Data protection and journalism: a guide for the media

DRAFT FOR CONSULTATION

Contents

Foreword

[Commissioner’s foreword]

1 About this guide

In brief...

This guide explains how the Data Protection Act applies to journalism, advises on good practice, and clarifies the role of the 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 Data Protection Act 1998 (the DPA) applies to journalism. It sets out the basic principles and obligations, advises on good practice, and clarifies how the 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 journalists, editors, and managers understand and comply with data protection law and 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 will not prevent public interest 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.

Who the guide is for

The guide is intended for media organisations involved in journalism – including the press, the broadcast media, and online news outlets. Individual journalists might also find parts of it useful, although legal responsibility under the DPA will usually fall on the organisation they work for. With this in mind, the guide is specifically addressed to those working in the media.

We have produced separate guidance for members of the public on their data protection rights in relation to journalism. This is available on the 'for the public' pages of our website.

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 our view of the existing law as set out in the DPA.

It is intended to help those working in the media to fully understand 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 of course always need to take into account the particular circumstances of the case.

More information

The Guide to Data Protection gives an 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.

2 Balancing privacy with freedom of expression

In brief...

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

The ICO must also 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 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 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 it is legally obliged to do so). This means that the ICO must respect and protect freedom of expression as well as individual privacy. We will always consider the importance of freedom of expression and the vital role of the media in our interpretation of the DPA and when we decide how best to use our powers in the public interest.

However, these rights are not absolute. The ECHR makes clear that it can be legitimate to restrict freedom of expression to protect other rights, including the right to privacy – just as it can be legitimate to interfere with someone's privacy to protect freedom of expression. Proportionality is the key issue.

In other words, both privacy and freedom of expression are of special importance in a democratic society, and neither consideration automatically trumps the other. They have equal status, and a fair balance must be struck if they conflict. There is no one-size-fits all answer, and where the balance lies in any one case will depend on the particular circumstances of that case.

In data protection law

Data protection law grew from concerns about protecting the individual's right to privacy. But it was 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 for 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. See chapter 4 below for more detail on how the exemption works.

The DPA also restricts the powers of the ICO in regulating the media, and ensures additional safeguards and points of appeal. And 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 chapter 6 below for more information on the role of the ICO in cases involving the media.

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. Each of those codes specifically incorporates a balancing act for invasions of privacy:

The Editors' Code of Practice

3. Privacy

i) Everyone is entitled to respect for his or her private and family life, home, health and correspondence, including digital communications.

ii) Editors will be expected to justify intrusions into any individual's private life without consent. Account will be taken of the complainant's own public disclosures of information.

The Ofcom Broadcasting Code

8.1 Any infringement of privacy in programmes, or in connection with obtaining material included in programmes, must be warranted.

… if that reason is the public interest, then the broadcaster should be able to demonstrate that the public interest outweighs the right to privacy.

BBC Editorial Guidelines

Section 7: Privacy

Meeting these ethical, regulatory and legal obligations in our output requires consideration of the balance between privacy and our right to broadcast information in the public interest. We must be able to demonstrate why an infringement of privacy is required.

Factors which will help ensure you strike a fair balance – including public interest tests, fairness, openness and accuracy – also pervade the other provisions of 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.

3 Data protection basics

In brief...

If you handle information about people, you 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. It is also a criminal offence to obtain, procure or disclose personal data without the consent of the data controller.

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 for journalism, but this does not give a blanket exemption from the DPA as a whole. See When does the DPA apply?

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. See What is 'personal data'? (But it's true the DPA will offer more protection for information someone wants to keep private.)

Myth: the DPA bans the disclosure of personal data

Reality: the DPA does not contain any absolute prohibitions. In general, the key is to consider what's fair in the circumstances. See The data protection principles.

Myth: the DPA 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. See Principle 1: Fairness.

Myth: the DPA sets time limits on keeping information

Reality: there are no set time limits. You can hold information for as long as necessary – you just shouldn't keep things you don't need. See Principle 5: Time limits.

Myth: the DPA says we should reveal our sources

Reality: the DPA can protect the privacy of your sources. See Confidential 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. See The data protection principles.

Myth: the exemption only applies if we publish

Reality: the exemption works case-by-case and does not apply automatically. But where it does apply, it can cover background investigations as well as the details published in any final story. See The exemption for journalism.

Myth: the ICO can 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. See The exemption for journalism.

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.

The DPA sets out a framework of rights and duties, which are designed to balance the legitimate needs of organisations to collect and use people's details for business or other purposes (including journalism) against the individual's right to information privacy. There are very few hard and fast rules. Instead, it is based around eight flexible common-sense principles.

A number of exemptions disapply some of the provisions in some circumstances. There is an exemption for journalism, art and literature – but this does not mean the media are automatically exempt from the DPA as a whole. See chapter 4 below for more information on when the exemption applies and what it covers.

It's important to emphasise that the DPA will not prevent public interest journalism. But the media cannot ignore it altogether, and will need to be aware of the main principles and comply with them wherever possible.

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 does **not** cover anonymous records, information about the deceased, or unstructured paper records (eg handwritten notebooks). However, information in notebooks is covered if you intend to transfer it to a computer or filing system at a later date.

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. Neither is personal data 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 truly anonymous 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. And 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 – (A)(3) Key definitions.

Sensitive personal data

Some types of information are designated 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 should be treated with extra care.

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. In other words, a subcontractor. (Employees are part of the data controller rather than separate data processors.)
- **Data subject** – the person the personal data is about.
- **Third party** – someone who's not a data controller, its employee, a data processor, or a data subject.
- **Inaccurate** – incorrect or misleading as to any matter of fact. This means someone's opinion cannot be 'inaccurate personal data' as long as it is marked as opinion and was correctly recorded.
- **Special purposes** – journalism, art or literature.

See The Guide to Data Protection – (A)(3) Key definitions for more information and exact 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 – you will need to judge how they apply to each case.

This chapter gives a brief overview of the principles. For a full discussion and links to more detailed guidance, see The Guide to Data Protection – (B) Data protection principles. For advice on how this all applies to key issues in practice, see Chapter 5 below.

Principle 1: Fairness

You must act fairly and lawfully. This generally means you need to be open and honest, tell the person who you are and what you are doing, not cause them any unjustified harm, and not do anything that they wouldn't reasonably expect. It also means that any breach of other laws, including a breach of confidence or defamation, will automatically breach the DPA.

You must also meet one of the six listed conditions. The two conditions likely to be relevant to the media are:

- You have the person's consent. 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 when they are fully aware of what you're going to do with it).

- The processing is necessary for 'legitimate interests' (which include both the public interest in publishing a specific story and general journalistic or business interests), and will not cause unwarranted harm to the person concerned. So you don't always need consent. If there's not much privacy impact, your interests may well override an individual's preferences. However, the default setting is not publication; you must have a justification. This is a balancing act – if there is a serious privacy intrusion or risk of harm, there will need to be a significant public interest at stake to justify this.

'Necessary' also means that there must be no other reasonable way to do things.

If the information is sensitive personal data (see page 14) you must meet one of the following conditions as well:

- You have the person's **explicit** consent.
- The person has deliberately made the information public. It's not enough that it's already in the public domain (eg published by a newspaper) – it must be the person concerned who took steps to make it public.

There is another condition set out in the Data Protection (Processing of Sensitive Personal Data) Order 2000, to allow someone to disclose sensitive personal data connected to wrongdoing or incompetence for public interest journalism. The 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, it only permits disclosures, not other types of processing. This means it cannot cover everything a journalist will need to do (eg collecting, recording and storing information). Our view is that this condition is intended to cover people who give information to journalists, but that journalists themselves will need to rely on either consent or the exemption for journalism instead (see chapter 4).

In short, in many cases you can comply with the first principle if you tell people who you are and what you're investigating, and follow industry codes of practice on privacy and the public interest. But for covert investigations or other methods of obtaining information without the subject's knowledge, or if your story involves sensitive personal data, you would generally need to rely on the exemption for journalism.

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 an entirely different and unexpected purpose.

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 don't need.

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 include their view.

Principle 5: Time limits

Personal data must not be kept for longer than necessary. The key point is to actively consider how long you need information for, and review it periodically. But there's no fixed time limit, and we accept in some cases it might be necessary to keep details for long periods.

Principle 6: Individuals' rights

You must comply with people's right:

- to access a copy of their personal data (subject access). See the section below 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.

- 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). Security measures should include physical and technical security, robust policies and procedures, and staff vetting and training. What is appropriate will depend on a risk assessment taking into account the nature of the information, the harm that could be caused by a security breach, the security technology available, and the cost.

You cannot rely on the journalism exemption to avoid security obligations.

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.

Publishing information on a website will count as a transfer as soon as someone outside the EEA accesses that website. However, this should not stand in the way of public interest journalism. If publication is genuinely in the public interest, the personal data should by its nature not require additional protection. And this principle does not apply at all if you can show the transfer is necessary for reasons of 'substantial' public interest.

The section 55 offence

It is an offence under section 55 of the DPA to knowingly or recklessly obtain, disclose, or procure the disclosure of personal data without the data controller's consent. This would for example 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 is a public interest defence. A court must agree that your actions were justified in the public interest. Other available defences include a reasonable belief that the data controller would have consented if they knew the circumstances, or showing that your actions were 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 you without their employer's knowledge might also be liable to prosecution.

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 in cases affecting the media. See Chapter 6 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 empowered the government to change this and give judges the power to impose a prison sentence, but this has not yet been implemented. To protect journalists, the same Act also provided for an enhanced public interest journalism defence (which would require only a reasonable belief that obtaining the information was in the public interest). However, this provision is not yet in force either.

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.

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. You should always make sure you understand the terms of an exemption before relying on it. 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. And they usually 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).

The exemption for journalism, art and literature is one of the broadest exemptions, and can exempt you from many of the DPA's provisions. However, as with other exemptions, it only works on a case-by-case basis and does not give a blanket excuse for non-compliance.

The next chapter considers the journalism exemption in detail. For more information on the other exemptions, see The Guide to Data Protection – (D) Exemptions.

4 The journalism exemption

In brief...

The exemption protects freedom of expression in journalism, art and literature. It applies if you act with a view to publishing something in the public interest, and believe you need to disapply a provision of the DPA to do so – as long as those views are reasonable.

In practice, this means that journalists have the chance to mount a kind of public interest defence to most apparent breaches of the DPA. But you must consider each case on its own merits. The law does not provide journalists with a blanket exemption.

You should find it easier to rely on the exemption if you can show robust policies and procedures, compliance with industry codes of practice, good internal awareness of the DPA, and appropriate record keeping for difficult decisions.

Basic principles

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 – but please note that 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 fair amount of leeway to decide for themselves what is in the public interest. However, this is no 'get out of jail free' card. In effect, it gives you a chance to justify your actions in the public interest, case by case. But even if a story is clearly in the public interest, this still doesn't mean you can ignore the DPA altogether: if you can comply, you must. The exemption will only come into play if you actually need to disapply a provision of the DPA in order to do your job in

relation to a public interest story. This is why it's important that journalists still 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) you reasonably believe publication is in the public interest; and
(4) you reasonably believe compliance is incompatible.

The focus will usually be on elements three and four. In essence, you should have a reasonable argument that the public interest in the story 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 widely. In general, you won't need to focus on this too closely, because it overlaps with other elements of the test. In short, if you are acting with a view to publishing something in the public interest, it's highly likely to be for the purposes of journalism, art or literature.

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 will 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 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, information about things such as advertising revenue, property management, financial debt, circulation or public relations would not usually be held for the purposes of journalism.

Citizen bloggers

We also 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."

If amateur bloggers claim their purpose was journalism (or art or literature), the focus is therefore likely to be on the public interest part of the exemption – see (3) In the public interest below.

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 which 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.

Processed only for the special purposes

The exemption covers information processed only for journalism, art or literature. On one view, this might mean that information cannot be exempt once it is used for any other purpose, even if that other purpose is minor or incidental. However, we do not consider this interpretation would give enough protection to freedom of expression.

Our view is that the exemption can apply as long as the particular processing activity in question is purely for the purposes of journalism. If so, that processing can be exempt, even if the same information is also separately processed for other purposes which are not exempt. For example, once a story has been published, it might be retained as part of a historical archive rather than purely as a journalistic resource. However, this would not prevent you using the exemption to justify the way the information was originally obtained, or its publication.

(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…"*

You must be handling the information with a view to publication of journalistic material. This doesn't mean you must be aiming to publish the actual information in question. As long as your aim is to publish a story (or for someone else to publish it), all the background information you collect, use or create as part of your investigation can also be exempt, even if those details are not included in the final article or programme – or even if the story itself is never actually published or broadcast.

On the other hand, if you collect and keep some details for general future use without a particular story in mind (eg contact details), it might be difficult to argue you are keeping them with a view to publication. However, our view is that you are unlikely to need the exemption for this type of information. You should be able to retain contact details without breaching the DPA – see keeping contact details in chapter 5 below for more on how to comply.

As long as the information was originally collected and used with publication in mind, the exemption can protect you 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.

In effect, this means that your actions up to (and including) publication can be exempt, and will remain exempt even if someone complains at a later date. However, the exemption cannot apply to anything you do with the information after publication.

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

(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, you will need to be able to demonstrate that there was a suitable decision-making process.

What is the public interest?

It is often said that the public interest is not the same as what is interesting to the public. So what is it? Claiming to be acting in the public interest has to involve making, and being able to defend, a judgement about what is in the best interests of society as a whole.

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. You must always consider the circumstances of the case in front of you, rather than assuming something is acceptable because you or others have published comparable material in the past.

Existing guidance set out in industry codes of practice will help you 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.

There are similar provisions in the Editors' Code and the Ofcom Broadcasting Code.

Of course, even if these factors are present, it doesn't automatically mean that publication is always in the public interest. For example, revealing information about crime or wrongdoing may sometimes undermine police investigations or court proceedings, and so work against the public interest. You should consider the extent to which publication will actually serve the overall interests of society.

In particular, you should not make a general assumption that the private life of a public figure is always the subject of legitimate public interest.

These factors will carry more weight in some cases than in others, depending on the context. For example, revealing corruption or incompetence in public office is likely to carry significantly more weight than discussing the misbehaviour of celebrities, even though both cases are nominally about exposing wrongdoing.

It is true that there will always be some public interest in freedom of expression itself, regardless of the content of the story. This might be enough to justify a very minor technical exemption from the DPA.

However, we do not consider it would be reasonable to think that this on its own could justify a publication which involves a significant intrusion into someone's privacy.

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. There must be a corporate decision that the story is in the public interest, which is likely to mean some editorial involvement (which might be a formal commissioning process, or might be a much more informal go-ahead, depending on the context and usual practice). But if a journalist investigates a story without discussing it with an editor first, it will be difficult to rely on the exemption, particularly in controversial cases.

Our view is that it is the belief at the time of the processing that is important. So, if you initially consider that a story will be in the public interest, but in the end change your mind and decide not to publish, the exemption can still cover the information you collected up to that point. On the other hand, it also means that the exemption cannot cover 'fishing expeditions' undertaken with no particular story or journalistic aim in mind.

The second key point is that the exemption requires only your 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 your view is a reasonable one. In controversial cases it might well be possible for reasonable people to disagree. If so, it is your belief that counts.

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

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

In practice, if you have complied with industry codes on the public interest, this should be enough to show your view of the public interest was reasonable. It is not the role of the ICO to make findings on compliance with industry codes, so we would generally defer to the

relevant media regulator on this question (see chapter 6 for more information on our role and our approach to complaints). A regulator's decision that you complied with the code would not automatically mean you have complied with the DPA – we can still decide that the exemption does not apply – but, given the importance of a free and independent media, we would only question a regulator's view on the public interest in exceptional circumstances.

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

- there was editorial involvement from an early stage;
- you can show there was a public interest check; and
- you have complied with industry codes.

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

- there was no editorial involvement until the story was filed;
- journalists acted outside of company policies or accepted practice;
- there is no evidence that you thought about the public interest; or
- an industry regulator finds you 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 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.*"

You must also believe that complying with the relevant provision of the DPA is incompatible with the purposes of journalism. In other words, you must decide that the provision in question would stop you from doing your job, and the public interest is strong enough to justify your actions. But if you can reasonably get the story in another way which would

comply with that provision, you must. The DPA must be more than just an inconvenience; you must have no other reasonable way to proceed.

You must take into account all the circumstances of the particular case. You cannot rely on a blanket policy that you don't have to comply with certain requirements; you must make a case-by-case decision. And this is not necessarily a blanket exemption from the whole DPA – just because you need to disapply one provision, that doesn't mean you can ignore the rest. You must be able to justify every apparent breach.

Again, the focus is on the reasonable belief of the data controller. As with the public interest, we don't have to agree with you, as long as your decision was reasonable. But you do need to show that you gave proper thought as to whether you could comply with the provision in question. Ensuring that standard checks for common data protection issues are embedded in existing editorial decision-making processes, and showing that you have a good institutional understanding of the DPA (eg staff training and guidance), will help you show that you made a reasonable decision.

You will find it more difficult to rely on the exemption if there is no evidence that data protection concerns were understood, raised or considered. It's a good idea to keep some sort of audit trail in cases you think are controversial or particularly likely to prove contentious.

Practical tips

In practical terms, we recommend that you:

- 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;
- have an inbuilt data protection check at key stages of a story;
- keep an audit trail for decisions you think might be challenged.

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

These checks will not need to be particularly formalised or onerous in most cases, and you may well have suitable policies and procedures in place already which you can review and adapt if necessary. In fact, data protection checks will work best when embedded in existing editorial judgements, practices and procedures. Expert input and a detailed audit trail are only likely to be helpful in difficult or controversial cases.

You might find it helpful to create a standard checklist to suit the needs of your particular organisation, if you don't already have one. This can act both as a reminder and (if you fill it out) an audit trail to record borderline decisions and help you demonstrate that the exemption applies.

What is not exempt

Section 32 can exempt you from most of the DPA, but not all of it. It can never exempt you from:

- Notification. You will still need to register your organisation with the ICO. See The duty to notify in chapter 3.
- 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 in chapter 5 on security.
- The section 55 offence. You will not be exempt from prosecution if you unlawfully obtain, procure or disclose information in breach of section 55. However, there is a public interest defence within section 55 itself. See the section in chapter 3 on The section 55 offence for more information.
- The right to object. If you receive a written request from someone to stop (or not to begin) using their personal data because it is likely to cause them substantial and unwarranted damage or distress (a section 10 notice), you must reply within 21 days either agreeing to stop, or explaining why you think their objection is unjustified.
- The right to opt out of direct marketing. If you receive a written request to stop (or not to begin) using personal data for direct marketing, you must stop within a reasonable period. For more

information, see The Guide to Data Protection – (B)(6)(c) Preventing direct marketing.

- The right to compensation for damage and distress. Individuals have the right to claim compensation from you through the courts if they have suffered damage or distress because you breached the DPA. The exemption does not remove this right. In other words, you cannot argue that you are exempt from paying compensation for a breach. However, you can argue that you did not breach the DPA because you were exempt from the underlying provision. You can also defend a claim on the basis that you took reasonable care in the circumstances to avoid a breach. For more information, see the section on court claims in chapter 6.

Like any other organisation, you will also need to comply with the DPA when handling personal data which is not related to the publication of a particular story – eg HR records, information about your suppliers or customers, information related to marketing and advertising, or information about property management.

Finally, it's worth repeating that you always need to comply with as much of the DPA as you can. Even if a story is clearly in the public interest, if you can reasonably get it in a way which complies with the standard provisions of the DPA, you must.

5 In practice

In brief...

This chapter summarises what this all means in practice, advising on good practice measures and our recommended approach in key areas.

Obtaining information

Key points:

- You should be open and honest wherever possible. In general, people should know if you are collecting information about them.
- Only use covert methods if there is no other way to get the story, and 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 very confident the public interest overrides their right to privacy.

Most 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.

You should collect information in a fair way if at all possible. This means you should have legitimate reasons for collecting the information, tell the person who you are and what you are doing, and not do anything that they wouldn't reasonably expect. In general, people should be aware that you are investigating them or seeking information about them. If you do need to use undercover or otherwise covert methods to get a story, you may be exempt from this requirement if you reasonably believe it is in the public interest to do so – as long as there is no other way to get the story.

The DPA gives more protection to some sensitive categories of information. In particular, you should ensure you have a particularly compelling public interest justification before collecting information about someone's health, sex life or allegations of criminal activity.

Although there is a broad exemption for public interest 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 underhand methods). There is a public interest defence, but currently this holds you to a stricter standard than the usual exemption for journalism. You should therefore be very clear about your public interest justification before using such methods.

Other organisations must also comply with the DPA, and may occasionally be reluctant to disclose information to you for this reason. However, in our view the DPA does not prevent genuine public interest disclosures to journalists.

Other organisations can generally provide you with information about someone without breaching the DPA if they are satisfied that the disclosure is justified in the public interest. If the public interest justification is sufficiently compelling, this would mean that the disclosure would be fair and meet the 'legitimate interests' condition (see page 16), and would not breach the first principle. 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 (see page 17). And, in our view, a genuine public interest disclosure to a journalist would generally not be incompatible with an organisation's purposes, and so would not breach the second principle.

Of course, the issue may really be that the organisation in question does not agree with your view of the public interest, or in fact has other overriding legal, professional or reputational reasons to refuse to disclose the information. They must satisfy themselves that the disclosure would be fair and lawful, and the DPA cannot oblige them to supply you with information if they have doubts.

Keeping contact details

Key points:

- The DPA does not stop you keeping useful contact details, as long as they were obtained legitimately.
- Review them from time to time to ensure they are still up to date and relevant, and delete any you no longer need.

We understand that phone numbers of useful contacts 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.

Contact details will generally be personal data if you intend to store them digitally or in an indexed paper system. You are 'processing' them just by keeping them, so you must comply with the DPA.

If the details are being kept for general future use rather than only for a particular story, the exemption is not relevant. But you can still keep them and comply with the DPA as long as you came across the details legally and the person would be aware you have access to their number. The DPA will recognise your legitimate interest in access to useful contacts in this situation.

The DPA does not impose a time limit, and in some cases it will be reasonable to keep contact details indefinitely. You should however review contact lists from time to time to ensure that the details are still up to date and relevant, and delete any details which you no longer need (eg if a contact has retired or changed their number).

It can be possible to justify holding the contact details of children, but the need to review and justify keeping this information beyond a specific public interest story will be stronger.

Obviously this does not mean you have carte blanche to **use** a phone number however you want – you will still need to use it fairly and reasonably (unless the exemption applies) and keep it secure, especially if it's a home or private mobile number.

Confidential sources

Key points:

- The DPA requires you to protect the identity of your sources.
- You can remove the identity of confidential sources if answering a subject access request as long as it is reasonable to do so.

The media have raised concerns about forced disclosure of sources under the DPA. This concern is likely to arise when the subject of a story makes a subject access request to see the information you have on them.

The DPA allows you to redact the identity of your sources in this situation. You only have to disclose information about a source (or anyone else identified in the information) if they consent, or if it is reasonable to do so. It is unlikely to be reasonable to disclose confidential sources in most cases, unless the requester already knows who it is.

There is no need to use the exemption for this, or rely on the public interest. This is already carved out of subject access rights.

More generally, the identity of your sources will usually itself be personal data. So the DPA actually requires you to keep their identity secure, and any disclosure must be fair and lawful. It is unlikely to be fair or lawful to disclose information about confidential sources in most cases. In other words, the DPA actually requires you to protect your sources.

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.

We recognise that accuracy is, of course, at the very core of a professional journalist's work, and features at the heart of industry codes of practice. Indeed, it forms the very first clause of the Editor's Code:

> **The Editors' Code of Practice**
>
> ***1. Accuracy***
>
> *i) The press must take care not to publish inaccurate, misleading or distorted information, including pictures.*
>
> *ii) A significant inaccuracy, misleading statement or distortion once recognised must be corrected, promptly and with due prominence, and – where appropriate – an apology published. […]*
>
> *iii) The press, whilst free to be partisan, must distinguish clearly between comment, conjecture and fact.*
>
> *ii) A publication must report fairly and accurately the outcome of an action for defamation to which it has been a party, unless an agreed settlement states otherwise, or an agreed statement is published.*

In our view, if you comply with this provision (or similar provisions in other industry codes), you are also likely to comply with the DPA.

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.

No doubt you 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 inaccurate stories 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 any accuracy checks very difficult. As with any use of the exemption, you will still need to show that you gave proper thought to how far you could comply (ie what checks might be possible, and whether you could delay for further checks) and the public interest at stake, and that your decision had some reasonable basis.

Security

Key points:

- You must take reasonable steps to prevent people's information being lost, stolen or misused.
- You will need to consider technical (computer) and physical security measures, your policies and procedures, and staff training and supervision. These should cover staff working both in and outside of the office.

The DPA says 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.

There is no one-size-fits-all answer to what security measures might be appropriate, but you should be able to justify the level of security you have. You should take into account how sensitive or confidential the information you hold is, the harm that might result from its loss or improper use, the technology available, and the costs involved. You 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 likely to be different to the level of security appropriate for information which is publicly available.

You should consider your:

- technical (computer) security. This includes log-on controls, firewalls, encryption, remote wiping facilities, suitable back-ups, and proper disposal of old equipment. You should consider both office computer systems and any mobile devices used out of the office (eg smartphones, laptops or tablets). If you allow people to use their own mobile devices, refer to our Bring Your Own Devices (BYOD) guidance.
- physical security. This includes things like doors and 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.

- 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. You should vet new staff 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 – (B)(7) Information security.

Subject access requests

Key points:

- Ensure you have a process in place for subject access requests.
- Always consider whether you can provide the information (or some of it) without undermining public interest journalism.
- If you decide not to comply with a request, record your reasons.
- You can redact information about the identity of your 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 days. You should not charge more than £10.

You may be able to rely on the exemption to refuse the request if you hold the information in connection with the publication of a story in the public interest, and you believe responding to the SAR would stop you doing your job. However, you are not automatically exempt. If you can

provide the information (or some of it) without undermining your activities, you should do so.

In practice, this means that when you receive a SAR you will need to give proper thought to whether you could respond, and how much information you can provide. If you decide not to 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 be harmful. As with other areas where the exemption might apply, you will need to be able to show you have a proper process for considering requests, and some clear reasons for the decision you made.

The exemption can apply to SARs made before or after publication of a story. However, you might find it harder to justify rejecting a SAR made after publication, as you cannot argue that providing the information will undermine the story by tipping someone off to a forthcoming publication. We would therefore 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. You may still be able to use the exemption after publication, but only if you can explain why you think responding would undermine future investigations or publications, or journalism more generally.

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.

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. You can generally redact references to your confidential sources. You should also consider whether it is reasonable to redact references to anyone else mentioned in the information.

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

General good practice

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 and flag up common data protection issues. 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 on staff who can give detailed case-by-case advice when required.

Corporate governance

Data protection is embedded in existing 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.

6 Disputes

In brief...

The ICO 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 DPA. 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 regulators, and refer issues to them wherever appropriate.

Individuals can also make DPA claims directly through the courts, but only after any relevant story has been published.

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.

We are not a specialist media regulator. Our focus is on compliance with the specific 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 place to usurp that role. We will refer complaints to industry regulators wherever appropriate, and will seek to work with them where our roles overlap. For example, compliance with a code of practice will often be a key factor in our decision on whether the DPA exemption for journalism applies, but it is not our role to decide whether you complied with a code. We would defer on this issue to the relevant industry regulator.

However, this does not mean that industry regulators have the final say on compliance with the DPA. We will take the decision of the industry regulator into account, but we are not bound by its decision. 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 – although in practice we expect this would be rare.

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 certain steps to remedy this. We would usually highlight where improvements are required and ask that you take action to avoid complaints being raised in the future.

In order to impose penalties or 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 general concerns about media conduct or standards, we will generally advise individuals to contact the relevant industry regulator in the first instance, as they are likely to be better placed to deal with the complaint.

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

If the complaint is about your actions in relation to a story which you have not yet published, our powers of investigation are restricted. We can compel you to answer our questions after publication, or if you are not acting with any view to publication.

Our main focus is likely to be on appropriate decision-making processes and procedures. If you can show good internal data protection awareness, clear policies and procedures which include data protection checks, and an audit trail showing you thought about any particularly difficult issues, you will be in a strong position to demonstrate compliance with the DPA.

We will also look at the public interest balance, but we expect that we would only overrule your considered opinion on the public interest in genuinely exceptional cases, or where an industry regulator has found you did not comply with a relevant code of practice.

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 should 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 regulator 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 you 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 that you are either processing the information for other purposes (ie not just for journalism, art or literature), or that you are not intending to publish any previously unpublished material. Our powers to investigate this are limited unless there is a specific complaint or court claim against you. You can appeal this decision to the Information Rights Tribunal. In effect, this means that we cannot take action until after you have published a story.

2. We must then apply to a court for permission to serve the Enforcement Notice. The court must be satisfied that we have reason to suspect a breach of substantial public importance. You will generally be given the chance to defend this application before the court.

3. We can then serve an Enforcement Notice. You can appeal this 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 you 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, but if the breach relates to a story which you have not yet published, our powers of investigation are restricted. We can compel you to answer our questions after publication, or if you are not acting with a view to publication.

You can also appeal to the Information Rights Tribunal against a monetary penalty.

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. There is currently no power to impose a custodial sentence.

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.

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 in cases involving the media. He will have regard to:

- The ICO prosecution policy statement;
- The Code for Crown Prosecutors; and
- 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 because you have breached the DPA, they 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 you to correct, block, erase or destroy the information in question.

You can obviously defend a claim for compensation if you have not breached the DPA, which will include any case where the exemption applies (in essence, if you reasonably believed that the public interest in a story justified what would otherwise have been a breach).

If you did breach the DPA (and the exemption does not apply), you can still defend a claim if you can prove that you took all reasonable care to avoid the breach. In most cases, this is likely to mean showing that you have looked at the way you process and protect personal data, and put appropriate checks in place to prevent problems.

You can also apply to stay the proceedings indefinitely 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) that you answer a subject access request;

- a court order under section 10(4) that you stop any processing which is likely to cause substantial damage or distress;
- a court order under section 12(8) that you reconsider an automated decision (unlikely to be relevant in the context of journalism); or
- a court order under section 14 that you rectify, block, erase or destroy inaccurate data, or any expression of opinion based on inaccurate data (section 14(1)).

If the claim is about information you were using for a story, you can defend it using the exemption for journalism as long as you reasonably believe that the story is in the public interest, and that the court order would stop you doing your job.

You can also apply to stay the proceedings indefinitely if you are still using the information with a view to publishing new material.

Your right to stay pre-publication proceedings

If the claim is 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 you withdraw your 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 the story). You can appeal the Commissioner's decision to the Information Rights Tribunal.

In effect, this means that someone can only make a claim after you have published a story, and 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 0.4 (DRAFT FOR CONSULTATION)
23 January 2014