Data protection and journalism: a guide for the media

ico.
Information Commissioner's Office

Contents

* About this guide 3

1 Practical guidance 6

Data protection basics 6

Obtaining information 9

Retaining information 11

Publication 12

Accuracy 13

Subject access requests 14

Confidential sources 16

Good corporate practice 17

2 Technical guidance 18

Data protection and freedom of expression 18

An overview of the DPA 21

The journalism exemption 27

The first principle: fairness 40

The seventh principle: security 42

The section 55 offence 43

3 Disputes 46

Role of the ICO 46

Complaints to the ICO 47

ICO enforcement powers 49

Court claims 51

About this guide

In brief...

This guide explains how the Data Protection Act (DPA) applies to journalism, advises on good practice, and clarifies the role of the Information Commissioner's Office (ICO). It does not have any formal legal status and cannot set any new rules, but it will help those working in the media understand and comply with existing law in this area.

Purpose of the guide

In the report of the Leveson Inquiry into the culture, practices and ethics of the press, Lord Justice Leveson recommended that the ICO:

> "should take immediate steps, in consultation with the industry, to prepare and issue comprehensive good practice guidelines and advice on appropriate principles and standards to be observed by the press in the processing of personal data."

This guide responds to that need. It explains how the DPA applies to journalism. It sets out the basic principles and obligations, advises on good practice, and clarifies how an exemption for journalism works to protect freedom of expression. It also explains what happens when someone complains, and the role and powers of the ICO.

It is intended to help the media understand and comply with data protection law and follow good practice, while recognising the vital importance of a free and independent media. It highlights key data protection issues, and also explains why the DPA does not prevent responsible journalism.

This guide is not intended to take the place of industry codes of practice. It is a guide to data protection compliance, not to wider professional standards or media regulation. It does however refer to existing codes, where directly relevant, to show how everything fits together.

Status of the guide

This guide does not have any formal status or legal force. It cannot and does not introduce any new rules or new layers of regulation. It is the DPA itself that places legally enforceable obligations on the media. This guide simply clarifies the ICO's view of the existing law as set out in the DPA. It is intended to help those working in the media to understand fully their obligations, and to promote good practice.

Following this guide will help to ensure compliance, but the guide itself is not mandatory. There are no direct consequences simply for failing to follow guidance, unless this leads to a breach of the DPA.

The guide sets out our interpretation of the law and our general recommended approach, but decisions on individual stories and situations will always need to take into account the particular circumstances of the case.

Who this guide is for

The guide is intended for media organisations involved in journalism – including the press, the broadcast media, and online news outlets. With this in mind, its focus is specifically on journalism and those working in the media.

The guide is aimed primarily at senior editors or other staff with compliance or training responsibilities. Staff journalists might find some parts of the guide useful – but as legal responsibility under the DPA will usually fall on their employer, not all of the technical detail will be relevant. Journalists might therefore find it easier to start with our separate quick guide.

Much of the guide will also be relevant to freelance journalists, who are likely to have their own responsibilities under the DPA.

Non-media organisations publishing material may also find parts of the guide useful. Please note, however, that the guide is not intended to be a comprehensive text on all aspects of freedom of expression or its interaction with the DPA. We may produce separate guidance for other types of organisation in future, if we think it would be helpful.

Separate guidance for members of the public on their data protection rights in relation to journalism is available on our website.

How to use the guide

The guide is split into three main sections, each with a different focus. Each section can be read separately, although links between them are provided where appropriate.

Section 1 (Practical guidance) introduces some data protection basics and provides broad guidelines on the effect of the DPA on key areas. It expands on our "Data protection and journalism: a quick guide". This section is likely to be of interest to anyone working in the media.

Section 2 (Technical guidance) gives an overview of the DPA, with more detail on how we interpret the exemption for journalism and some of the other key legal provisions. This section is aimed at those with particular data protection compliance responsibilities, who want a more detailed understanding of what the DPA says. It is addressed largely to organisations, but much of the advice will also be relevant to freelance journalists.

Section 3 (Disputes) sets out the role of the ICO, and what happens if someone complains under the DPA. This will be of most interest to senior editors or staff responsible for data protection compliance.

More information

The Guide to Data Protection gives a general overview of the main provisions of the DPA. More detailed guidance on various aspects of data protection is also available on the guidance pages of the ICO website.

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

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.

1 Practical guidance

This section introduces some data protection basics and sets out our general recommended approach to key areas (although decisions in individual cases will always need to take account of the particular circumstances of the case). It expands on our quick guide for journalists. This section is likely to be useful for anyone working in the media, including editors, compliance staff, journalists, freelancers and producers.

The media will often need to deviate from some or all aspects of this approach when it is not viable in the context of journalism and in these scenarios the media can consider relying on the section 32 exemption. Section 2 offers more detail and outlines when and how the exemption for journalism, art and literature can be applied.

Data protection basics

In brief...

The Data Protection Act (DPA) applies whenever anyone collects, retains, uses, or discloses any information about a living person. It does not prevent responsible journalism, as the main principles are flexible enough to accommodate day-to-day journalistic practices, and there is also a specific exemption to protect journalism where necessary. However, the media are not automatically exempt and will need to ensure they give some consideration to the data protection rights of individuals.

Legal responsibility usually falls on the relevant media organisation rather than individual employees, although freelance journalists are likely to have their own separate obligations. Employees of media organisations will need to be aware of their DPA responsibilities, particularly day to day adherence, when working for their employer. The references to "you" in this section are to anyone working in a media organisation.

Some data protection myths

Myth: the DPA doesn't apply to the media.

Reality: the DPA applies to any organisation handling information about people. There is an exemption to protect journalism, but this does not give an automatic blanket exemption from the DPA.

Myth: the DPA only covers 'private' information.

Reality: any information about someone can be personal data – even if it's in the public domain or is about someone's public role. (But the DPA takes account of whether such information is already public.)

Myth: the DPA bans the disclosure of personal data.

Reality: the DPA does not ban the disclosure of personal data and has very few hard and fast rules. In general, the key is to consider what's justified in the circumstances.

Myth: the DPA always requires consent.

Reality: you can use information without consent – or even against a person's express wishes – if there are good reasons to do so.

Myth: the DPA sets time limits on keeping information and says we have to delete our contacts.

Reality: there are no set time limits. You can hold information for as long as you need to, but you shouldn't keep things you don't need. The DPA does not say you have to delete your contacts.

Myth: the DPA says we should reveal our sources.

Reality: the DPA can protect the privacy of sources.

Myth: we can't do anything unless we're exempt.

Reality: as a general rule, you will comply with the DPA if you are fair, open, honest, handle information responsibly, and don't cause unnecessary harm. You will not need the exemption in every case.

Myth: the ICO will dictate what's in the public interest.

Reality: you decide whether publication is in the public interest. The ICO does not have to agree, as long as your decision is reasonable.

When does the DPA apply?

The scope of the DPA is very wide. It applies to the processing of personal data. Broadly speaking, this means that anyone – including the media – must comply if they handle information about people. This includes information about employees, customers, contacts, sources, or people you are investigating or writing about.

It's important to emphasise that the DPA will not prevent responsible journalism, but the media cannot ignore data protection altogether, and will need to be aware of the main principles and comply with them wherever possible.

Section 2 addresses in greater detail when the exemption for journalism, art and literature will apply and how compliance with the DPA will be affected when it is relied upon.

What does the DPA say?

The DPA sets out a framework of rights and duties, that are designed to balance an individual's right to information privacy against the legitimate needs of others to collect and use people's details (including for the purposes of journalism and freedom of expression).

There are very few hard and fast rules. Instead, the DPA is based around eight common-sense principles, which are flexible enough to accommodate most responsible day-to-day journalistic practices. The key is to act fairly and proportionately, and avoid causing unwarranted harm.

The act includes a number of exemptions, notably an exemption to protect processing for the purposes of journalism, art and literature where necessary – but this does not mean the media are automatically exempt from the DPA as a whole.

Legal responsibility under the DPA will usually fall on the relevant media organisation rather than individual employees, although freelance journalists are likely to have their own obligations. However, individual journalists should be aware that they can be guilty of a criminal offence if they obtain information unlawfully in breach of section 55. There is currently no specific exemption from this section for journalists, though there is a public interest defence.

See section 2 for more detail on specific provisions of the DPA, including the exemption and the section 55 offence.

Obtaining information

Key points:

- Be open and honest wherever possible. People should know if you are collecting information about them where it is practicable to tell them. We accept that it will not generally be practicable for journalists to make contact with everyone they collect information about.
- You do not need to notify individuals if this would undermine the journalistic activity. This will be a trigger to consider the section 32 exemption.
- Only use covert methods if you are confident that this is justified in the public interest.
- Only collect information about someone's health, sex life or criminal behaviour if you are confident it is relevant and the public interest in doing so sufficiently justifies the intrusion into their privacy.

Much of the information you collect will include some personal data. The act of obtaining it counts as 'processing' and is therefore covered by the DPA.

The DPA expects you to collect information in a fair way. In practice, this means:

- a journalistic justification for collecting the information,

- where practical, telling the person you are collecting the information from, and the person the information is about (if different), who you are, and what you are doing with their information,
- only using someone's information as they would reasonably expect.

We understand you will not always want to notify individuals that you are investigating them. You will need a valid reason to do this, and the justification should reflect the privacy intrusion. We recognise that notifying individuals can be impractical or undermine the journalistic activity. This can be enable the section 32 exemption to be considered but you should always consider whether notification is possible, and at different stages of the story or investigation.

If you do need to use undercover or intrusive covert methods to get a story, such as surveillance, you may do so if you reasonably believe that these methods are necessary (in other words it is not reasonably possible to use a less intrusive way to obtain the information) and the story is in the public interest. To establish whether covert investigation is justified in the public interest, you must balance the detrimental effect that informing the data subject would have on the journalistic assignment against the detrimental effect employing covert methods would have on the privacy of any data subjects. The importance of the story, the extent to which the information can be verified, the level of intrusion and the potential impact upon the data subject and third parties are all relevant factors. Section 2 explains how the exemption for journalism might apply in relation to obtaining information.

Even if covert investigation can be justified, you should still consider whether you can inform the data subject about the information collected once it has been gathered.

The DPA gives more protection to some categories of information that it classes as sensitive. In particular, you should ensure you have an appropriate public interest justification before collecting information about someone's health, sex life or allegations of criminal activity. See section 2 on the 1st Principle, for more detail.

Although there is a broad exemption for journalism from many provisions of the DPA, this does not exempt you from prosecution under section 55. It is an offence if you knowingly or recklessly obtain personal data from another organisation without its consent (eg by blagging, hacking or other covert methods). There is a public interest defence to this offence, but currently this holds you to a stricter standard than the usual exemption for journalism. You should therefore be confident about your public interest justification before using such methods.

Other organisations may be able to provide you with information about someone without breaching the DPA, if they are satisfied that the disclosure is lawful, sufficiently justified in the public interest, and would be fair and meet the 'legitimate interests' condition. If the information in question is sensitive personal data, there is a specific condition to allow a public interest disclosure to journalists if it is related to wrongdoing or incompetence but otherwise the person disclosing the information would need to be satisfied that one of the conditions for processing sensitive personal data applies.

If the organisation in question does not agree with your view of the public interest, or has other overriding legal, professional or reputational reasons to refuse to disclose the information to you, the DPA cannot oblige them to supply you with information.

Retaining information

Key points:

- The DPA does not stop you keeping useful information, as long as it was obtained legitimately.
- Review retained information from time to time to ensure that it is still up to date and relevant, and delete any you no longer need.
- Organisational policies should specify whether certain categories should be reviewed more regularly eg very sensitive types of information or information relating to children.
- Take reasonable steps to retain people's information securely and prevent it being lost, stolen or misused.

Research and background materials

Contact details and background research are a vital journalistic resource, and you are likely to want to keep them for long periods or indefinitely, even if there is no specific story in mind at present. But you are 'processing' personal data just by keeping it, so you must comply with the DPA.

The DPA does not impose a time limit on how long you can retain personal data, and in some cases it will be reasonable to keep certain information indefinitely. However, you should review your retained information from time to time to ensure that the details are still up to date, relevant and not excessive for your needs, and you should delete any details which you no longer need (eg if a contact has changed their number). How retained information is reviewed should be set out in organisational policies.

Security

You must keep information about people secure. This means you must take reasonable steps to stop it being lost, stolen or misused. You are not exempt from these security obligations.

You should be particularly aware of security when out of the office with documents, phones or laptops containing personal data. All staff should be aware of, and follow, the organisations policies and procedures. Information should be locked, password protected and encrypted where possible.

Serious security lapses can result in a civil monetary penalty from the ICO.

Security policies and procedures need to take into account the fast-paced nature of the media industry and all the different types of portable media that could be used to record information, including, for example, notebooks, mobile telephones, dictation machines, tablets, laptops and memory sticks. More information on security can be found in the ICO's Guide to Data Protection.

Publication

Even where information has been fairly obtained and retained, you will need to consider separately what information it is fair to publish. This question means determining how much personal data it is necessary to publish to properly report the story, balanced against the level of intrusion into the life of the data subjects, and the potential harm this may cause.

For instance, if a story would be highly intrusive or harmful then it is less likely to be fair to publish personal data. This is also the case with stories

with little obvious public interest, or where publication should have been delayed to verify facts.

The public interest in publication should be considered by someone at an appropriate level depending on the story. We recognise that senior editorial or expert input will usually not be needed for day-to-day stories.

Publication is likely either to be fair and to comply with the DPA or to fall within the journalism exemption if it can be shown that someone at an appropriate level considered whether the public interest in publication outweighed individual privacy in the circumstances of the case and can give good reasons for this view when challenged.

We recognise the inherent public interest in journalism is always relevant however it cannot on its own always justify a story. In section 2 we explain why each story will need to be considered on a case-by-case basis.

Online archives

The exemption for journalism can apply to the retention and publication of a full online news archive. Where possible, stories that are later shown to be inaccurate or unfair should be linked to subsequent corrections.

Accuracy

Key points:

- Take reasonable steps to check your facts.
- If the individual disputes the facts, say so.
- Distinguish clearly between fact, opinion and speculation.

Accuracy is, of course, at the very core of a professional journalist's work, and features at the heart of industry codes of practice.

The DPA requires you to record details correctly and take reasonable steps to check your facts. You should also clearly distinguish between fact and opinion and if the individual disputes the facts you should say so.

Responsible journalists will always take care to ensure reports are accurate and not misleading, which means you should be able to comply

in the vast majority of cases. We would not expect you to fall back on the exemption very often, as it is hard to argue it is in the public interest to publish clearly inaccurate stories or to retain clearly inaccurate information without making reasonable checks. However, the exemption may be available if, for example, the story is urgently in the public interest and the short deadline makes a complete accuracy check very difficult. As with any use of the exemption, you will still need to show that proper thought was given by someone at an appropriate level to what checks might be possible, whether publication could be delayed for further checks, the nature of the public interest at stake and that the decision to publish was, therefore, reasonable.

Subject access requests

Key points:

- Ensure you have a process in place for handling subject access requests.
- Always consider whether you can provide the information (or some of it) without undermining your journalistic activities.
- If you decide you cannot comply with a request or you can only comply in part, record your reasons.
- You can redact information about third parties, including individual sources, as long as it is reasonable to do so.

If someone makes a written request to find out whether you hold information about them, what information you have, where you got it, what you are doing with it, or asks to see copies, you must consider whether you can comply with their request.

This is commonly known as a subject access request or SAR, and you must respond promptly and at least within 40 calendar days. You should not charge more than £10 for doing so.

More information on subject access can be found in the ICO's Guide to Data Protection.

You may be able to rely on the journalism exemption to refuse the request if you hold the information in connection with the publication of a story that is in the public interest, and you believe responding to the SAR would be incompatible with journalism. However, you are not

automatically exempt. If you can provide the information (or some of it) without undermining your journalistic activities, you should do so.

In practice, this means that when you receive a SAR you will need to give thought to whether you can respond, and how much information you can provide. If you decide you cannot comply with the request and the individual complains about your decision, we may ask you to show that you considered the request, and to explain why you thought providing the information would undermine journalism. As with other areas where the exemption might apply, you will need to be able to show you have a process for considering requests, and clear reasons for the decision you make.

The exemption can apply to SARs made before or after publication of a story. You may be able to justify rejecting a SAR made before publication, for example, if providing the information would undermine the story by tipping someone off to forthcoming publication. You may still be able to use the exemption after publication if you can explain why responding would undermine future investigations or publications, or journalistic activities more generally. The resource implications of compliance with a particular SAR (both financial and human) may be relevant factors, but only if they can be shown to be such as to genuinely frustrate the journalism. However, resources cannot justify a blanket policy of rejection of all SARs including those with minimal human or financial impact.

We would always expect you to take the timing of the SAR into account when considering whether you can respond. Even if you have rejected a similar request in the past a significant passage of time and the extent of publication since the previous request may mean that you should consider afresh whether compliance is still incompatible with journalism. Even if you decide that you cannot provide copies of all the information, you should still consider whether you can partially comply by providing some of the information, or a description of the information, or even just confirming whether or not you hold some information.

You do not have to comply with a SAR by providing a copy of the information in permanent form if this would be impossible or would involve disproportionate effort. However, you still have to comply with the request in a different manner, for example by allowing inspection of the data, unless an exemption applies.

Remember that even if you do answer the request, you do not have to include any information about other people unless they have consented, or it is reasonable to supply it without their consent. For detailed

information on the right of subject access and general advice on responding to requests, see our Subject access code of practice.

Confidential sources

Key points:

- Where a source is an individual or individuals the DPA requires you to protect their identities.
- You can remove the identities of individuals who are sources in response to a subject access request, as long as it is reasonable to do so.

Journalists will naturally want to protect the identity of their confidential sources. Concern is likely to arise when the subject of a story makes a subject access request to see the information you have on them and this would reveal a source.

The DPA allows you to redact the identity of individuals who are sources in this situation. You only have to disclose information about individuals who are sources (or anyone else identified in the information) if that individual consents, or if it is reasonable to do so. In most cases, it is unlikely to be reasonable to disclose information about individuals who are confidential sources.

Where the source is an individual or individuals, there is no need to use the exemption or to rely on the public interest to withhold their identities as the DPA already provides for this.

The identity of your source may itself be personal data. If so the DPA actually requires you to keep it secure, and any disclosure must be fair and lawful. It is unlikely to be fair or lawful to disclose information about confidential sources in many cases.

If your source is an organisation, not an individual, you will need to rely upon the journalism exemption to withhold its identity if it is not appropriate to disclose it.

Good corporate practice

Larger organisations with a positive approach to data protection are likely to have the following indicators of good practice:

Training

All staff are given basic data protection training. Journalists are trained to recognise significant data protection issues and to raise their concerns with the appropriate person at their organisation with responsibility for data protection compliance. More detailed training is provided to editorial staff.

Guidance

Data protection is embedded in any general guidance on compliance or standards. A dedicated data protection page is available to staff on the organisation's intranet with links to specific data protection guidance, policies and procedures, and who to contact for further advice.

Data protection experts

There are data protection experts within the organisation who can give detailed case-by-case advice when required.

Corporate governance

Data protection is embedded in existing journalistic or editorial decision-making processes and legal checks, rather than being considered an add-on. There is a suitably senior management figure with overall responsibility for data protection compliance.

2 Technical guidance

This section gives an overview of the Data Protection Act (DPA), with more detail on how we interpret the underlying legal provisions – and in particular the s32 exemption for journalism.

This section is aimed at those with some specific data protection compliance responsibilities, who want a more technical understanding of what the DPA says and how to apply particular provisions. It is addressed primarily to media organisations and freelance journalists. This level of detail is likely to be of less use to staff reporters.

Data protection and freedom of expression

In brief...

The right to respect for privacy and the right to freedom of expression are both important rights, and neither automatically trumps the other. The DPA protects people's information privacy, but also recognises the importance of freedom of expression, aiming to strike a fair balance.

The ICO must consider the importance of freedom of expression when deciding how best to use its powers in the public interest.

Convention rights

Any guidance in this area must recognise and respect the underlying rights at stake: the right to respect for privacy and the right to freedom of expression.

Both rights are considered fundamental to our democratic society. They are both enshrined in the European Convention on Human Rights (ECHR) and incorporated into UK law via the Human Rights Act 1998 (HRA).

Article 8 of the ECHR sets out the right to respect for privacy:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 10 sets out the right to freedom of expression:

> (1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent states from requiring the licensing of broadcasting, television or cinema enterprises.
>
> (2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

The HRA requires that other laws, including the DPA, must be interpreted to give full effect to these rights wherever possible. It is also unlawful for the ICO as a public authority to act in breach of these rights (unless that is the result of the ICO fulfilling some other legal obligation). This means that the ICO must respect and protect freedom of expression as well as upholding the privacy of individuals. We will always consider the importance of freedom of expression and the inherent public interest in journalism and the maintenance of a free press in our interpretation of the DPA and when we decide how to use our powers in the public interest.

Neither of these rights – privacy or freedom of expression - is absolute. The ECHR makes clear that it can be legitimate to restrict freedom of expression to protect other rights, including privacy rights – just as it can be legitimate to interfere with someone's privacy to protect freedom of expression. Proportionality is the key issue.

Both privacy and freedom of expression are of special importance in a democratic society, and they have equal status. A fair balance must be struck if they conflict. Where the balance lies in any one case will depend on the particular circumstances of that case.

The right to respect for private and family life (article 7), the right to the protection of personal data (article 8) and the right to freedom of expression (article 11) are all fundamental rights under the Charter of Fundamental Rights of the European Union. This is relevant to the interpretation and application of the DPA, which is derived from a European Directive.

Freedom of expression in the DPA

Data protection law grew from concerns about protecting individual privacy, but it is also about ensuring economic and social progress. Its aim is not to ensure privacy at all costs, but to strike a fair balance between individual privacy and the wider interests of society.

The balance with freedom of expression in particular is explicitly recognised in Article 9 of European Directive 95/46/EC (the data protection directive on which the DPA is based):

> "Member states shall provide for exemptions… for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression."

This is the basis for the exemption to protect journalism, art and literature in section 32 of the DPA, which is specifically designed to protect freedom of expression. In accordance with the directive, it does not give an automatic blanket exemption in every case. It is only intended to apply where necessary to strike a fair balance – but it is still one of the broadest exemptions available.

The DPA also restricts the powers of the ICO in regulating the media, and ensures additional safeguards and points of appeal. The ICO will always consider the importance of freedom of expression – and specifically, a free and independent media – when deciding how best to use its powers in the public interest, in line with its obligations under the HRA. See Section 3 below for more information on the role of the ICO in cases involving the media.

Privacy in industry codes of practice

We also recognise that this same balance between privacy and freedom of expression is already reflected in industry codes of practice such as The Editors' Code of Practice, The Ofcom Broadcasting Code and the BBC Editorial Guidelines. Each of those codes prescribes an appropriate balancing test for decision making on invasions of privacy.

Factors which will help ensure you strike a fair balance – including public interest tests and definitions for fairness, openness and accuracy – are to be found throughout these codes.

We would therefore emphasise that if you comply with industry codes, this will go a long way to ensure you also comply with the DPA.

An overview of the DPA

In brief...

Organisations (or self-employed individuals) who handle any information about people will usually need to notify the ICO and comply with eight common sense principles. The principles cover fairness, transparency, quantity, accuracy, time limits, individuals' rights, security, and international transfers. There are exemptions available in some circumstances, including an exemption to protect journalism.

It is a criminal offence to obtain, disclose or procure personal data from another data controller without its consent. There is no specific exemption for journalists to this offence, but there is a public interest defence.

Definitions and key terms

What is 'personal data'?

The definition in the DPA is complicated but in essence, personal data is:

- any information about an identifiable living person
- which is (or will be) stored on a computer or other digital device, or filed in an organised filing system where it can be easily found.

This means the DPA covers a very wide range of information. Note that information does not have to be 'private' to be personal data. Anything about a person can be personal data, even if it is innocuous or widely known. For example, a public figure's job title can be personal data, as can a photograph taken in a public place, a listed phone number, or information posted online. Obviously the use of publicly available personal data is less restricted. Personal data is not limited to hard facts: someone else's opinions about a person, or intentions towards them, can also be personal data.

The DPA does **not** cover anonymised records, information about deceased persons, or unstructured paper records (eg unstructured handwritten notebooks). However, information in notebooks is covered if it will be transferred to a computer or filing system at a later date.

The DPA does not cover truly anonymised information, but this does not mean that information is only personal data if the person is named. It will be personal data if they can be identified in any other way – for example, from their image, description, or address. It will also be personal data if they can be identified by cross-referencing with other information (including written notes) you hold.

For more information and links to our detailed guidance on this topic, see The Guide to Data Protection.

Sensitive personal data

The DPA designates some types of information as 'sensitive personal data'. This is information about:

- race or ethnic origin
- political opinions
- religious beliefs
- trade union membership
- health
- sex life
- criminal activity or allegations
- criminal proceedings

There is no outright ban on using sensitive personal data, but there are more restrictions and it must be treated with extra care. As journalism often involves this type of information, this is an area where the media may need to invoke the section 32 exemption for journalism.

What counts as 'processing'?

Almost anything counts as 'processing'. Collecting, using, keeping, publishing, or discarding – all these are 'processing'. It is difficult to think of something you might do with data that would **not** count as processing.

The definition in the DPA specifically includes obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, aligning, combining, blocking, erasing or destroying data.

Other key terms

In this guide we have tried to avoid using legal jargon as far as possible. However, in some circumstances you will need to understand the technical meaning of a term defined in the DPA. The key terms are:

- **Data controller** – the person who decides why and how personal data is processed. This is usually an organisation, but can be an individual if they are acting on their own initiative – for example, a blogger or freelance journalist. It is the data controller who is responsible for complying with the DPA. If two data controllers work together, they can be jointly responsible.
- **Data processor** – someone the data controller instructs to process data on their behalf - usually a subcontractor. (Employees are part of the data controller rather than separate data processors.)
- **Data subject** – the individual the personal data concerns.
- **Third party** – someone else who's not the data controller, its employee, a data processor, or a data subject.
- **Special purposes** – journalism, art or literature.

See The Guide to Data Protection for more information and precise definitions as they appear in the DPA.

The duty to notify

Most organisations processing personal data will need to notify with the Information Commissioner, who keeps a public register. There is a fee. Failure to notify is a criminal offence.

Private individuals and some organisations (generally very small businesses or not-for-profits) are exempt from notification, but the media are not generally exempt. The exemption for journalism does not apply to the obligation to notify.

For more information on how to notify, see our guidance pages and the register your organisation page on our website.

The data protection principles

The key to the DPA is to comply with the eight data protection principles. These principles apply to all processing (unless an exemption applies). There are very few hard and fast rules – organisations will need to judge how they apply to each case.

This section gives a brief overview of the principles. For a full discussion and links to more detailed guidance, see The Guide to Data Protection. Bear in mind that although these principles provide the basic starting point, an exemption will be available in some cases. For more practical advice on how the DPA as a whole applies to key issues in practice, see Section 1.

Principle 1: Fairness

Personal data must be collected and used fairly and lawfully, without causing unjustified harm or intrusion into someone's private life. You must also meet one of six listed conditions (and an additional condition if it's sensitive personal data).

This is a key principle - see the separate section on the first principle for more detail.

Principle 2: Transparency (specified purposes)

You must be clear why you are collecting personal data and what you intend to do with it, and you can't later use it for a different and unexpected purpose. In the context of journalism, this means you

shouldn't use information for non-journalistic purposes. However, you can still reuse information for other stories in future, or keep it as a general journalistic research archive.

Principle 3: Quantity

Personal data must be adequate, relevant, and not excessive for your purposes. In other words, you must have enough information to do the job, but shouldn't have anything you really don't need. Note that this principle takes account of your purpose. As the nature of journalism requires the collection and cross-referencing of large volumes of information, we accept that information without immediate relevance to a current story can be justifiably retained for future use if it relates to a person or subject of more general journalistic interest.

Principle 4: Accuracy

Personal data must be accurate and, where necessary, up to date. In practice this means you must take reasonable steps to ensure your facts are correct and not misleading, and if the individual disputes any facts you should investigate and reflect their view. What steps are reasonable will depend on the circumstances, including the urgency of the particular story.

See also the practical guidance section on accuracy for further guidelines in this area.

Principle 5: Time limits

Personal data must not be kept for longer than necessary. The key point is to actively consider how long you are likely to need information for, and to review it periodically. There's no fixed time limit, and we accept in the context of journalism it is likely to be necessary to keep some information for long periods.

Principle 6: Individuals' rights

Subject to exemptions, you must comply with people's rights:

- to access a copy of their personal data (subject access). See the practical guidance section on subject access requests for more information,

- to object to processing likely to cause damage or distress. Note that this is not a right to prevent processing, just a right to ask you to stop. You must reply within 21 days either agreeing to stop, or else explaining why you think the request is unjustified,

- to opt out of direct marketing. If you receive a written request to stop (or not to begin) using personal data for marketing, you must stop within a reasonable period, and

- to object to automated decisions (ie decisions by computer). This is unlikely to be relevant in the context of journalism.

Principle 7: Security

You must have appropriate security to prevent personal data being accidentally or deliberately compromised (eg stolen, lost, altered or misused). You cannot rely on the journalism exemption to avoid security obligations.

See the separate section below on the seventh principle for more detail.

Principle 8: International transfers

You should not send personal data to anyone outside the European Economic Area (EEA) without adequate protection. What counts as 'adequate protection' will generally depend on the nature of the information, the purpose of the transfer and the legal position at the other end, among other things.

This principle will not prevent online publication, even if this makes information available outside the EEA. If publication complies with the DPA in other respects (or is exempt as being in the public interest), it will be appropriate to publish it to the world at large.

Exemptions

The principles are designed to be flexible enough to cover most situations, but there are a number of specific exemptions to accommodate special cases. For example, there are exemptions to protect:

- national security
- criminal investigations
- regulatory functions
- public registers
- disclosures required by law
- legal advice and proceedings

- confidential references
- management planning
- negotiations
- journalism, art and literature
- research
- domestic purposes

The detail of the exemptions can be complicated, and they work in different ways. As a general rule, they only exempt you from the DPA to the minimum extent necessary to protect the relevant interests. In other words, you must consider each case on its own merits and can't rely on a blanket policy. Most exemptions only exempt you from some of the provisions (most commonly, to allow you to use information without the data subject's knowledge, or to allow you to disclose it to a third party) – but the exemption for journalism, art and literature is one of the broadest exemptions, and can exempt you from many of the DPA's provisions. Even so, it only works on a case-by-case basis and does not give a blanket exemption from compliance.

The next section considers the journalism exemption in detail. For more information on the other exemptions, see The Guide to Data Protection.

The journalism exemption

In brief...

The exemption protects freedom of expression in journalism, art and literature. The ICO must interpret it broadly to give proper protection to freedom of expression but we will also expect organisations to be able to justify why the exemption is required on the merits of each case. The law does not provide journalists with an automatic exemption.

Your only purpose must be journalism (or art or literature), and you must be acting with a view to publication. You must reasonably believe publication is in the public interest – and that the public interest justifies the extent of the intrusion into private life. You must also reasonably believe that compliance with the relevant provision is incompatible with journalism. In other words, it must be impossible to comply and fulfil your journalistic purpose, or unreasonable to comply in light of your journalistic aims, having balanced the public interest in journalism against the effect upon privacy rights.

Organisations will find it easier to rely on the exemption if they can show robust policies and procedures, compliance with any relevant industry

codes of practice, good internal awareness of the DPA, and appropriate record keeping for particularly controversial decisions.

Introduction

Section 32 sets out the exemption for journalism. Its purpose is to safeguard the right to freedom of expression as set out in Article 10 of the ECHR. It covers the 'special purposes' of journalism, art and literature – although this guide focuses primarily on journalism.

The scope of the exemption is very broad. It can disapply almost all of the DPA's provisions, and gives the media a significant leeway to decide for themselves what is in the public interest. Media organisations must be able to justify their actions in the public interest and on the merits of each case.

Even if publication is clearly in the public interest, this still doesn't mean the media can ignore the DPA altogether: if you can reasonably comply, you must. This is why it's important that those working in the media understand the basics of data protection.

There are a few provisions that are not covered by the exemption and will always apply. See below for guidance on What is not exempt.

The exemption breaks down into four elements:

(1) the data is processed only for journalism, art or literature,
(2) with a view to publication of some material,
(3) with a reasonable belief that publication is in the public interest, and
(4) with a reasonable belief that compliance is incompatible with journalism.

The focus will usually be on elements three and four. In essence, there should be a reasonable argument that the public interest justifies what would otherwise be a breach of the DPA.

(1) Only for journalism

> "**32.**—(1) Personal data which are processed only for the special purposes are exempt from any provision to which this subsection relates if—…"

The special purposes are defined in section 3 as: "(a) the purposes of journalism, (b) artistic purposes, and (c) literary purposes".

Journalism, art and literature are interpreted broadly. This will include most of the day-to-day business of media organisations, and may also cover some activities of others (eg citizen bloggers or civil society groups) although this guidance is intended for media organisations.

What is journalism?

There is no definition of journalism in the DPA itself. Taking into account its everyday meaning and the underlying purpose of protecting freedom of expression, we consider that it should be interpreted broadly.

This is in line with the European Court of Justice's ruling in the *Satamedia* case (Case C-73/07), which found that the reference to journalism in the European data protection directive should be interpreted broadly and covered the disclosure to the public of information, opinions or ideas by any means.

Journalism will clearly cover all output on news, current affairs, consumer affairs or sport. Taken together with art and literature, we consider it is likely to cover everything published in a newspaper or magazine, or broadcast on radio or television – in other words, the entire output of the print and broadcast media, with the exception of paid-for advertising.

This accords with the Supreme Court's decision in *Sugar (Deceased) v BBC* [2012] UKSC 4, which found that 'journalism, art or literature' would cover the whole of the BBC's output to inform, educate or entertain the public. (This was a case about the Freedom of Information Act, but the court drew a direct and explicit parallel with the words in the DPA.)

> **Example**
> *Top Gear* was originally a consumer programme about cars. This would count as journalism. When the format was changed to an entertainment programme, it "moved from the pigeonhole of journalism to that of literature", but would still be covered. (Lord Walker, at paragraph 70 of the *Sugar* case.)

The Supreme Court also confirmed that journalism would involve a wide range of activities, loosely grouped into production (including collecting, writing and verifying material), editorial, publication or broadcast, and management of standards (including staff training, management and supervision).

In short, the exemption can potentially cover almost all information collected or created as part of the day to day output of the press and broadcast media, and comparable online news or current affairs outlets.

However, advertising revenue, property management, financial debt, circulation, or public relations would not usually be considered as journalism.

Citizen bloggers

We accept that individuals may be able to invoke the journalism exemption if they are posting information or ideas for public consumption online, even if they are not professional journalists and are not paid to do so.

> **Example**
> In *The Law Society and others v Kordowski* [2011] EWHC 3182 (QB), the High Court looked at a website set up by an individual to name and shame 'solicitors from hell'. The court was clear that a private individual can engage in internet journalism:
>
> "Journalism that is protected by s32 involves communication of information or ideas to the public at large in the public interest. Today anyone with access to the internet can engage in journalism at no cost. If what the Defendant communicated to the public at large had the necessary public interest, he could invoke the protection for journalism and Article 10."

Of course, this doesn't mean that every blog or comment posted online will be journalism. In many cases, people will simply intend to take part in normal social interaction or other recreational internet use. Individuals posting personal blogs or comments online that were not intended as public interest journalism might instead be able to rely on the domestic purposes exemption in section 36. See our guidance on social networking and online forums for more information.

Non-media organisations

We also accept that non-media organisations may be able to invoke the exemption. If their purpose in processing the specific information is to publish information, opinions or ideas for general public consumption, this will count as a journalistic purpose – even if they are not professional journalists and the publication forms part of a wider campaign to promote

a particular cause or achieve a particular objective. However, the information must be used only for publication, and not for the organisation's other purposes.

Processed 'only' for the special purposes

The exemption covers information processed **only** for journalism, art or literature. In other words, if an organisation is also using the same information for any other purpose, the exemption cannot apply.

In our view this is not likely to be an issue for the press or broadcast media or comparable online media outlets, as their whole purpose is journalism, art or literature and they are unlikely to have any other overlapping purpose for journalistic information.

It is more likely to be relevant to non-media organisations seeking to rely on the exemption. Such organisations will inevitably have other purposes apart from journalism, art or literature. However, the focus here is on what the specific information in question is being used for, rather than the purposes of the organisation as a whole. The exemption can still apply if the particular data is collected and used with the exclusive aim of disseminating some information, opinions or ideas to the public. However, if it is also used for the organisation's other purposes – eg in political lobbying or in fundraising campaigns – the exemption will not apply.

(2) A view to publication

> "(a) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material…"

The information must be used with a view to publication of journalistic material. This doesn't mean the organisation must be aiming to publish the personal data in question at that time for that particular story. Personal data can be retained with a view to it being used in a different story or in updating a story that has been already published. As long as the ultimate aim is to publish a story (or for someone else to publish it), all the background information collected, used or created as part of a journalist's day-to-day activities could also be exempt, even if those details are not included in any final article or programme – and even if no story is actually published or broadcast.

In this context, 'publish' means 'make available to the public or any section of the public'.

As long as the information was originally collected and used with the ultimate aim of publication, the exemption can protect the media both before and after publication. This follows the approach of the Court of Appeal in *Campbell v MGN Ltd* [2002] EWCA Civ 1373. The court was also clear that the act of publication itself can be exempt. This was because the relevant 'processing' here is not taken to be each processing operation in isolation (eg collection, use, or publication), but the end-to-end process involved in publishing journalistic material. For this reason, we accept that the exemption can apply to retention and re-use of information even after publication. This is an inevitable part and parcel of the journalistic process.

In short, this means that the exemption can potentially cover any information collected, created or retained as part of a journalist's day-to-day activities, both before and after publication. However, the exemption cannot apply to anything that is not an integral part of the newsgathering and editorial process. For example, information created in response to a complaint about a particular story after publication is unlikely to be processed with a view to publication.

(3) In the public interest

> "(b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest …"

The DPA puts the onus on the media to make their own independent decisions on whether publication is in the public interest, as long as those decisions are reasonable. However, we will expect organisations to be able to explain their reasons for believing publication is in the public interest, and to show that there was an appropriate decision-making process.

What is the public interest?

There is no definitive public interest test. Whether and how something is in the public interest, and, if so, how strong that public interest is, will

differ from case to case. Comparable material published in the past will be relevant, but it cannot be assumed that something is acceptable because similar information has been published before. Each case must be considered on its own merits.

Any consideration of the public interest should ultimately aim to strike an appropriate balance between freedom of expression and privacy rights. We advise organisations to take into account:

- the general public interest in freedom of expression,
- any specific public interest in the subject matter,
- the level of intrusion into an individual's private life, including whether the story could be pursued and published in a less intrusive manner, and
- the potential harm that could be caused to individuals.

Existing guidance set out in industry codes of practice can help organisations to think about what is in the public interest. For example, the following statement of the public interest in the BBC Editorial Guidelines is a good starting point:

BBC Editorial Guidelines

Section 7: Privacy

Private behaviour, information, correspondence and conversation should not be brought into the public domain unless there is a public interest that outweighs the expectation of privacy. There is no single definition of public interest. It includes but is not confined to:

- exposing or detecting crime
- exposing significantly anti-social behaviour
- exposing corruption or injustice
- disclosing significant incompetence or negligence
- protecting people's health and safety
- preventing people from being misled by some statement or action of an individual or organisation
- disclosing information that assists people to better comprehend or make decisions on matters of public importance.

There is also a public interest in freedom of expression itself.

When considering what is in the public interest we also need to

take account of information already in the public domain or about to become available to the public.

When using the public interest to justify an intrusion, consideration should be given to proportionality; the greater the intrusion, the greater the public interest required to justify it.

We recognise that there is an inherent public interest in freedom of expression itself, regardless of the specific content of the story. It is in the public interest to have a free and independent media informing the public about current events and providing information of general interest to the audience. We therefore accept that there will be a public interest in the full range of media output, from day-to-day stories about local events to celebrity gossip to major public interest investigations.

However, this does not automatically mean that publication is always in the public interest. Any consideration of what is in the public interest must involve an element of proportionality – it cannot be in the public interest to disproportionately or unthinkingly interfere with an individual's fundamental privacy and data protection rights. If the method of investigation or the details to be published are particularly intrusive or damaging to an individual, a stronger and more case-specific public interest argument will be required to justify that, over and above the general public interest in freedom of expression.

In particular, media organisations should not make a general assumption that the private life of a public figure is always the subject of sufficient public interest to justify publication. Whether publication of this type of material is in the public interest in any particular case is likely to depend on a variety of factors such as:

- the role and profile of the individual
- the extent to which they have courted publicity or held themselves out as a role model
- the significance of the story to the organisation's audience
- how intrusive or damaging the story is likely to be to the subject or to any other individuals associated with the story.

For example, there is a much stronger public interest in a leading story about the misbehaviour of a prominent public figure than the reporting about the family life of a minor celebrity that might have a very damaging effect upon their family life or career.

Reasonable belief of the data controller

The first key point here is that it is the belief of the data controller that counts, not the individual journalist. However a particular journalist's belief could count as the belief of the data controller depending on the organisation's policies and how they allocate responsibility for reaching the decisions. Therefore in principle the data controller could allow individual journalists to apply the public interest test in each case and it would be the journalists' beliefs that count as being the beliefs of the data controller and these would be looked at for reasonableness.

We will expect organisations to be able to show that there was an appropriate decision-making process in place to consider the public interest of a story. We accept that the level and availability of audit trails of decision making will vary from case to case, but there should be an overarching decision making process in place that can support decision making related to data protection issues. What is appropriate is likely to depend on the case – in many day-to-day stories it may well be appropriate for the journalist to use his or her own judgement, but more high-profile, intrusive or damaging stories are likely to require more editorial involvement and a more formal consideration of the public interest. Organisational policies should be used to explain when greater editorial involvement is required.

Our view is that it is the belief at the time of the processing that is important. The data controller must be able to demonstrate that it had a belief about the public interest, ie that the issue of public interest was actually considered. It should be able to show too that it was considered at the time of the relevant processing of personal data and not just after the event.

If a journalist initially considers that a story will be in the public interest, but in the end the organisation decides not to publish, the exemption can still cover all journalistic activities undertaken up to that point.

Secondly, the exemption requires only a reasonable belief. This gives much more leeway than other exemptions, and reflects the importance of a free and independent media. In other words, the DPA respects the media's independent decisions on the public interest, and doesn't disregard them lightly. The ICO does not have to agree that publication is in the public interest, as long as the intended publisher's belief is a reasonable one.

Section 32(3) says that compliance with any relevant industry codes of practice may be relevant here. The relevant codes are currently:

- the Editors' Code of Practice
- the Ofcom Broadcasting Code
- the BBC's Editorial Guidelines

In practice, if an organisation is subject to one of these codes and has clearly complied with its provisions on the public interest, this will be a strong indication that the belief that publication was in the public interest was reasonable. It is not the role of the ICO to make findings on compliance with industry codes, so if in doubt we may seek to confer with the body responsible for the particular code. (See section 3 for more information on our role and our approach to complaints). If the responsible body decides that an organisation has complied with the code this does not automatically mean that the organisation has complied with the DPA – we retain the right to decide that the exemption does not apply. However, given the importance of a free and independent media, we would only question the responsible body's view on the public interest in exceptional circumstances. A responsible body's decision that there had been a breach of a relevant code would help to inform our view over whether the belief that publication was in the public interest may not have been reasonable.

In practice, we are likely to accept there was a reasonable belief that publication was in the public interest if an organisation:

- has clear policies and procedures on public interest decisions,
- can show that those policies were followed,
- can provide a cogent argument about the public interest, and
- has complied with any relevant industry codes.

Organisations might find it more difficult to rely on the exemption if:

- they have no clear policies or procedures.
- journalists acted outside of company policies or accepted practice,
- there is no evidence that anyone thought about the public interest, or
- an industry body finds them in breach of a code of practice.

We note that the Editors' Code requires print editors to be able to demonstrate their reasonable belief in the public interest, including details of how, and with whom, this was established at the time. We would therefore expect that the press should already have suitable procedures and (where necessary) audit trails in place.

(4) Compliance is incompatible

> "(c) the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes."

Organisations must also be able to explain why complying with the relevant provision of the DPA is incompatible with the purposes of journalism. In other words, there must be a clear argument that the provision in question presents an obstacle to responsible journalism. You should be able to show it was impossible to both comply with a particular provision and to fulfil your journalistic purpose. Alternatively, you can show that it was unreasonable in the circumstances to comply with a particular provision, by virtue of it being impractical or inappropriate. You must balance the detrimental effect compliance would have on journalism against the detrimental effect non-compliance would have on the rights of the data subject.

Relevant factors when considering incompatibility can include consideration of the practicality of compliance and whether the burden on resources is disproportionate, but always weighed against the privacy impact on the data subject. However, compliance must be more than just an inconvenience, and it is not enough simply to assert that compliance is not standard industry practice. We will expect organisations to be able to explain the effect compliance would have, and why this would be unreasonable.

Organisations must take into account all the circumstances of the particular case. They cannot rely on a blanket policy that the media don't have to comply with certain requirements; there must be specific consideration given to each case, at an appropriate level.

This is also not necessarily a blanket exemption from the whole DPA – just because compliance with one provision can be shown to be incompatible with journalism doesn't mean that compliance with a different provision will necessarily be incompatible. Organisations must be able to justify their use of the exemption in respect of every provision they have not complied with.

Again, the focus is on the reasonable belief of the data controller (see previous section on the reasonable belief of the data controller). As with the public interest, the ICO doesn't have to agree, as long as the decision was reasonable. Organisations do need to show that someone at an appropriate level gave thought to whether they could comply with the

provision in question. What an appropriate level is will depend on how unusual the circumstances are. Organisations will find it more difficult to rely on the exemption if they cannot explain how data protection issues were understood, raised or considered in cases of significant privacy intrusion. Ensuring that standard checks for common data protection issues are embedded in existing journalistic and editorial decision-making processes, and showing that there is a good institutional understanding of the DPA (eg clear policies, staff training and guidance), will help to show that data protection concerns are understood and considered.

It's a good idea to keep an audit trail in cases that are controversial or particularly likely to prove contentious, though this will not be necessary in every case.

Practical tips

We recommend that organisations:

- have clear policies about what needs editorial approval,
- give all staff some basic data protection awareness training,
- have an inbuilt public interest check at key stages of a story,
- consider the data protection implications at key stages of a story, and
- keep an audit trail for unusually high-profile or intrusive stories.

The key stages where you might need a check are the initial decision to pursue a story, any decision to use covert methods of investigation, and final decisions on what to publish.

These checks do not need to be particularly formalised or onerous in most cases, and organisations are likely to have suitable policies and procedures in place already which they can review and adapt if necessary. In fact, data protection checks will often work best when embedded in existing journalistic or editorial judgements, practices and procedures. Senior or expert input and a formal audit trail are only likely to be necessary in difficult or controversial cases.

What is not exempt

Section 32 can exempt the media from most of the DPA, but not all of it. It does not provide an exemption from:

- Notification. Media organisations will still need to register with the ICO. See The duty to notify above.
- Security. The exemption does not cover the seventh data protection principle. You must always have adequate security measures to protect personal data. See the section below on security.
- The section 55 offence. Journalists and media organisations will not be exempt from prosecution if they unlawfully obtain, disclose or procure information in breach of section 55. However, there is a public interest defence within section 55 itself. See the section below on The section 55 offence for more information.
- The right to opt out of direct marketing.
- The right to compensation for damage and distress. Individuals have the right to claim compensation through the courts if they have suffered damage or distress as a result of a breach of the DPA. The exemption does not remove this right. In other words, the media cannot argue that they are exempt from paying compensation for a breach. However, an organisation can argue that it did not breach the DPA because it was exempt from the underlying provision. It can also defend a claim on the basis that it took reasonable care in the circumstances to avoid a breach. For more information, see the section on court claims in section 3.

Like any other organisation, the media will also need to comply with the standard provisions of the DPA when handling personal data for a non journalistic purpose – eg HR records, information about suppliers or customers, information related to marketing and advertising, or information about property management.

Finally, it's worth repeating that the media always need to comply with as much of the DPA as they can. Even if a story is clearly in the public interest, if a journalist can reasonably research and present it in a way that complies with the standard provisions of the DPA, they must.

The first principle: fairness

In brief...

Wherever possible the media should collect and use information about people fairly and lawfully, and not cause any unjustified harm. Journalists will often be able to collect information without the subject's knowledge or consent, but it will be unfair to actively mislead people about the journalist's identity or intentions.

Covert investigations or stories involving details of someone's health, sex life or allegations of criminal activity are less likely to comply with the first principle, although media organisations may be able to invoke the exemption if there is sufficient public interest in publication.

Organisations must act fairly and lawfully.

This generally means they need to:

- be open and honest, tell the people they are dealing with (and the data subject, if different) who they are and what they are doing, unless this is not practical,
- not cause people any unjustified harm, and
- not do anything that they wouldn't reasonably expect.

In the context of journalism, we accept that it will not generally be practicable for journalists to make contact with everyone about whom they collect information. It will often be fair to collect information on matters of potential journalistic interest without the subject's knowledge. However, there will be cases where fairness may require some direct contact with the subject of a major investigation, to offer them the opportunity to put forward their side of the story. It is also likely to be unfair to mislead people about a journalist's identity or intentions (although the exemption may apply if there is sufficient public interest justification).

These provisions bring in the notion of proportionality. So, for example, there would be no requirement of prior notice to the individual if this would represent an unduly burdensome interference with freedom of expression disproportionate to any real need of the individual.

The requirement to act lawfully also means that any breach of other laws, including a breach of confidence or defamation, would automatically breach the DPA unless an exemption applies.

Organisations must also meet one of the six listed conditions in order to process personal data. The two conditions likely to be relevant to the media are:

- The person who is the subject of the information has given consent to the processing. Consent must be freely given, specific, and informed, and cannot just be assumed from someone's silence (although it can be implied from their actions – eg if they volunteer information to a journalist when they are fully aware of the journalist's identity and intentions).

- The processing is necessary for 'legitimate interests', and will not cause unwarranted harm to the person concerned. Legitimate interests will include a media organisation's commercial and journalistic interests in gathering and publishing material, as well as the public interest in freedom of expression and the right to know.

This means that the DPA does not always require consent. The organisation's interest in publication, together with the public interest in freedom of expression may well override an individual's preferences or privacy interests. However, this is not automatic, and again, the key is proportionality. It is a balancing act – if there is a serious privacy intrusion or risk of harm, there will need to be a significant public interest to justify this.

If the information is 'sensitive personal data' organisations must also meet one of the following conditions:

- The person has given their **explicit** consent.

- The information has already been made public as a result of steps that person has deliberately taken. It's not enough that it's already in the public domain – it must be the person concerned who took the steps which made it public.

While our view is that the section 32 exemption will tend to be of more practical use to the media, there is another condition set out in the Data Protection (Processing of Sensitive Personal Data) Order 2000, to allow public interest disclosures of sensitive personal data connected to wrongdoing or incompetence. This requires that disclosure must be in the **substantial** public interest, with a view to publication, and the data

controller disclosing the information must reasonably believe that publication is in the public interest. However, this only permits disclosures, not other types of processing. Although it could cover people who give information to journalists, or the act of publication itself, it cannot cover everything else a journalist would need to do (eg collecting, recording and storing information). For this reason, our view is that the media will generally need to invoke the section 32 exemption for journalism in these circumstances. In fact, the exemption is likely to be easier to apply, as it is not limited to disclosures of 'substantial' public interest, or cases of wrongdoing.

In short, in many cases the media can comply with the first principle if they take a reasonable and proportionate approach, don't actively mislead anyone, and follow any relevant industry codes of practice. However, for covert investigations or other methods of obtaining information without the subject's knowledge, or if the story involves previously undisclosed details of someone's health, sex life or allegations of criminal activity, media organisations would generally need to invoke the exemption for journalism.

The seventh principle: security

In brief...

The media must take reasonable steps to prevent people's information being lost, stolen or misused.

Organisations will need to consider technical (electronic) and physical security measures, policies and procedures, and staff training and supervision. These should cover staff working both in and outside of the office.

Information about people must be kept securely. The DPA says organisations must take reasonable steps to stop it being lost, stolen or misused. The media are not exempt from these security obligations.

There is no single answer to what security measures might be appropriate, but organisations should be able to justify the level of security they have. They should take into account how sensitive or confidential the information they hold is, the harm that might result from its loss or improper use, the technology available, and the costs involved. They don't have to have state-of-the-art security, but it should fit the

level of risk. The level of security appropriate for employee records or information from confidential sources is clearly going to be different to the level of security appropriate for information which is publicly available.

Organisations should consider their:

- technical (electronic) security. This includes log-on controls, firewalls, encryption, remote wiping facilities, suitable back-ups, and proper disposal of old equipment. Consider both office computer systems and any mobile devices used out of the office (eg smartphones, laptops or tablets). If employees are allowed to use their own mobile devices, refer to our Bring Your Own Devices (BYOD) guidance.

- physical security. This includes locks, alarms, supervision of visitors, disposal of paper waste, and how to prevent notebooks and mobile devices being lost or stolen when staff are out of the office. This may be a particular issue for journalists who spend a lot of time out of the office gathering information or filing reports on location.

- management and organisational measures. For example, ensuring that a person with the necessary authority and resources has day to day responsibility for ensuring information security, and putting in place robust policies and procedures, including a breach-management plan.

- staff training and supervision. Organisations should vet new staff to a level appropriate to their position to confirm their identity and reliability, and provide training (including regular refresher training) on key security risks, procedures and responsibilities.

For more detailed advice and links to further guidance, see The Guide to Data Protection.

The section 55 offence

In brief...

It is a criminal offence for anyone to knowingly or recklessly obtain (or disclose) information about someone from a data controller without its consent.

There is currently no specific defence for journalists, but there is a public interest defence. The ICO will always take full account of the special importance of the public interest in freedom of expression and a free and independent media.

It is an offence under section 55 of the DPA to knowingly or recklessly obtain, disclose, or procure the disclosure of information about someone without the consent of the data controller responsible for that information. This could cover obtaining information from another organisation by deception ('blagging'), hacking, exploiting poor security, via an unauthorised leak, or employing unscrupulous private investigators who use such methods. There will be a defence available if there is sufficient public interest justification.

At present, there is no specific exemption for journalists. The Criminal Justice and Immigration Act 2008 provided for an enhanced public interest journalism defence (which would require only a reasonable belief that obtaining the information was in the public interest). This provision has not yet been brought into force. However, there is a general public interest defence, if in the particular circumstances obtaining (or disclosing) the information was objectively justified in the public interest.

When considering the availability of this defence in the context of journalism, we will always take into account the special importance of the public interest in freedom of expression and a free and independent media. In particular, we recognise the important role that undercover investigations and unauthorised leaks can play in major public interest stories.

Other available defences include a reasonable belief that the data controller would have consented if they knew the circumstances, or showing that the relevant action was necessary for the prevention or detection of crime.

It's important to be aware that this is not just a corporate offence: individuals can also be prosecuted. Any source leaking information to journalists from an organisation without that organisation's knowledge might also be committing an offence.

The Information Commissioner will only bring a prosecution if he considers it is in the public interest to do so, and will always assess the public interest carefully. See section 3 below for more information on the Commissioner's approach to prosecution.

On conviction, the penalty is currently limited to a fine. The Criminal Justice and Immigration Act 2008 sections 77 and 78 made provision enabling judges to impose a prison sentence, replacing the current 'fine only' regime. The Act also provided for a stronger defence of 'reasonable belief' for journalists. Neither provision has, as yet, been commenced.

There are also a number of other criminal offences which overlap with section 55 or other provisions of the DPA, including hacking offences under the Computer Misuse Act 1990 and unlawful interception under the Regulation of Investigatory Powers Act 2000. However, the ICO's prosecution role is limited to offences under the DPA. Evidence of other criminal behaviour would be referred to the police. The police or other agencies (eg the National Crime Agency) can also refer cases to the ICO.

3 Disputes

In brief...

The Information Commissioner's Office upholds information rights in the public interest. We consider complaints, and have the power to take enforcement action for serious breaches, although our powers are more restricted in cases affecting the media. We can also prosecute offences under the Data Protection Act. However, we cannot prevent publication or award compensation.

We will always consider the impact on freedom of expression carefully before deciding to take any action. We will also seek to work with industry bodies and refer issues to them wherever appropriate.

Individuals can also make DPA claims directly through the courts.

Role of the ICO

The Information Commissioner is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner's data protection responsibilities are:

- to promote good practice and give advice and guidance,
- to keep a register of organisations processing personal data,
- to review complaints from the public and to consider whether further regulatory action is required,
- to take enforcement action against organisations that persistently ignore their obligations, and
- to bring prosecutions for offences committed under the DPA.

The Commissioner can also make reports to the UK Parliament on issues of concern.

The ICO is not a specialist media regulator. Our focus is on compliance with the provisions of the DPA, not media conduct more generally. Various industry bodies are responsible for standards and codes of practice in this area and it is not the ICO's job to usurp that role. Equally, any investigation conducted by, or decision of, an industry body that relates to DPA compliance cannot take the place of the Commissioner's own investigation and decision.

Without derogating from our statutory responsibilities, we will consult with industry bodies wherever appropriate, and will seek to work with them where our roles overlap. For example, compliance with an industry code of practice may be a relevant factor in our decision as to whether the DPA exemption for journalism applies. The DPA states that the ICO may take into account compliance with any relevant code of practice (as designated by the Secretary of State) when considering whether a data controller's view that publication would be in the public interest was reasonable.

The codes currently designated for this purpose by the Secretary of State are:

- the Editors' Code of Practice
- the Ofcom Broadcasting Code
- the BBC's Editorial Guidelines

It is not our role to decide whether a media organisation has complied with an industry code. However, we will take any relevant decision of an industry body into account, even though we are not bound by its decision. Not all media organisations are subject to oversight by industry bodies and the weight we give to the decision of an industry body will depend upon the nature of that body (for example whether it oversees compliance with one of the designated codes of practice above) and the nature of its investigation, including its rigour. It is still open to the ICO to find that there was a breach of the DPA even if you complied with the relevant code of practice.

Complaints to the ICO

If someone complains about the way you have handled their personal data, we will review their concerns and we may investigate your actions and compliance with the DPA. If we decide that it is likely you have failed (or are failing) to comply with the Act, we may ask you to take the

necessary steps to remedy this. We would usually highlight where improvements are required and ask that you take action to avoid potential breaches in the future.

In order to impose penalties or to order you to comply, we would have to decide to take further formal enforcement action. See the section below for more information on ICO enforcement powers. We have no power to award compensation. Only the courts can do this. See the section below on Court claims for more information.

If we consider that a complaint raises concerns about media conduct or standards rather than a specific data protection issue we may also advise individuals to contact a relevant industry body (if there is one available).

If a complaint raises specific issues about data protection compliance and we decide to investigate, we will generally contact the person complained about first to ask some initial questions and give them an opportunity to explain their position. If they are relying on the exemption for journalism, we may also seek to consult with relevant industry bodies on whether they have complied with any code of practice. We may also ask for details of their policies and procedures, any audit trail of their decisions on the story, and an explanation of the public interest factors that influenced the decision.

If the complaint is about actions in relation to a story that has not yet been published, our powers of investigation are restricted until we have assessed whether the processing complained about was, or is, for journalistic, literary or artistic purposes with a view to publication.

Good internal data protection awareness, clear policies and procedures which include data protection checks, and an audit trail showing that particularly difficult issues are addressed at an appropriate level, will all help to demonstrate compliance with the DPA.

We will also look at the public interest balance, but our role will be to determine whether the decision maker's belief that the activity was in the public interest was a reasonable decision, not to determine whether we would have reached the same decision. Where an industry body has found you did not comply with a relevant code of practice this may be an indication that the decision was not reasonable.

We are most likely to find against you if it appears that you did not actually give proper thought to the public interest or whether you could comply with the DPA.

ICO enforcement powers

The ICO has powers to take formal enforcement action for breaches of the DPA. Tools at our disposal include enforcement notices, civil monetary penalties (fines), and criminal prosecutions.

In recognition of the importance of the public interest in freedom of expression, these powers are more restricted in cases involving the media. However, subject to those restrictions, the ICO is committed to taking regulatory action against the media, just as it would against organisations in other sectors, where this is necessary to ensure compliance with the DPA.

Any action we take will be targeted and proportionate, in line with our Regulatory Action Policy. We will always consider the potential impact on freedom of expression carefully before deciding to take any action. We will also take into account whether a breach has caused, or is of a kind likely to cause, significant damage or distress to anyone.

We are most likely to consider action where there is a risk of significant damage or distress together with evidence of inadequate policies and procedures, inadequate corporate oversight, independent findings of unethical or unlawful behaviour (ie adverse decisions of an industry body or adverse court judgments), or clear institutional disregard for data protection compliance.

Enforcement notices

If there is a breach of substantial public importance, we can serve an enforcement notice requiring the data controller to take steps to comply. Failure to comply with an enforcement notice is a criminal offence.

However, we cannot prevent publication, and there are significant procedural safeguards to protect freedom of expression. This results in a three-stage process:

1. We must make a written finding either that the information is being processing for other purposes (ie not just for journalism, art or literature), or that there is no intention to publish any previously unpublished material. Our powers to investigate this are limited unless there is a specific complaint or court claim against the data controller. This decision is subject to appeal to the Information Rights Tribunal.

2. After this stage we can then apply to a court for permission to serve an enforcement notice in relation to use of personal data for journalism. The court must be satisfied that we have reason to suspect a breach of substantial public importance. Generally the intended recipient of the notice will be given the chance to defend this application before the court.

3. We can then serve an enforcement notice which can be appealed to the Information Rights Tribunal.

Civil monetary penalties

We can also impose a civil monetary penalty (fine) of up to £500,000 if we are satisfied that:

- there was a serious breach,
- it was likely to cause substantial damage or distress, and
- it was either deliberate, or the data controller knew (or should have known) of the risk but failed to take reasonable steps to prevent it.

We don't need the court's permission to impose a civil monetary penalty, though these penalties can be appealed to the Information Rights Tribunal.

For more information about our approach to monetary penalties, see our separate guidance about the issue of monetary penalties.

Prosecution

The Information Commissioner can investigate and prosecute offences under the DPA (except in Scotland, where the Procurator Fiscal brings prosecutions).

A person or company found guilty is liable to a fine up to £5,000 if the case is heard in a magistrates' court or the sheriff court, or to an unlimited fine on conviction in the Crown Court or the High Court of Justiciary. The power to impose a custodial sentence contained in the Criminal Justice and Immigration Act 2008, together with the strengthened 'reasonable belief' defence for journalists, has yet to be commenced.

Criminal offences created by the DPA include:

- the section 55 offence,
- processing personal data without notifying the ICO,
- failing to comply with an Enforcement Notice, and
- failing to comply with an Information Notice or a Special Information Notice.

The Commissioner will only bring prosecutions when he considers it is in the public interest to do so, and will always assess the public interest carefully. He will have regard to:

- The ICO prosecution policy statement
- The Code for Crown Prosecutors
- CPS guidelines for prosecutors on assessing the public interest in cases affecting the media.

Court claims

Claims for compensation

If an individual suffers damage or distress as a result of a breach of the DPA, he can make a claim in court for compensation under section 13. There are no guidelines about levels of compensation a court might award in this area. In some circumstances, the court can also order the information in question to be corrected, blocked, erased or destroyed.

A claim for compensation can obviously be defended if there has been no breach of the DPA, or if an exemption applies. If there has been a breach, you can still defend a claim for compensation, but only if you can show that you took such care as was reasonably required in the circumstances to comply with the DPA. What you will have to prove will depend on the nature of the breach and what is reasonable will depend on the circumstances. In most cases, this is likely to mean showing that there were appropriate policies and training in place to protect personal data, and checks in place to prevent problems. You can apply to stay the proceedings if you are still using the information with a view to publishing new material.

Other types of claims

Individuals can also apply to the courts for:

- a court order under section 7(9) for an answer to a subject access request,
- a court order under section 10(4) to stop any processing which is likely to cause substantial damage or distress,
- a court order under section 12(8) to force reconsideration of an automated decision (unlikely to be relevant in the context of journalism), or
- a court order under section 14 for rectification, blocking, erasure or destruction of inaccurate data, or any expression of opinion based on inaccurate data (section 14(1)).

If a claim is made against you about information you were using for a story, you may be able to defend it using the exemption for journalism

You may also be able to stay the proceedings if you are still using the information with a view to publishing new material.

Your right to stay pre-publication proceedings

If a claim is made against you about information which you are still using with a view to publishing new material, you can ask the court to stay the proceedings under section 32(4).

The claim can only recommence if the claimant withdraws his application, or if the Information Commissioner makes a written decision that you are either using the information for other purposes, or that you are not intending to publish new material (for example, because you have now published or abandoned the story). You can appeal the Commissioner's decision to the Information Rights Tribunal.

In effect, this means that someone cannot use the DPA to prevent publication.

ICO assistance for claimants

Individuals bringing court claims in relation to journalism can ask the ICO for assistance under section 53. This might include advice, representation, or help with costs. We must consider the request, but don't have to agree. We can only provide assistance if we think the case involves a matter of substantial public importance, and we will tell you if we do so.

If you would like to contact us please call 0303 123 1113

www.ico.org.uk

Information Commissioner's Office
Wycliffe House, Water Lane,
Wilmslow, Cheshire SK9 5AF

Version 1.0
4 September 2014