Disclosure of personal data

What to do if you are concerned about the way that your personal data is disclosed to third parties

The Data Protection Act 1998 is designed to protect your personal data and control how it is used by businesses, organisations or the government. It requires organisations to handle your personal data responsibly. This factsheet will outline what you can do if you are concerned about an organisation disclosing your personal data to a third party.

The UK Data Protection Act 1998 (DPA 1998) imposes various restrictions and obligations on organisations that control how and why your personal data is processed. Under the DPA, these organisations are called **data controllers**. Any organisation which retains data about you and processes it is a data controller. Processing data can be storing it on a system or having a record on an index. You can also find out whether an organisation is a data controller by asking them.

The DPA 1998 requires data controllers to handle your personal data responsibly, and this extends to who they share your personal data with, and why. They must also adhere to a set of rules called the 'data protection principles'. These principles require that data controllers ensure that the information is:

- Used fairly and lawfully
- Used for limited, specifically stated purposes
- Used in a way that is adequate, relevant and not excessive
- Accurate
- Kept for no longer than is absolutely necessary
- Handled according to people's data protection rights
- Kept safe and secure
- Not transferred outside the European Economic Area without adequate protection.

What is personal data?

Personal data is information that relates to an identified individual. The individual, however, must be alive. This catches quite a broad category of information, and includes information such as your name, address, and any identification number they may also have.

Political opinions, sexual life, medical history and conviction history fall into a different category. This category is “sensitive personal data”. There are stricter rules in relation to sensitive personal data due to their nature.

Information relating to the following are considered sensitive personal data under section 2 DPA 1998:

- race or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- sex life;
- commission or alleged commission of any offence; and,
- proceedings for any committed or alleged offence, the disposal of such proceedings, or the sentence of any court in such proceedings.

Does an organisation have to get my consent if it wants to pass my personal data to a third party?

Not necessarily. Information sharing can usually take place without your consent. In many cases where you are not asked your permission, the information sharing will be reasonable and expected. However, it should be clear why the information is being shared and who is involved.

If an organisation wants to share sensitive or confidential information, it is likely to need your consent. For example, if it wants to share information about your health.

In some cases organisations may share your personal data without you even knowing about it. This might be the case where telling you about the sharing would be likely to prejudice a criminal investigation, or prevent a vulnerable person receiving proper protection.

If you are concerned that, for example, an organisation has disclosed information about you, or that it is not keeping your information secure, then you should raise your concerns with that organisation.

How can I find out whether my personal data is being disclosed?

Your first step should be to gather all information and documents related to your concern, and then to contact the organisation and explain your concerns. Most organisations take these concerns seriously and will co-operate with you to resolve your concerns:

- You have a legal right to get a copy of the information that is held about you. This is known as a 'subject access request', and you would need to make this request to the organisation in writing (e.g. via letter or email). It can be difficult to work out how to get access to information shared by a number of different organisations. However, any of the organisations involved should be able to tell you what you need to do.
- The organisation should be able to tell you:
    - whether your personal data is being disclosed to someone else; and
    - if your personal data is being disclosed:
        (i) what information is being shared;
        (ii) who it is being shared with; and,
        (iii) the reasons for the sharing of information.
- Where the organisation that is sharing your personal data, is a public body, you can also make a request under the Freedom of Information Act 2000 for information relating to that public body's information sharing activities. This information would include, for example, their policies and procedures.

Can I stop the organisation from disclosing my personal data?

You can also ask an organisation to stop disclosing the information about you. However, this is a very narrow right. Generally, an organisation only has to comply with your request where:

- you have only objected to the sharing of your own personal data;
- the sharing causes you unjustified damage or distress; and
- you have specified why the organisation's disclosure of your personal data has this effect.

How soon can I expect a response?

The organisation must respond within 21 days of receiving your objection to the sharing of your personal data. Its response must state:

- what it intends to do and,
- if it does not intend to comply with your objection in some way, give reasons for its decision.

Can the organisation refuse to comply with my request?

Yes. Even if your request satisfies the criteria set out above, the organisation also does not have to comply with your request that they stop disclosing your personal data, if:

- you have consented to the sharing of your information;
- the disclosure is necessary:
    - in relation to a contract that you have entered into; or
    - because you have asked for something to be done so that you can enter into a contract
- the organisation needs to disclose your personal data because of a legal (not contractual) obligation that applies to it; or
- to protect your vital interests.

What if I'm not happy with the outcome?

You have two options in the event you are unhappy with your complaint to the data controller:

Option 1: Complain to the ICO

In the UK, the data protection regulator is called the **Information Commissioner's Office** (**ICO**). You can complain to the ICO if you want to stop an organisation from disclosing your data but you have not been able to prevent that disclosure.

You should report your concern to the ICO no later than three months after your last meaningful communication with the organisation. The ICO will usually ask you to confirm that you have

already contacted the organisation and received a full and final response before they will investigate your concerns.

If the ICO chooses to investigate your concern, it may give the organisation advice on how to improve its practices to resolve any concerns that you have raised. In the most severe of breaches, the Information Commissioner may also consider taking other enforcement action, like imposing a fine or bringing criminal proceedings.

You can raise a concern with the ICO here: https://ico.org.uk/concerns/handling/

Would the ICO help with my court case?

You can ask the ICO to assess if you think the organisation breached the DPA. They will not get involved in your court case, but they can write you a letter stating whether they think it is likely or unlikely that the organisation breached the DPA. You can show this letter to the judge as part of your evidence to help to build your case, but he or she may disagree with the ICO's assessment.

Can I get financial compensation?

The Information Commissioner has **no power to award you with any compensation**. If you have suffered damage or distress and wish to claim for compensation, you will need to go to court and start a legal claim.

Option 2: Take the matter to court

You can go to court to force the organisation to stop disclosing your data.

Bringing a claim in court involves a lot of time and effort and should be considered a last resort, and only in cases where you have suffered considerable damage. It will involve costs like court fees, time spent off work or travel expenses that you are unlikely to recover fully even if your claim is successful. There are also greater risks, including being ordered to your opponent's legal fees if you lose. You should not consider pursuing legal action in this area without legal representation.

The amount of compensation you may be awarded will depend largely on the circumstances of the case, including how serious the disclosure of your information was and how much of an impact it has had on you. This is particularly relevant for any compensation for distress.

If you go to court, you can claim compensation for damage or distress caused by the organisation if they have broken the law by disclosing your information. However, you only need to go to court if you cannot reach an agreement with the organisation. You do not have to go to court if the organisation has already agreed to pay you compensation.

If you have suffered financial damage as a result of the unlawful disclosure of your information, you may also be able to claim for the distress you have suffered. You may be able to claim compensation for distress alone, but this is rare, except if the organisation has broken the law in using your information for journalistic, artistic or literary purposes.

***Note*: The information in this leaflet reflects the position under the Data Protection Act 1998. From 25 May 2018, the new EU General Data Protection Regulation will come into force. The information in this leaflet may therefore need to be updated to reflect these changes to the law.**