Information Commissioner's Office

Data protection and journalism code of practice

ico.
Information Commissioner's Office

Contents

Information Commissioner's foreword

With so much more information at our fingertips, rapid changes to technology, and concern about access to accurate information, trusted journalism has never been more important.

A free media is at the heart of any healthy democracy – keeping us informed, encouraging debate and opinion, and entertaining us. It is a crucial part of the fundamental right to freedom of expression and information.

A free media is also often called the public's watchdog because of its role in uncovering wrongdoing and holding the powerful to account.

In 2011-2012, the Leveson Inquiry examined the media's own power, finding that there was a culture of unethical practices in parts of the press. This followed evidence of unlawful information gathering by some media organisations.

The crucial public interest role served by the media and its power is the reason journalism is covered by data protection law. The law includes important provisions that enable journalism, whilst also protecting people by ensuring that personal information is used lawfully.

As required by Parliament, I have produced this code to help the media apply data protection law in a journalism context. It builds upon guidance for the media we published in 2014 following a recommendation from the Leveson Inquiry.

Constructive feedback from a wide range of stakeholders, including industry representatives, media organisations, civil society, lawyers and academics has shaped the code from the beginning and at each stage of the consultation process.

I am grateful to everyone who helped develop this code and complete what is rightly a challenging task. I understand that there will always be strongly held views and convictions whenever fundamental rights are concerned.

I believe this is a clear and practical code, which strikes the right balance between supporting journalists' work and protecting people's personal information.

By continuing to work with industry and others, the code will make an important contribution, complement existing industry codes and help build public trust in journalism. Ultimately, that will support the vital public interest journalism serves.

John Edwards
UK Information Commissioner

1. About this code

You **must** generally comply with the requirements of data protection law when you use personal information for journalism. In a lot of cases, this is straight-forward.

You can, however, apply the **journalism exemption** when you meet certain criteria. When you apply it, you no longer have to comply with specific requirements of data protection law.

You can apply the exemption to most requirements as specified in the highlighted boxes at the start of each section of the code.

To apply the exemption, you **must**:

- use personal information for a journalistic purpose;
- act with a view to the publication of journalistic material; and
- reasonably believe both that:
    - publication would be in the public interest; and
    - complying with a specific requirement would be incompatible with your journalistic purpose.

See Apply the journalism exemption for more information.

1.1 This is a statutory code of practice under the Data Protection Act 2018 (DPA 2018).

1.2 This code applies to anyone using personal information for journalism. However, it is mainly for media organisations and journalists including the press, broadcasters, and online media outlets.

What is personal information?

Personal information is any information about a living and identifiable person, that is, or will be, stored on a digital device or kept in an organised way. Personal information means the same as "personal data" in the UK GDPR.

1.3 This code is about data protection law. It does not concern press standards in general but is intended to complement industry codes.

1.4 This code will help you understand what data protection law says, focusing on its key principles. It will help you comply effectively with the law in practical ways, explained where possible in a journalism context, taking into account the special public interest in freedom of expression and information.

1.5 To help you understand what the law says, we say **must** in the code when doing something is a legislative requirement. However, you no longer have to comply with specific requirements when the journalism exemption applies.

1.6 To help you comply with the law, we say **should** when something is good practice, not a legislative requirement. If you choose to take a different approach, you **must** be able to demonstrate that your approach complies with the legislation.

1.7 We must review this code and how personal information is used for journalism periodically.

1.8 Further information is set out in the code's supporting Reference notes, which are not part of the code itself. These also link to our wider guidance to help you comply with data protection law.

2. Demonstrate how you comply

You cannot apply the **journalism exemption** to the requirement to demonstrate how you comply. However, if you meet the criteria to apply the exemption, you no longer have to comply with the specific requirement to consult us if a Data Protection Impact Assessment (DPIA) reveals a high risk you cannot mitigate (see Apply the journalism exemption).

What does the legislation say?

2.1 You **must** be able to demonstrate how you comply with the data protection principles. This is a key principle of data protection law which you cannot apply the journalism exemption to.

2.2 To be able to demonstrate how you comply, you **must** implement appropriate and proportionate data protection measures and update them when you need to.

2.3 To decide what measures are appropriate and proportionate, you **must** consider:

- what personal information you are using;
- what you plan to do with it and why;
- the wider context, including the special public interest in protecting freedom of expression and information; and
- the risk of harm (see 2.3 in Reference notes).

2.4 You **must** integrate data protection into any system, service, product, policy or process you design that involves personal information.

2.5 Where proportionate, you **must** put in place data protection policies to make sure that all the personal information you use is in line with data protection law and complies with its key principles.

2.6 You **must** have a Data Protection Officer (DPO), if legally required (see 2.6 in Reference notes).

2.7 If you have 250 or more employees, you **must** keep specific records about your use of personal information. This includes records about any use of special category or criminal offence data (see Use personal information lawfully). There is a limited exemption for smaller organisations (see 2.7 in Reference notes).

2.8 You **must** do a DPIA if there is likely to be a high risk (see 2.8 in Reference notes). For example, this is more likely if you are using special category or

criminal offence data or using intrusive methods such as covert surveillance (see Use personal information lawfully and Use personal information fairly).

2.9 However, you do not necessarily need to do a DPIA for individual stories. Your DPIA can generally cover the high-risk ways you may use personal information for journalism. For example, particularly intrusive techniques, such as surveillance or subterfuge, which you may use for investigative journalism (see Use personal information fairly).

What is a DPIA?

A DPIA is a form of risk assessment. The UK GDPR says that as a minimum it **must** describe:

- how you plan to use personal information and why;
- whether it is necessary and proportionate to use it; and
- how you plan to manage the risks.

How do we comply?

Managing risk

2.10 The principle to demonstrate how you comply is very flexible, with few strict rules. It allows you to use your discretion about how best to comply with data protection law while also enabling journalism.

2.11 What measures are appropriate and proportionate is based largely on risk. Generally, the greater the risk of harm to people, the more you **should** do to protect personal information.

2.12 You **should** consider risks that can be significant, such as discrimination, financial loss, damage to reputation or loss of confidentiality. However, much of the day-to-day work of journalists will not be high risk.

2.13 When there is a high risk, you do not necessarily need to do a DPIA for individual stories. Your DPIA can generally cover the different ways you use personal information for journalism and types of information likely to pose higher risks, such as special category and criminal offence data (see Use personal information lawfully).

Implementing data protection measures

2.14 There is no one-size fits all approach. You **should** consider how best to implement data protection measures within your organisation, so they are effective whilst still enabling journalism.

2.15 You do not need to have standalone policies or processes that are dedicated to data protection. For example, data protection can form part of your existing editorial and legal processes.

2.16 Whatever approach you take, it **should** cover all the personal information you use and:

- encourage good data protection practice;
- be clear about who is responsible for complying;
- give staff appropriate training; and
- practice good records management.

Demonstrating how you comply

2.17 Based on the risk, you **should** be able to give a clear and practical explanation of the steps you take to comply and, where appropriate and proportionate, be able to show how you comply.

3. Keep personal information secure

You cannot apply the **journalism exemption** to the requirement to keep personal information secure. However, if you meet the criteria to apply the exemption, you no longer have to comply with the specific requirement to tell people affected by a data breach when there is a high risk (see Apply the journalism exemption).

What does the legislation say?

3.1 You **must** keep personal information secure. To do this, you **must** have appropriate, proportionate security measures, and update them when needed.

What is a security measure?

Security measures include cyber-security, organisational measures, and physical security.

3.2 To decide what measures are appropriate and proportionate, you **must** consider the same factors you do when you are demonstrating how you comply (see Demonstrate how you comply). However, you **must** also consider the available technology and the cost of security measures.

3.3 You **must** be able to restore personal information if there is a security incident as soon as possible (eg a backup system).

3.4 You **must** ask anyone acting on your behalf to demonstrate they can keep personal information secure (see Be clear about roles and responsibilities).

3.5 You **must** keep a record of personal information breaches and tell us as soon as possible if the breach is likely to cause harm to someone.

What is a personal information breach?

A personal information breach occurs if personal information is used in an unauthorised or unlawful way, is accidentally lost, destroyed, or damaged.

3.6 You **must** tell anyone affected by the breach if there is likely to be a high risk.

How do we comply?

3.7 The code's guidance about demonstrating how you comply is also generally applicable to security (see Demonstrate how you comply).

Managing risks

3.8 To decide what security measures are appropriate and proportionate, you **should** consider significant risks and factors, such as:

- your organisation's premises and computer systems;
- who has access to personal information; and
- any personal information a third party uses on your behalf.

3.9 In some cases, a security breach could pose a risk to someone's physical health and safety. For example, if a breach could identify a journalist's confidential source. In that case, you **should** have strong security measures, including strict measures controlling access.

3.10 Reviewing and updating your security measures **should** include scanning for network vulnerabilities to prevent risks developing that compromise your security.

Implementing security measures

3.11 There are a wide range of low-cost and easy to implement cyber-security solutions. You **should** consider common techniques such as encryption and password protection. You **should** also secure physical locations.

Working flexibly and travel

3.12 Journalism often relies on remote working and portable devices. You **should** consider how you keep your IT equipment secure, especially portable media and devices. You **should** consider the increased security risks if you allow employees to work remotely or use their own devices for work purposes.

3.13 If your employees are travelling with personal information, you **should** train them to follow fundamental security advice and be aware of common security issues.

4. Use personal information lawfully

If you meet the criteria to apply the **journalism exemption**, you can rely on it to make sure your use of personal information is lawful, rather than relying on one of the usual data protection lawful bases, such as legitimate interests or consent. This section of the code sets out what the legislation says and how to comply when you are **not** applying the exemption (see Apply the journalism exemption).

What does the legislation say?

4.1 You **must** use personal information lawfully. This means relying on one of the six specific lawful bases in data protection law and acting in line with other laws.

4.2 In most day-to-day journalism, the legitimate interests lawful basis is likely to be the most appropriate basis. It often applies in a straight-forward way when you need to use personal information to pursue your legitimate interests and those interests are not outweighed by any harm caused to a person.

4.3 If you use the consent lawful basis, you **must** comply with the specific high standards and meaning of UK GDPR consent. There will often be circumstances where other lawful bases are likely to be more appropriate, in particular legitimate interests.

What does UK GDPR consent mean?

Consent has a specific legal meaning in the UK GDPR. It is different from asking someone as a general courtesy whether it is ok to use their personal information. The UK GDPR sets high standards for consent. If you use the UK GDPR consent lawful basis, your request for consent **must** be easily accessible, clear and in plain language. You **must** provide consent by a positive, opt-in action that someone can easily withdraw at any time.

4.4 If you are offering an online service directly to children, such as a news website for children, only those aged 13 or over can provide UK GDPR consent. You **should** also consider our Children's code of practice.

Sensitive types of personal information

4.5 There are some specific types of personal information that are more sensitive and merit additional protection in data protection law. These types of information are known as special category and criminal offence data.

4.6 If you are using special category data, you **must** have a lawful reason **and** meet a separate condition. For some of these, you **must** also meet additional conditions and safeguards that are set out in Schedule 1 of the DPA 2018.

4.7 If you are using criminal offence data, you **must** have a lawful reason **and** meet a relevant condition under Schedule 1 of the DPA 2018.

Special category data

What is special category data?

Special category data is personal information revealing or concerning:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where used for identification);
- health;
- sex life; or
- sexual orientation.

4.8 If you are using special category data, you **must** rely on one of the six lawful bases **and** meet a separate condition.

4.9 For some of the conditions that apply to special category data, you **must** also meet additional conditions and safeguards.

4.10 There are 10 conditions that can give you a valid reason for using special category data. Those most likely to be relevant to journalism are:

- you have explicit consent;
- the personal information is manifestly made public by the person it is about; or
- there is a substantial public interest with a reason in law.

4.11 If you are considering the manifestly made public condition, personal information is made public if it is realistically accessible to a member of the public. This includes if it is only accessible to part of the public.

4.12 If you want to use the condition relating to a substantial public interest, there are 23 "substantial public interest conditions" that provide a valid reason in law.

4.13 There are two substantial public interest conditions that may be particularly relevant in a journalism context. One applies if you need to use personal information for the administration of justice because journalists have an important role in increasing the transparency of the justice system. Another applies when, in certain circumstances, personal information is disclosed to you for journalism in connection with unlawful acts and dishonesty.

4.14 If you want to use the substantial public interest condition concerning the administration of justice, you **must** have an Appropriate policy document (see 4.14 Reference notes).

Criminal offence data

What is criminal offence data?

Criminal offence data covers a wide range of information about:

- criminal activity;
- allegations;
- investigations;
- proceedings;
- penalties;
- conditions or restrictions placed on someone as part of the criminal justice process; or
- civil measures that may lead to a criminal penalty, if not adhered to.

4.15 If you are using criminal offence data, you **must** have a lawful reason and meet a relevant condition.

4.16 There are 28 conditions that allow you to use criminal offence data. Those most likely to be relevant to journalism are:

- consent (this does not need to be explicit in the case of criminal offence data);
- the personal information is necessary for the administration of justice;
- personal information is disclosed for journalism relating to unlawful acts and dishonesty; and
- personal information is manifestly made public by the person it is about (see above).

How do we comply?

4.17 From the start, you **should** choose the lawful basis that appears to be most relevant in the circumstances and consider if more than one applies. It is likely to be unfair to change your lawful basis at a later stage (see Use personal information fairly).

4.18 The lawful basis most relevant to journalism is legitimate interests. The consent lawful basis is likely to be the next most common, but only applies when you are giving people genuine control over how you use their personal information and you meet the standards of UK GDPR consent.

The legitimate interests lawful basis

4.19 In most day-to-day journalism, the legitimate interests lawful basis is likely to be the most appropriate basis. It often applies in a straight-forward way when there is a legitimate interest in pursuing journalism and it is clear that this is not outweighed by the interests of the person the information is about.

4.20 In many cases, journalists do not need to do anything more than simply highlight privacy information, unless the journalism exemption applies (see Apply the journalism exemption). Most organisations publish a privacy notice on their website (see Use personal information transparently).

4.21 A legitimate interest may be a public interest or a commercial interest. For example, many media organisations are commercial enterprises with a legitimate interest in selling news. Much of the freedom of the press, its diversity, and the societal value we derive from it, depends on being commercially successful.

4.22 In the context of journalism, there is a public interest in the right to freedom of expression and information that is protected by the Human Rights Act 1998 (HRA). A free press is vital to exercising this right (see Apply the journalism exemption for more detail).

4.23 If it is not already obvious that you have a legitimate interest that is not outweighed by harm to a person, you **should** consider the specific circumstances in more detail. This includes whether there is another reasonable and less intrusive way to achieve the same result and you can justify any harm.

4.24 You **should** take extra care if:

- there are significant risks involved (see Demonstrate how you comply);
- you are using sensitive types of personal information, especially special category or criminal offence information (see below); or

- you are using personal information about children or other people who may be less able to understand the risks (see Use personal information fairly).

The consent lawful basis

4.25 Although you are likely to rely on the legitimate interest lawful basis most often in a journalism context, you may sometimes use one of the other lawful bases, such as consent. For example, if you want to use sensitive types of personal information (see below).

4.26 Before deciding to rely on the consent lawful basis, you **should** consider whether it is the most appropriate basis. People can withdraw consent at any time which, in many circumstances, may be difficult in the context of journalism.

4.27 If you decide to use the consent lawful basis, you **should** take extra care with people less likely to understand consent, such as children. You **should** consider their competence to consent.

Special category personal data

4.28 Before you use special category data, you **should** consider why you want to use it. This will help you choose a lawful basis and condition, and where relevant, a further condition and safeguard.

4.29 If you want to use the explicit consent condition, you **should** make sure that the consent you receive is expressly affirmed in a clear statement, whether verbal or written.

4.30 If you want to use the condition relating to personal information that is manifestly made public, it **should** be clear and obvious that the person concerned has made the personal information publicly available. The use of the word "manifestly" reflects the specific, extra protection given to special category and criminal offence by data protection law (see also Use personal information fairly).

4.31 The condition about disclosures relating to unlawful acts and dishonesty may be relevant if a whistle-blower discloses information to you. You may need to consider whether the journalism exemption applies if you want to use the information (see Apply the journalism exemption).

Criminal offence personal data

4.32 Before you use any criminal offence data, you **should** consider why you want to use it. This will help you choose a relevant lawful basis and condition.

4.33 If you are considering the necessary for the administration of justice condition, you **should** remember that once a person is charged with a criminal offence, the open justice principle generally means you can identify the person charged.

5. Use personal information fairly

If you meet the criteria to apply the **journalism exemption**, you no longer have to comply with the requirement to use personal information fairly. This section of the code sets out what the legislation says and how to comply when you are **not** applying the exemption (see Apply the journalism exemption).

What does the legislation say?

5.1 You **must** use personal information fairly. To do this, you **must** also use it lawfully and transparently. These are part of the same data protection principle (see also Use personal information lawfully and Use personal information fairly).

How do we comply?

5.2 To use personal information fairly, you **should** use it in ways people reasonably expect **or** you **should** be able to justify any unexpected use.

Reasonable expectations

5.3 You **should** consider all the circumstances to decide whether using personal information is within someone's reasonable expectations.

5.4 When considering a person's reasonable expectations, it may be relevant for you to consider whether a reasonable person would consider that the information is private in the circumstances.

5.5 Not all personal information is private (see About this code). However, if there might be a reasonable expectation of privacy, considering this may help you judge a person's expectations more clearly, as well as the strength of any such expectation.

5.6 There are some types of information that are generally more sensitive in nature, and which may also be private (see Sensitive types of information below). However, the courts consider all the circumstances to help them decide whether a reasonable expectation of privacy exists, including the extent to which information is already in the public domain where relevant.

Unwarranted harm

5.7 You **should** act proportionately, taking into account the public interest in using the personal information and any harm to the person concerned. You **should** be able to justify any harm in view of the person's reasonable expectations (see above).

5.8 If personal information is private, to decide whether using it is justifiable, the courts balance the right to freedom of expression and information and the right to privacy in line with the HRA where relevant (for further detail about how the courts balance these rights, see Apply the journalism exemption and the Reference notes).

When to take particular care

5.9 You **should** take particular care to consider fairness when using some types of personal information and in some circumstances. This is because there is more likely to be a greater risk of harm generally when you are:

- using sensitive types of personal information, particularly special category or criminal offence data;
- using personal information about children or other people who may be more at risk of harm; or
- there is a risk of discrimination, financial loss, damage to reputation, loss of confidence or a risk of physical harm (see Demonstrate how you comply).

Sensitive types of information

5.10 While you **should** always consider all the circumstances, there are certain types of personal information that are generally more sensitive in nature, and which may also be private. For example, personal information about:

- someone's home life;
- correspondence or finances; or
- a victim or a witness to a crime.

5.11 Special category data is given extra protection in data protection law because it is generally more sensitive. This is because using this type of personal information is more likely to pose significant risks to a person's fundamental rights and freedoms, or risk discrimination (see Use personal information lawfully).

5.12 Criminal offence data is also given extra protection in the UK GDPR (see Use personal information lawfully). The interests of society, such as protecting the public from criminal activity, are however likely to mean that you can justify the

use of criminal offence data in a wider variety of circumstances than special category data.

5.13 The principle of open justice means that post-charge the media can generally report on criminal trials (see Use personal information lawfully) and play a crucial part in ensuring the transparency of the justice system.

5.14 Criminal offence data includes allegations about criminal activity. If you are considering using this type of personal information, you **should** consider any reasonable expectations of privacy and any risk of serious harm to the suspect, particularly reputational harm.

5.15 If you decide to use personal information about a criminal allegation, you **should** make sure you can justify this. You **should** consider the circumstances, taking into account any specific public interest.

Children and other vulnerable people

5.16 You **should** take extra care when dealing with personal information about children or any other people who may be more at risk of harm. For example, some elderly people or those with certain disabilities. This is because they may be less able to understand the risks of what you are doing with their personal information.

Intrusive methods

5.17 Covert surveillance and subterfuge are particularly intrusive methods that you are more likely to deploy in investigative journalism. Such techniques include using private detectives, covert recording, disguise, and long-lens photography.

5.18 As these methods are particularly intrusive, you **should** take extra care to consider whether it is proportionate or if there is a less intrusive way to achieve your journalistic purpose.

5.19 It is likely that in some cases (such as covert surveillance), these methods will be incompatible with some of the usual requirements of data protection law, such as transparency. Where this is the case, you can consider whether you meet the criteria to use the journalism exemption (see Apply the journalism exemption).

5.20 You **should** carefully consider the strength of the public interest in publishing, taking into account harm to the person concerned. There is likely to be a greater risk of harm if you are using sensitive types of personal information (see above).

Considering fairness in specific circumstances

5.21 You **should** always consider the specific circumstances to decide whether it is fair to use personal information, including when considering using personal

information about people who fall within certain groups or who are in certain situations. You **should** avoid making general assumptions about what people may reasonably expect or what would be a justifiable use of their personal information.

Professionals and business people

5.22 For example, generally a senior business person at a large company may expect a greater level of scrutiny about their role. However, this is not automatically the case and personal information about people acting in a professional or business capacity can still be private, such as special category or criminal offence data.

People with a role in public life or public profile

5.23 Generally, those playing a role in public life may also expect a greater level of scrutiny about their role (eg politicians and senior public officials). However, again, this is not automatically the case. Someone with a public role, or who has a public profile for other reasons, may attract or seek publicity about some aspects of their life without necessarily losing the right to privacy about other matters.

5.24 If you are considering allegations about those with a role in public life or a public profile, damage to their reputation may have a greater impact and they may also be more vulnerable to false allegations.

Public places

5.25 The public nature of the activity under consideration may generally mean that someone can either no longer reasonably expect privacy or that expectation may be significantly reduced. However, it is not automatically fair to publish personal information simply because an activity is happening in a public place. This is one factor to consider, but you **should** consider all the relevant circumstances.

5.26 People should reasonably expect that they may sometimes be photographed or caught on film in public in an incidental way, but you **should** always consider the circumstances to decide whether using their personal information is fair. For example, who the person is, what they are doing and any harmful impact on them.

5.27 An arrest in public does not automatically mean that someone cannot have any reasonable expectation of privacy or that publishing the personal information is justified in all circumstances (see above Sensitive types of information).

6. Use personal information transparently

If you meet the criteria to apply the **journalism exemption**, you no longer have to comply with the requirement to use personal information transparently. This section of the code sets out what the legislation says and how to comply when you are **not** applying the exemption (see Apply the journalism exemption).

What does the legislation say?

6.1 You **must** use personal information transparently. In particular, you **must** provide privacy information to people including:

- why you are using the personal information;
- how long you expect to keep it; and
- where relevant, who you will share it with.

6.2 If you obtain personal information from the person it is about, you **must** provide privacy information to them unless they already have it.

6.3 When you obtain personal information from a source other than the person it is about, you do **not** need to provide privacy information in some circumstances (see 6.3 in Reference notes). For example, if it would be impossible, involve disproportionate effort, or seriously impair your journalistic objective.

6.4 You **must** provide privacy information to people at the time you collect their personal information from them unless they already have it.

6.5 If you obtain personal information from a source other than the person it relates to, you **must** provide privacy information to them within a reasonable period of obtaining it and no later than one month. If you plan to communicate with the person or disclose the information, you **must** provide privacy information at the latest at the time of the first communication or when you disclose the information, including by publishing it.

6.6 The privacy information you provide **must** be concise, easy to understand in clear and plain language and easily accessible.

6.7 You **must** bring any new uses of a person's personal information to their attention before you use it for that purpose (see also Use personal information for a specified purpose).

6.8 You **must** regularly review and update privacy information, when needed.

How do we comply?

6.9 If you obtain personal information from the person it is about, there are no exceptions to the requirement to provide privacy information, unless you have already provided it to them. However, the journalism exemption may apply if you reasonably believe it would be incompatible with your journalistic purpose to provide privacy information (see Apply the journalism exemption).

6.10 However, there are exceptions available if you obtain information from a source other than the person it relates to. This includes if it would be impossible or would involve disproportionate effort. For example, you do not have relevant contact details and could not reasonably obtain them, or you have used a large number of different sources.

6.11 You also do not need to provide privacy information if it would seriously impair your journalistic purpose. This gives you an alternative means of protecting your journalistic purpose other than applying the journalism exemption.

6.12 You **should** actively provide privacy information. For example, you can put a privacy notice on your website, as long as you make people aware of it and give them an easy way to access it.

6.13 There are different ways to provide privacy information. You **should** think about who it is for to help you decide the best way to communicate the information.

6.14 You **should** take particular care to write clear, age-appropriate privacy notices for children or other groups who may be more at risk of harm and less able to understand what will happen to their personal information and what rights they have.

7. Use accurate personal information

If you meet the criteria to apply the **journalism exemption**, you no longer have to comply with the requirement to use accurate personal information. This section of the code sets out what the legislation says and how to comply when you are **not** applying the exemption (see Apply the journalism exemption).

What does the legislation say?

7.1 You **must** use personal information that is accurate and, where necessary, keep it up-to-date.

What does accurate mean?

Accurate means correct or not misleading as to any matter of fact.

7.2 You **must** take reasonable steps to make sure that personal information is accurate, even in lower profile stories.

7.3 In some circumstances, you may not be able to carry out your usual accuracy checks. However, you **must** still be able to demonstrate that you considered what steps are reasonable and how to manage the risks appropriately (see Demonstrate how you comply).

7.4 If people complain that you have used inaccurate personal information about them, you **must** help people to exercise their individual rights under data protection law (see Help people to use their rights).

How do we comply?

7.5 Personal information does not become inaccurate because of new facts that did not exist at the time. For example, personal information contained in news archives remains accurate as long as it is clear that it is part of a news archive.

7.6 If personal information is deliberately inaccurate, and this is obvious from the context, it is unlikely to breach the accuracy principle (eg satire or parody).

7.7 A record of an opinion is not necessarily inaccurate personal information just because someone disagrees with it, or it is later proven to be wrong. Opinions are, by their nature, subjective and not intended to record matters of fact.

Reasonable steps to make sure personal information is accurate

7.8 To take reasonable steps to make sure personal information is accurate, you **should**:

- make sure the source of the information is clear where possible;
- consider challenges about accuracy as appropriate; and
- consider whether you need to update the information.

7.9 To decide what is a reasonable step, you **should** consider the circumstances, in particular, the nature of the personal information and what you are using it for. Generally, the greater the risk of harm to someone, the more thoroughly you **should** check that you are using accurate personal information.

7.10 You can consider the journalistic context when deciding what steps are reasonable to make sure personal information is accurate. There may be some circumstances when it is in the urgent public interest to publish personal information without carrying out your normal accuracy checks. For example, this may occur when broadcasting live. However, someone at an appropriate level **should** always consider whether it is reasonable to publish or broadcast personal information and consider how to manage the risks.

7.11 If possible, you **should** be clear about the source of the personal information when you publish or broadcast a story. When you need to protect a source, you may still be able to give some general information (eg about their status).

7.12 You **should** take particular care when using online material, especially social media, or other user-generated content, which may be mistakenly or deliberately inaccurate and is easily spread.

7.13 Wherever appropriate and proportionate, you **should** keep records about your sources and other research that you use to report someone's personal information. This allows others to verify the accuracy of the information you use where necessary, such as if there is a later dispute.

7.14 To decide whether you need to update personal information, you **should** consider what you are using it for. If the information needs to be current for you to use it, you **should** take proportionate steps to keep it up-to-date.

8. Use personal information for a specified purpose

If you meet the criteria to apply the **journalism exemption**, you no longer have to comply with the requirement to use personal information for a specified purpose. This section of the code sets out what the legislation says and how to comply when you are **not** applying the exemption (see Apply the journalism exemption).

What does the legislation say?

8.1 You **must** use personal information for a specified purpose that is legitimate and clear. If you want to use it for a different purpose, this **must** be compatible with your original purpose.

How do we comply?

8.2 This data protection principle is closely linked to other principles. As long as you comply with the other principles, you are unlikely to need to do anything more to comply.

8.3 You can use personal information for a new purpose if it is in line with your original purpose. For example, keeping personal information for a news archive is still using it for journalism because this is part of the end-to-end process.

8.4 If you are not sure whether using the information for another purpose is compatible, factors you **should** consider include:

- any link between the original and new purpose;
- how you collected the personal information and people's reasonable expectations;
- the nature of the personal information and any harm; and
- how you will keep the personal information safe.

8.5 It is not likely to be compatible if you are using personal information for a purpose that is very different, unexpected, or which would have an unjustified impact on people. However, you can consider whether the person would consent (see Use personal information lawfully).

8.6 You **should** regularly review how you use personal information to check that your purposes have not changed over time.

9. Use only the personal information you need

What does the legislation say?

If you meet the criteria to apply the **journalism exemption**, you no longer have to comply with the requirement to use only the personal information you need. This section of the code sets out what the legislation says and how to comply when you are **not** applying the journalism exemption (see Apply the journalism exemption).

9.1 You **must** use personal information that is:

- adequate (enough to do what you need to do);
- relevant (has a rational link to that purpose); and
- limited (not more than you need for that purpose).

9.2 You **must** also use accurate personal information. This also involves considering how much you need to be factually accurate and not misleading (see Use accurate personal information).

9.3 You **must** only use personal information that is relevant.

How do we comply?

9.4 Before you collect any personal information, you **should** think about why you need it. This will help you to decide whether you have the information you need for your journalistic purpose.

9.5 You **should** keep in mind what you are trying to achieve and aim to collect only the personal information you need to do that efficiently.

9.6 Using irrelevant personal information may cause significant harm to people, especially when you use special category or criminal offence data. This is because this type of personal information is more likely to interfere with someone's fundamental rights or open them up to discrimination (see Use personal information lawfully).

9.7 Even if personal information is not obviously relevant to a specific story, it can still be relevant to your wider journalistic purpose. However, you **should** be able to justify this (see Keep personal information only for as long as you need it).

9.8 To make sure you do not use excessive personal information, you **should** think about what personal information you need at the different points in the journalistic process as your story develops.

9.9 You **should** periodically review the information you hold to make sure you do not have more than you need for your purpose (see Keep personal information only for as long as you need it).

10. Keep personal information only for as long as you need it

If you meet the criteria to apply the **journalism exemption**, you no longer have to comply with the requirement to keep personal information only for as long as you need it. This section of the code sets out what the legislation says and how to comply when you are **not** applying the journalism exemption (see Apply the journalism exemption).

What does the legislation say?

10.1 You **must** only keep personal information for as long as you need to. How long it is appropriate to keep personal information for varies depending on the circumstances, however you **must** be able to justify how long you keep it.

10.2 You **must** also consider the risk of harm to a person if you keep personal information. You **must** only keep it if it is fair and lawful to do so (see Use personal information fairly, Use personal information lawfully and Use personal information transparently).

10.3 You **must** record how long you expect to hold different types of personal information, where possible, and review this at appropriate intervals (see Demonstrate how you comply).

How do we comply?

10.4 There are no specific time limits, so you **should** consider why you are using the personal information to decide how long it is reasonable to keep it. You are best placed to decide this, based on the circumstances, but you **should** establish time limits to delete or erase personal information and to conduct a periodic review.

10.5 If it is appropriate to delete personal information from a live system, you **should** also delete it from any back-up system.

Research and background materials

10.6 Research and background details, such as contact details, are vital to journalism, so you may often be justified in keeping this personal information for long

periods of time or indefinitely. You **should** review any personal information you decide to keep to make sure you still need it.

11. Be clear about roles and responsibilities

You cannot apply the **journalism exemption** to the specific requirements in this section. However, if the criteria to meet the exemption is met, you no longer have to comply with the general principles for restricted transfers of personal information (see Apply the journalism exemption).

What does the legislation say?

What does controller, joint controller and processor mean?

Controller is a term used in the UK GDPR to describe the main decision-making body who has control over why and how personal information is used.

If two or more controllers jointly decide why and how the same personal information is used, they are joint controllers. If the information is being used for different purposes, they are not joint controllers.

Processors act on behalf of, and only on the instructions of, the relevant controller.

11.1 If acting as a joint controller, you **must** have an agreement with the other party or parties that sets out your respective responsibilities, particularly about transparency and individual rights. You **must** make this information available to people.

11.2 Whenever you use a processor, you **must** have a written contract with them. You **must** also make sure any processors you use give you sufficient guarantees that they will meet the UK GDPR's requirements and protect people's rights.

11.3 When sharing personal information or receiving it, you **must** comply with the data protection principles. In particular, you **must**:

- share personal information lawfully, fairly, and transparently (see Use personal information lawfully, Use personal information fairly and Use personal information transparently); and
- take reasonable steps to check it is accurate (see Use accurate personal information).

11.4 You **must** keep certain records whenever you share personal information and you **must** carry out a DPIA, if needed (see Demonstrate how you comply).

How do we comply?

11.5 If you are dealing with personal information and any third parties, you **should** decide whether they are a controller, joint controller, or a processor under the UK GDPR because this affects legal responsibilities.

11.6 To decide whether a third party is a controller, joint controller, or processor, you **should** consider the nature of the activities they are carrying out and how much control they have over why and how information is used.

11.7 For example, private investigators, freelance photographers, and freelance journalists are likely, in many cases, to be controllers because they are likely to have a significant degree of independence.

11.8 If you ask a third party to help you with a story and they are permitted to act **only** on your instructions, they are a processor, even if they make some technical decisions about how to use personal information.

Sharing personal data

11.9 You **should** consider our Data sharing code of practice to help you comply with the law and good practice when sharing personal information.

International data transfer rules and online publication

11.10 There are specific rules about making international data transfers. These do **not** apply to online publication, even if this makes information available outside the UK.

12. Help people to use their rights

If you meet the criteria to apply the **journalism exemption**, you no longer have to comply with the specific rights people can exercise relating to their personal information, except for rights about automated uses of personal information. This section of the code sets out what the legislation says and how to comply when you are **not** applying the journalism exemption (see Apply the journalism exemption).

What does the legislation say?

12.1 People have specific rights they can exercise relating to their personal information. This code focuses on rights most likely to be relevant to journalism (see also Use personal information transparently and our separate guidance about automated use of personal information).

12.2 People can make requests in writing or verbally to use their rights. If someone makes a request, you **must** comply with it without undue delay and within one month. However, you can extend the time to respond in certain circumstances (see 12.2 in Reference notes).

12.3 You **must** be able to justify any decision you take to refuse someone's request. You can refuse to respond to a request if:

- an exemption applies (eg see Apply the journalism exemption); or
- it is manifestly unfounded or manifestly excessive.

12.4 If you refuse to comply with a request, you **must** tell the requester why and that there is a right to complain to us and the court.

Right of access

12.5 People have the right to ask you to:

- confirm you are using their information;
- give them access to it; and
- provide other supplementary information.

12.6 You **must not** give someone personal information about another person in response to an access request, unless:

- the other person has consented (see Use personal information lawfully); or

- it is reasonable to disclose it without their consent. There is very strong legal protection for a journalist's sources.

Right to restriction

12.7 People have the right to ask you to restrict the use of their personal information in certain circumstances (see 12.7 in Reference notes).

12.8 You **must** be able to restrict personal information, if required. For example:

- by temporarily moving it to another system;
- making it unavailable to users; or
- temporarily removing published personal information from a website.

12.9 You **must** tell each recipient of the personal information that you have restricted it unless this proves impossible or involves disproportionate effort. If the person concerned wants to know who these recipients are, you **must** tell them.

12.10 In many cases, the restriction is only temporary. You **must** tell the person concerned before you lift the restriction.

Right to correct or complete personal information

12.11 People have a right to ask you to correct their personal information if it is inaccurate, or to complete it if it is incomplete. If necessary, you **must** correct or complete personal information.

12.12 You **must** tell recipients about any correction or completion unless this proves impossible or involves disproportionate effort. If the person concerned wants to know who these recipients are, you **must** tell them.

Right to object

12.13 People have the right to object to the use of their personal information in certain circumstances (see 12.13 in Reference notes).

12.14 You **must** clearly tell people about their right to object when you first communicate with them at the latest.

12.15 If you have no reason to refuse the objection, you **must** stop using the personal information (see 12.15 in Reference notes).

Right to erasure

12.16 People have the right to have their personal information erased without undue delay in certain circumstances (see 12.16 in Reference notes).

12.17 Crucially, the right to erasure does **not** apply if it is necessary for you to use the information to exercise the right to freedom of expression and information.

12.18 If personal information is made public and you are required to erase it, you **must** take reasonable steps to inform other parties with legal responsibility for using it that the requester has asked them to erase any links to, or copies of, the personal information.

12.19 You **must** tell recipients about any erasure unless this proves impossible or involves disproportionate effort. If the person concerned wants to know who these recipients are, you **must** tell them.

How do we comply?

Right of access

12.20 If you are considering the right of access, you **should** make reasonable efforts to find relevant information.

Right to correct or complete personal information

12.21 Personal information, such as that contained in news archives, does not become inaccurate because of new facts that did not exist at the time (see Use accurate personal information).

12.22 However, if a person exercising this right brings to your attention that their personal information in the news archive was inaccurate when you used it, you **must** correct or complete it, where necessary.

12.23 As long as it is clear that someone is expressing an opinion, you are unlikely to need to correct or complete it. Opinions are subjective by their nature. The courts have developed well-established principles to distinguish between fact and opinion (see 12.23 in Reference notes).

Right to erasure

12.24 There is a strong, general public interest in the preservation of news archives and protecting the integrity of records, which contributes significantly to people's access to information about the past and contemporary history. This is a strong factor in favour of not erasing personal information from news archives if someone asks you to.

Refusing requests

12.25 An exemption may exempt you in whole or only in part. You **should** avoid taking a blanket approach.

12.26 If you are deciding whether to refuse a request because it is manifestly unfounded or manifestly excessive, you **should** consider objectively whether the request would clearly have a disproportionate or unjustifiable impact.

13. Apply the journalism exemption

What does the legislation say?

13.1 You **must** generally comply with the requirements of data protection law when you use personal information for journalism. In a lot of cases this is straightforward.

13.2 You can, however, apply the journalism exemption when you meet certain criteria. When you apply it, you no longer have to comply with specific requirements of data protection law.

13.3 You can apply the exemption to most requirements as specified in the highlighted boxes at the start of each section of this code (see 13.3 in Reference notes).

13.4 To apply the exemption, you **must**:

- use personal information for a journalistic purpose;
- act with a view to the publication of journalistic material;
- reasonably believe publication would be in the public interest; and
- reasonably believe that complying with a part of data protection law would be incompatible with your journalistic purpose.

13.5 You **must** form, and be able to demonstrate, a reasonable belief that publication would be in the public interest and that complying with part of data protection law would be incompatible with your journalistic purpose.

13.6 You **must** have regard to specific industry codes or guidelines that are relevant to you as specified in the DPA 2018.

13.7 You **must** consider the general special public interest in freedom of expression and information.

How do we comply?

13.8 In a lot of cases, it is straight forward to comply with data protection law when you use personal information for journalism. However, you can apply the journalism exemption if you reasonably believe that complying would be incompatible with your journalistic purpose and the other criteria for using the exemption are met.

Using personal information for a journalistic purpose

13.9 Data protection law does not define journalism, so you **should** interpret it broadly in line with its everyday meaning and purpose, using relevant case law as a guide as appropriate (see 13.9 in Reference notes).

13.10 Journalism is one of the "special purposes" in data protection law covered by the exemption. This includes artistic, literary, and academic purposes. The special purposes as a whole are likely to cover everything published in a newspaper or magazine, or broadcast on radio or television, including their online content (except paid-for advertising).

13.11 However, journalism is not limited to professional journalists and media organisations. For example, members of the public may carry out journalism, typically online. This is sometimes known as "citizen journalism".

13.12 The exemption can also apply when you use personal information for journalism, as well as another purpose. For example, a campaign group can use personal information for both journalism and campaigning.

Acting with a view to the publication of journalistic material

13.13 Where you use personal information for journalism with a view to the publication of journalistic material, the exemption can cover all the personal information you collect, use, or create as part of your journalistic activity, both before and after publication and regardless of whether you actually publish it.

13.14 You publish material when you make it available to the public, even if it is not accessible to everyone (eg there is a subscription or a paywall).

Reasonable belief

13.15 Your reasonable belief for the purposes of the journalism exemption concerns whether:

- you reasonably believe there is a public interest in publication; and
- complying with part of data protection law is incompatible with your journalistic purpose.

13.16 Having a reasonable belief involves forming your own view on the points in 13.15 above. You **should**, however, be able to justify your view so that another reasonable person would consider that it is objectively reasonable. Forming a reasonable belief can include editorial discretion, which is an essential part of the journalistic exercise (see example 19 and example 20 in Reference notes).

13.17 When considering how you would demonstrate that you made a reasonable decision, you **should** decide what is appropriate depending on the circumstances, especially the level of risk (see 13.17 in Reference notes).

The public interest

13.18 To judge what is in the public interest, you **should**:

- consider the circumstances;
- balance relevant factors for and against publication; and
- judge how the public interest is best served proportionately (see also Use personal information lawfully and Use personal information fairly).

General public interest factors

13.19 The general public interest can take many forms. In the context of journalism, there is most obviously a public interest in the freedom to hold opinions and to receive and impart information. The right to freedom of expression and information is an essential foundation for democratic society protected by the HRA.

13.20 The right to freedom of expression and information concerns the right to exchange information, debate ideas and express opinion. A free press is clearly vital to this. Generally, a free press informs, entertains, and increases public debate and participation. It also acts as a public watchdog to hold the powerful to account and uncover wrongdoing.

13.21 There are many different journalistic fields, whether local or national, that can perform this role across a broad spectrum of news, from political, business, or investigative news to journalism focusing on lifestyle, arts, sports, and entertainment, such as showbusiness news and celebrity coverage.

13.22 There are also other rights that are fundamental to democracy. The courts balance these rights with the right to freedom of expression and information where relevant. The right to privacy is also protected by the HRA. A degree of privacy, and limits on intrusion is needed to protect people's private and family life, their home and correspondence.

13.23 There is also a strong general public interest in data protection that enables people to understand and exercise proportionate control over their personal information. Sometimes personal information may be private, in which case it also involves the right to privacy.

13.24 Generally, there may be a stronger public interest in publishing information if someone is a public figure or has a role in public life, or is a professional or business person (see also Use personal information fairly).

Specific public interest factors

13.25 Although there is a strong general public interest in freedom of expression, when you are deciding what is 'in the public interest' you **should** consider the specific

circumstances and balance different factors proportionately. Certain factors can generally add to the weight given to the public interest balance. For example:

- how likely and severe any harm to the person concerned could be;
- how likely the information is to enhance public debate and understanding; and
- the extent to which information is already in the public domain.

Incompatible with a journalistic purpose

13.26 To decide whether you reasonably believe that complying with part of data protection law would be incompatible with your journalistic purpose, you **should** consider:

- the specific part of data protection law in question; and
- your specific journalistic purpose.

13.27 In some cases, it will be obvious that this part of the exemption applies because it is not possible to both comply and achieve your journalistic purpose. For example, it is not possible to both comply with the principle to use personal information transparently and carry out covert surveillance at the same time. This would therefore be incompatible, and you would need to use the journalism exemption.

13.28 Alternatively, you may also reasonably believe that complying with part of data protection would harm your journalistic purpose to such an extent that it would become incompatible with it.

13.29 In general, the more serious the harm to your journalistic purpose, the more likely it is that you have formed a reasonable belief that compliance would be incompatible (see Reasonable belief above).

14. Complaints, enforcement, and investigations

14.1 People have the right to complain to you, us, and the courts about how you have used their personal information.

14.2 We publish statutory guidance for the public to help them complain about the media and decide the most appropriate organisation to make their complaint to.

14.3 Our role is about data protection, not general press standards. However, where there is overlap, we will work with other authorities to resolve issues effectively and efficiently.

14.4 People can also enforce their data protection rights or claim compensation for damages in court, or both. When the case concerns journalism, the person who is a party, or a prospective party, to the proceedings can ask us to assist if the case is of substantial public importance.

14.5 Courts must stay (or in Scotland, sist) some legal proceedings if certain criteria are met, which protects publication.

14.6 We can take formal enforcement action. However, there are specific and strong protections for journalism and various restrictions and safeguards built into the law.

14.7 Any action we take is targeted and proportionate, with our strongest measures reserved for the most serious incidents. We also carefully consider the potential impact on freedom of expression and information, and a free media, in any action we may take.

14.8 We can also investigate and prosecute criminal offences when we consider it is in the public interest. There are some defences relating to the public interest and journalism set out in the DPA 2018 that can apply in specific circumstances (see Key legal provisions in Reference notes).