the prejudice test is met in each case.

36. Application of the exemption is discretionary - it **allows** disclosure in specific circumstances but does not **require** it.

37. The exemption should only be applied to the extent that it is necessary to do so to avoid prejudicing the crime and taxation purposes. This means that the data controller making the disclosure must do as much as it can to comply with the usual requirements of the DPA. A data controller should only disclose the information that is necessary for the purposes, and should not assume that all the data they hold is exempt. Speculative requests for personal data, especially about large numbers of people, are unlikely to meet the tests of necessity and prejudice.

Example

Full-time students are exempt from council tax, but a non-student who lives with other students is not. A local authority is concerned that non-students in these households are deliberately failing to register on the electoral roll in order to avoid paying council tax. The authority writes to letting agents in areas with a high student population asking them to disclose all rental agreements, so that they can compare names with the electoral roll.

It is unlikely that s29(3) can be used to allow the disclosure. Without specific evidence of potential criminal activity, the local authority is undertaking a 'fishing expedition' which will mean disclosing the personal data of mainly innocent people. There is not enough evidence to suggest that the detection of crime would be prejudiced in the case of each specific disclosure.

38. Some police forces, and other bodies who often request disclosure, use standard forms to describe the requested information and why it is needed. Alternatively, data controllers who frequently receive requests sometimes design their own request forms. There is no obligation on either side to use specific forms when considering the exemption, but there are several reasons why it is good practice to do so. Recording the reasons for disclosure creates an audit trail that can be used to demonstrate why the exemption was applied. It can also help data controllers to make consistent decisions, and is a sign of good data protection governance.

Example

A detective constable contacts an employer and asks them to provide contact details for one of their employees. They say that the disclosure is necessary for the crime and taxation purposes but are unwilling to provide further details in case it compromises the investigation.

The employer needs to be satisfied that the exemption applies. They could ask that a more senior police officer signs off a request for disclosure and provides a statement that is as clear as possible about why the information is needed. If they are still concerned that disclosing the information would breach the DPA, they can ask the police

to obtain a court order.

39. If a data controller knows that it will be sharing personal data with a third party on an ongoing basis, it should consider how to comply with the principles without relying on the exemption. The Data sharing code of practice provides detailed guidance on how to ensure that data sharing is compliant with the DPA.

40. A data controller does not need to have received a formal request for disclosure before applying the exemption. If the disclosure is necessary to avoid prejudicing the crime prevention and taxation purposes, this is sufficient to allow the data controller to share personal data. This means that data controllers can make proactive disclosures using s29(3).

41. The police and similar bodies can apply this exemption when they are making disclosures. However, they should take care to ensure that the exemption is only applied when the disclosure is necessary for the purposes specified in s29. They cannot use the exemption if the disclosure is for another purpose, even if it is related to policing or taxation and uses data that was previously used for the crime prevention and taxation purposes. For example, disclosures made by the police as part of the victim support process or to assess compensation are unlikely to be covered by s29(3).

The non-disclosure provisions

42. The sections of the DPA from which personal data processed for the relevant purposes are exempt under s29(3) are called the 'non-disclosure provisions' and are defined in s27(4). The provisions are:

- The first data protection principle, except to the extent to which it requires compliance with the conditions in Schedules 2 and 3.
- The second, third, fourth and fifth data protection principles.
- Sections 10 and 14(1) to (3).

To understand how the exemption applies, it can be useful to think about how these parts of the DPA usually apply in the context of making a disclosure.

43. These provisions only apply in the context of the disclosure of personal data by the data controller to a third party. The s29(3) exemption does not exempt a data controller from its obligations when it is processing data in other ways, nor does it cover the sharing of data between two departments of the same data controller.

Principles one and two

44. The first principle requires that a disclosure is fair and lawful, and the data controller can identify a relevant condition for processing. In most cases this means that individuals should be aware that a disclosure is happening or is likely to happen. This information is often contained in a privacy notice, but if a disclosure is particularly unusual or unexpected then a data controller might need to specifically tell individuals about it when it happens. A disclosure that is necessary for the crime and taxation purposes is often outside the usual expectations of an individual. Furthermore, it may be necessary to keep the disclosure secret from the individual to avoid tipping them off about an investigation.

45. The exemption only applies to the extent that complying with the usual requirements would be likely to prejudice the crime prevention and taxation purposes. A data controller should tell individuals about disclosures of their personal data if this is unlikely to cause prejudice.

46. Disclosures made under s29(3) are not exempt from the first principle's requirement that the data controller has identified a relevant condition for processing personal data. In practice this is unlikely to be a problem because a disclosure that meets the prejudice test for this exemption is likely to be necessary for the administration of justice, functions carried out under another law, or the functions of a government department. This provides a condition for processing personal data (schedule 2 paragraph 5) and sensitive personal data (schedule 3 paragraph 7).

47. The second principle requires that personal data is obtained for specified lawful purposes, and not then used for incompatible purposes. In many cases the data being disclosed will have been obtained for activity which is unrelated to the crime prevention and taxation purposes. If the exemption applies, the data controller can disclose the information regardless of why it is usually processed.

Example

The police ask an employer for the home address of one of its employees as they wish to find him urgently in connection with a criminal investigation. The employee is absent from work at the time. The employer had collected the employee's personal data for its HR purposes, and disclosing it for another purpose would ordinarily breach the first and second data protection principles. However, applying those principles in this case would be likely to prejudice the criminal investigation. The employer may therefore disclose its employee's home address without breaching the DPA.

Principles three, four and five

48. Taken together, these principles set out information standards data controllers must follow when processing personal data. In a data sharing context, they would usually require a data controller to take steps to ensure the quality of the data they disclose. This is likely to include checking the data is adequate for the purposes, is accurate and will have reasonable retention periods.

49. The exemption means that these requirements do not apply to a disclosure if it is necessary for the crime prevention and taxation purposes. In practice this means that a data controller making a disclosure for the relevant purposes is unlikely to have breached the DPA if the data is inadequate, excessive, inaccurate or held for too long by the receiving party.

50. The exemption from these principles only applies to the disclosing party in the context of the disclosure. It does not affect how they process the data more generally and does not apply to the data controller receiving the information.

Section 10 and section 14

51. Section 10 allows data subjects to request that their personal data is not processed in a manner that would cause them unwarranted damage or distress. This could include a request not to disclose information to a particular third party. The exemption allows a data controller to make the disclosure regardless of any s10 request that might otherwise prevent it.

General guidance on complying with s10 is available in the Guide to data protection.

52. Section 14 allows a data subject to go to court if a data controller is processing inaccurate personal data, and ask the court to order the deletion, correction or blocking of the data. The s29(3) exemption removes this option to the extent that a section 14 application in respect of the data being processed or disclosed would be likely to prejudice one of the crime prevention or taxation purposes.

More information

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

55. 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.

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

57. 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.