

Draft journalism code of practice



Contents

Information Commissioner’s foreword.....	3
Summary	4
Navigating this code	12
About this code.....	15
1. Balance journalism and privacy.....	22
2. Be able to demonstrate compliance	36
3. Keep personal data secure.....	40
4. Justify your use of personal data.....	43
5. Take reasonable steps to ensure personal data is accurate	59
6. Process personal data for specific purposes	64
7. Use the right amount of personal data	67
8. Decide how long to keep personal data	70
9. Be clear about roles and responsibilities.....	74
10. Help people to exercise their rights.....	78
Disputes and enforcement	85
Annex 1 – UK GDPR provisions covered by the special purposes exemption.....	93

Information Commissioner's foreword

We will include a foreword by the Information Commissioner in the final version of the code.

Summary

About this code

- This is a statutory code of practice under the Data Protection Act 2018 (DPA 2018) to support organisations and individuals processing personal data for the purposes of journalism.
- It will help you to comply with your legal obligations under the DPA 2018 and the UK General Data Protection Regulation (UK GDPR) and follow good practice.
- This code is primarily aimed at media organisations and journalists whose purpose is to publish journalistic material and who are controllers. Controllers decide the purpose and means of personal data processing.
- For media organisations, the people most likely to benefit from using this code will be staff who have defined roles and responsibilities, such as lawyers, data protection officers and senior editorial staff.
- We have produced complementary resources to support journalists in their day-to-day work, and they may find this code helpful if further detail is required.
- This code is limited to data protection law. It does not concern press conduct or standards in general, which are covered by industry codes.
- This code informs our review of journalism processing in accordance with the statutory requirement under the DPA 2018.

1. Balance journalism and privacy

- Journalism plays a vital role in the free flow of communications in a democracy. It increases knowledge, informs debates and helps citizens to participate more fully in society. It also helps to hold the powerful to account.
- Journalism should be balanced with other rights that are also fundamentally important to democracy, such as data protection and the right to privacy.

- Data protection law specifically protects journalism and the special public interest in freedom of expression and information, reflecting its importance to society.
- In particular, the broad special purposes exemption under the DPA 2018 can dis-apply many of the usual requirements of data protection law.
- The special purposes are journalism, academic, artistic or literary purposes. This code is about journalism, however parts of this code will help you to consider the other special purposes.
- In relation to journalism, the exemption applies if you:
 - are processing personal data for journalism;
 - are acting with a view to publication;
 - reasonably believe publication is in the public interest; and
 - reasonably believe that compliance with a data protection provision would be incompatible with journalism.
- You can rely on the special purposes exemption even if you are processing personal data for another purpose, as well as journalism, such as campaigning.
- This code explains which data protection requirements are covered by the exemption.

2. Be able to demonstrate your compliance

- Accountability is a key principle of data protection law. Being able to show that you have appropriate data protection measures in place puts you in a much stronger position if challenged. It also helps to build and sustain public trust in journalism.
- Journalism often involves working at pace, under pressure and delegating significant responsibilities. Policies and procedures can support this type of work. For example, a good policy can clarify responsibilities around how decisions are made.
- You can comply with the accountability principle by acting proportionately and considering the risks of what you are doing with personal data.

- Many media organisations, in line with industry codes, will already have suitable broader policies and procedures in place that can be easily adapted to include data protection considerations.
- You do not need to carry out a data protection impact assessment (DPIA) for every story that is likely to involve high risk processing. A single DPIA that applies to the overall type of processing (eg investigative journalism) is very likely to be sufficient. A DPIA sets out how you manage the risks of the different types of processing you carry out.
- Reviewing the effectiveness of the data protection measures you have in place will help you to demonstrate you are complying with the law.
- You always need to comply with the accountability principle. It will stand you in good stead to comply with all aspects of data protection legislation.

3. Keep personal data secure

- Security is a key principle of data protection law. It involves protecting personal data against unauthorised or unlawful processing and accidental loss, destruction or damage.
- You can protect personal data by putting in place appropriate, risk-based organisational and technical security measures. This involves cybersecurity as well as how your staff handle paper records, for example.
- Your security arrangements should take into account the heightened security risks that may arise as a result of the work that journalists do. For example, risks concerning remote working, the use of portable devices, such as laptops and smart phones, and portable media, such as USB memory sticks.
- Asking processors acting on your behalf to show that they can keep personal data secure also helps you to protect people's personal data.
- You always need to comply with the security principle. As with the accountability principle, it provides strong foundations to help you to comply with other aspects of data protection law.

4. Justify your use of personal data

- Processing personal data lawfully, fairly and transparently is a key principle of data protection law. It helps you to make sure that individuals are treated according to commonly accepted general standards, in a way that is free from dishonesty and injustice.
- This principle helps you to balance different interests, which is often a key part of a journalist's role.
- You can process personal data lawfully using one of the lawful bases provided by the UK GDPR. You can process special category or criminal offence data if you can also satisfy one of the conditions concerning this type of personal data.
- One of the conditions concerns the disclosure of information for the purposes of journalism in connection with unlawful acts and dishonesty. This condition allows controllers to disclose these types of sensitive personal data to journalists in some circumstances.
- You can process personal data fairly by considering what a person would reasonably expect in the circumstances and whether the processing would cause any unwarranted harm.
- You can comply with people's right to be informed by providing privacy information when you collect their personal data.
- If you have collected personal data about an individual from someone else, you do not have to provide privacy information if doing so would be impossible or would seriously impair your work.
- The special purposes exemption provides additional protection for journalism where necessary.

5. Take reasonable steps to make sure personal data is accurate

- Accuracy is a key data protection principle. Taking reasonable steps to make sure that personal data is accurate is fundamental to both journalism and data protection.
- Complying with this principle complements journalism by helping to maintain public trust. It will also help you to protect the public from harm caused by inaccuracies, which can be magnified and spread quickly online.

- You can comply with the accuracy principle by taking reasonable steps to correct or erase personal data where necessary.
- Clearly distinguishing between fact and opinion, and taking the context into account, will help you to make sure personal data is accurate.
- You should be able to comply with the accuracy principle in the majority of cases because it complements the public interest served by journalism. Where necessary, the special purposes exemption specifically protects journalism.

6. Process personal data for specific purposes

- Processing personal data for specific purposes that are “compatible” with your initial purpose is a key data protection principle.
- Being clear about why you are using personal data helps individuals to be informed and exercise their rights. It also helps you to avoid function creep. This is when personal data is used for new purposes that are not acknowledged.
- You can comply with the purpose limitation principle by specifying your reasons for processing in your privacy information.
- Regular review will help you to check whether your purposes change over time and to keep your records up-to-date.
- Where necessary, the special purposes exemption specifically protects journalism.

7. Use the right amount of personal data

- You are required to make sure that you have sufficient personal data to do what you need to do, that it is relevant, and not excessive. This is known as the data minimisation principle.
- Limiting the amount of personal data that you hold helps to manage risks. It will also make it easier to limit requests about personal data and deal with them more efficiently.
- You can comply with the data minimisation principle by reviewing the personal data that you have from time to time and deleting anything you no longer need.

- Where necessary, the special purposes exemption specifically protects journalism.

8. Decide how long to keep personal data

- You are required to keep personal data for no longer than is necessary. This principle helps you to reduce risks and comply with other aspects of data protection law.
- A retention policy or schedule will help you to justify how long to keep personal data, where this is possible
- Where necessary, the special purposes exemption specifically protects journalism.

9. Be clear about third party roles and responsibilities

- When a third party is involved in processing personal data, consider whether they are a controller or a processor. Controllers determine the means and purposes for processing personal data, whereas processors act only on instructions.
- Understanding the respective roles of yourself and third parties will help you to be clear about responsibilities.
- You are required to have a written contract with processors and to make sure that they can comply with data protection law.
- If you are acting as a joint controller with a third party ie you both determine the means and purposes of the processing, the law requires you to have a transparent arrangement in place setting out your respective responsibilities.
- When sharing personal data with another controller, a data sharing agreement will help you to be clear about arrangements and responsibilities. Considering whether a DPIA is needed will help you to manage any associated risks.
- Carrying out appropriate checks when third parties share personal data with you that you want to use for journalism will help you to be confident that you are complying with data protection law. Relevant checks include

confirming the source, how and when the data was collected, and checking that it is accurate.

10. Help people to exercise their data protection rights

- Individuals have general data protection rights which they can exercise on request. These include an individual's right to access their own personal data and to ask for it to be erased if certain conditions are met. You are required to help people to exercise these rights.
- However, you may refuse to comply with individual requests in certain circumstances.
- There is a very strong, general public interest in protecting the identity of journalists' confidential sources. It is very unlikely you would be required to disclose information identifying a confidential source in response to an individual's request for their own personal data.
- You can keep records of mistakes. To make sure that your records are clear, you may need to add a note or a correction.
- The right to erasure does not apply if your processing is necessary to exercise the right to freedom of expression and information.
- There is a strong, general public interest in the preservation of news archives, which contribute significantly to the public's access to information about past events and contemporary history. This is generally a weighty factor in favour of not erasing personal data from news archives.
- Where necessary, the special purposes exemption specifically protects journalism. This applies to all individuals' rights except for rights relating to automated processing.









Disputes and enforcement

- If someone has concerns about your handling of personal data, it helps to save the time and resources of all parties if you are able to resolve the matter directly with the individual in the first instance.
- If a complaint is made to the ICO, we will consider whether it is likely that there has been a breach of data protection and we may ask you to take steps to put things right.

- We exercise our enforcement powers, where necessary, in a proportionate way. The DPA 2018 significantly restricts how we can use our powers for the special purposes, offering additional protection for journalism.
- There are a number of criminal offences under the DPA 2018. However, there are public interest defences available for some of these. This includes a specific defence to protect journalism, where the person acted with a view to the publication of journalistic material and in the reasonable belief that publication would be in the public interest.
- The ICO may offer assistance to claimants in cases of substantial public importance.
- In certain circumstances you can apply for a stay to legal proceedings. This prevents data protection being used to block publication.

Navigating this code

A quick reference guide to help you find the content you need on each topic.

What you need to do or consider		Where you can find it in the journalism code
Consider whether the personal data you are processing is for journalism.		Who is this code for? What is journalism?
Decide whether you need to comply with a data protection legal requirement to process personal data for journalism.		What is the special purposes exemption? Annex 1 – UK GDPR provisions covered by the special purposes exemption.
Satisfy the legal requirements to apply the special purposes exemption for journalism.		What does “with a view to the publication of journalistic material” mean? What does “reasonable belief” mean? What does “incompatible with journalism” mean?
Explain your decision to use the special purposes exemption for journalism.		Demonstrating your decision to use the special purposes exemption.
Put in place appropriate data protection measures.		Be able to demonstrate compliance. Keep personal data secure.
Manage the risks of processing personal data for stories that are likely to result in high risk to individuals.		Data protection impact assessments.
Pick an appropriate lawful basis for processing personal data for your story.		How do we process personal data lawfully?

Process special category data lawfully eg personal data about an individual's health or sex life.



[How do we process special category data lawfully?](#)

Process criminal offence data lawfully eg personal data about criminal activity or allegations.



[How do we process criminal offence data lawfully?](#)

Consider how people may provide personal data to journalists lawfully.



[Be clear about roles and responsibilities.](#)
[Journalism in connection with unlawful acts and dishonesty.](#)
[What criminal offences are there and what are the most relevant defences?](#)

Decide whether it is fair to publish your story in the circumstances eg when an individual has a public profile or an activity is taking place in public.



[How do we process personal data fairly?](#)
[What does "in the public interest" mean?](#)

Consider using covert surveillance, subterfuge or similar intrusive methods.



[Covert surveillance, subterfuge and similar intrusive methods.](#)

Decide whether you need to provide any privacy information to an individual about your story.



[What does transparent processing of personal data mean?](#)

Decide what checks are reasonable to make sure personal data for a story is accurate, including in urgent circumstances.



[Reasonable accuracy checks.](#)
[Sources of information.](#)
[Social media.](#)
[Receiving personal data from third parties.](#)

Use personal data that may be different from your original purpose.



[Purposes that are compatible with journalism.](#)
[Purposes that are not](#)

[compatible with journalism.](#)

Consider what is the right amount of personal data to process.



[How do we minimise personal data?](#)

Decide whether I can keep personal data for stories eg research and background materials.



[Research and background materials.](#)

Work with a third party to process personal data.



[Be clear about roles and responsibilities.](#)

Handle a request by an individual to exercise their data protection rights.



[Help people to exercise their rights.](#)

Protect a confidential source when someone has made a request to access personal data.



[Right of access.](#)

Consider a request for erasure concerning personal data in news archives.



[Right to erasure.](#)

Correct or complete inaccurate personal data.



[Right to rectification \(correcting or completing data\).](#)

About this code

At a glance

- This is a statutory code of practice under the DPA 2018 to support organisations and individuals processing personal data for the purposes of journalism.
- It will help you to comply with your legal obligations under the DPA 2018 and the UK GDPR and follow good practice.
- This code is primarily aimed at media organisations and journalists whose purpose is to publish journalistic material and who are controllers. Controllers decide the purpose and means of personal data processing.
- For media organisations, the people most likely to benefit from using this code will be staff with defined roles and responsibilities, such as lawyers, data protection officers and senior editorial staff.
- We have produced complementary resources to support journalists in their day-to-day work, and they may find this code helpful if further detail is required.
- This code is limited to data protection law. It does not concern press conduct or standards in general, which are covered by industry codes.
- This code informs our review of journalism processing in accordance with the statutory requirement under the DPA 2018.

In more detail

- [Who is this code for?](#)
- [How will this code help us?](#)
- [How does this code reflect the special public interest in freedom of expression and information?](#)
- [How does this code relate to other laws affecting the media?](#)
- [How will the ICO, a court or a tribunal take this code into account?](#)
- [How will the ICO review this code?](#)

Who is this code for?

This code contains guidance for those processing personal data for journalism (see [What is journalism?](#)) who are required to comply with the UK GDPR and the DPA 2018. In this code, we may refer to this legislation as data protection law.

Following the UK's exit from the European Union (EU), the EU GDPR was incorporated into UK law, with amendments so that it works in a UK-only context. The GDPR as amended is referred to in this code as the UK GDPR. It sits alongside the DPA 2018, which has also been amended following the UK's exit from the EU.

This code is primarily aimed at media organisations and journalists whose purpose is to publish journalistic material. It is addressed to "controllers" as defined by the UK GDPR. When we refer to "you" throughout the code, we are addressing the controller who has the main legal responsibility for complying with data protection law.

Controllers decide the purpose and means of personal data processing. The controller of personal data may be an organisation, or the controller may be an individual such as a freelance journalist or photographer (see [Be clear about roles and responsibilities](#)).

For media organisations, people most likely to benefit from using this code will be staff with defined roles and responsibilities, such as lawyers, data protection officers and senior editorial staff. We have produced complementary resources to support journalists in their day-to-day work, and they may also find this code helpful if further detail is required.

The code applies when you are processing personal data for the purposes of journalism. This is often clear. For example:

- newspapers, news agencies, and magazines, and their online content;
- television and radio broadcasters, such as the BBC, including broadcast content made available online, such as the BBC iPlayer; and
- other approaches to providing news, such as blogs, citizen journalism and other web-based news. Citizen journalism is journalism that is produced by non-professional journalists, typically online.

In other types of online service, you may need to consider more carefully whether the code applies. You may find it helpful to consider:

- whether the material is journalistic;
- and the purpose(s) for which the service processes the personal data. A service may process personal data for journalism, as well as other purposes. Where this is the case, the code can still apply to the service regarding the journalistic material.

Some online services include journalistic material that is produced by someone else. Such services may exert a degree of editorial control over the material's content, presentation, and the decision to publish it that goes beyond moderation. The more editorial control exerted, the more likely it is

that the service is processing personal data for the purposes of journalism. This is different to third party user-generated content, which is any form of content posted by individuals using online platforms, where there is usually no or little editorial control other than moderation.

Further reading

For more information about the scope of data protection law and the meaning of “controller” and “processor”, please see [Guide to the UK GDPR: Key definitions](#).

Please read our guidance [Data Protection after the end of the end of the transition period](#) if you require further information about the impact of the UK leaving the EU.

How will this code help us?

This code provides practical guidance on how to comply with data protection law when you are using personal data for journalism. It will help you to understand your legal obligations by explaining what the law says and the importance of specific data protection requirements. The code will also help you to comply effectively.

The code recognises the unique nature of journalism and how data protection compliance works most effectively when linked to journalistic practice. It also recognises that processing personal data is a key component of journalism and the importance of journalism to the wider public interest. Even though there are important exemptions for journalism, complying with data protection law is essential to public trust and confidence in journalism.

The DPA 2018 says that the ICO must prepare a code of practice containing practical guidance about processing personal data for journalism in accordance with data protection law and “such other guidance as the Commissioner considers appropriate to promote good practice in the processing of personal data for the purposes of journalism”. Good practice is defined as practice that “appears to the Commissioner to be desirable”. This must take into account:

- the interests of data subjects and others, including compliance with the requirements of the data protection legislation; and
- the special importance of the public interest in freedom of expression and information.

Following this code will make it easier for you to demonstrate that you are complying with data protection law. Each section of this code will help you to balance journalism and privacy by explaining:

- what the law says, focusing on the [seven key data protection principles](#);
- the importance of specific data protection provisions; and
- how to comply effectively.

We have focused on key points and practical information relevant to journalism, where possible, rather than covering all aspects of the legislation. We also assume knowledge of some general data protection terms and concepts. For example, what is meant by “personal data” or “processing”. Where relevant, the code may link to further reading, but if you need more detail, please read the [Guide to the UK GDPR](#).

This code does not concern press conduct or standards in general. It is limited to the requirements of data protection law and good practice within the context of journalism. Press standards more generally are covered by other industry codes including:

- [Independent Press Standards Organisation \(IPSO\) Editors’ Code of Practice](#);
- [IMPRESS Standards Code](#);
- [BBC Editorial Guidelines](#); and
- [Ofcom Broadcasting Code](#).

However, this code is generally well-aligned with the above codes and complements industry guidance. Where relevant, we will take industry codes of practice into account. Complying with industry codes will therefore also help you to comply with data protection law.

How does this code reflect the special public interest in freedom of expression and information?

Under the DPA 2018, we must take into account “the special importance of the right to freedom of expression and information” when drawing up this code.

Data protection law specifically protects the importance of the public interest in freedom of expression and information. The main provision is a broad exemption that dis-applies many of the usual requirements of data protection law. We refer to this as the special purposes exemption. Other relevant provisions concerning freedom of expression and information are addressed in this code.

Freedom of expression and information, and the right to privacy, are both rights enshrined in UK law via the Human Rights Act 1998. In principle, neither is more important than the other. The ICO and the courts must give effect to both these rights as far as possible. The relevant provisions of data protection law are designed to reconcile these competing rights where necessary. This code will help you to balance these rights in the context of data protection law.

How does this code relate to other laws affecting the media?

Compliance with this code should help you to comply with other aspects of the law affecting the media.

The UK GDPR and the DPA 2018 operate in the context of other laws affecting the media. Sometimes data protection law and other legal provisions are raised at the same time in legal claims. Although each legal provision merits separate consideration, there are some similarities. For example:

- Considering whether processing is “fair” under the fairness data protection principle is similar to considering whether a “reasonable expectation of privacy” exists under the tort of misuse of private information. However, it is important to note that not all personal data is necessarily private.
- The courts sometimes draw on concepts from defamation law to help them to assess whether personal data is inaccurate (See [Aven and Others v Orbis Business Intelligence Limited \[2020\] EWHC 1812 \(QB\)](#)). Defamation law also includes a defence if there is a “reasonable belief” publication is in the public interest. This is similar to the special purposes exemption under the DPA 2018.

How will the ICO, a court or a tribunal take this code into account?

This is a statutory code of practice under the DPA 2018 and following it will make it easier for you to demonstrate that you have complied with data protection law.

The ICO must take relevant provisions of this code into account when determining a question relating to its functions under data protection legislation or the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426). The question must relate to a time when the relevant provision was in force.

A court or tribunal must take into account any provision of this code that appears relevant when determining a question arising in legal proceedings. The question must relate to a time when the relevant provision was in force. The code may also be admitted as evidence in legal proceedings.

Generally, the courts give weight to statutory codes of practice, taking the approach that this guidance must be considered carefully and followed unless there is a good reason not to do so.

What is the status of 'further reading' or other linked resources?

We provide links to further reading and other resources within this code. Although these are not part of the code, you may find them helpful. Where we link to other ICO guidance, that guidance will inevitably reflect our views and inform our general approach to interpretation, compliance and enforcement.

How will the ICO review this code?

Under the DPA 2018, the ICO is required to review the processing of personal data periodically for the purposes of journalism and report to the Secretary of State.

The first review period began on 25 May 2018 and ends after four years. The ICO must begin a review within six months from the end of the first review period and must submit a report to the Secretary of State within 18 months from when the review was started. Subsequent review periods are five years long.

The code will in due course act as an important tool to enable the ICO to assess data protection compliance when personal data is processed for journalism. We will engage with stakeholders, including industry bodies, as we develop the review process.

We will review this code as part of the statutory review periods to evaluate how it is working in practice. We will also keep the code under general review and update it where necessary in line with changes to the law, court or regulatory decisions, our guidance or other industry codes or developments.

Key legal provisions

[DPA 2018 section 124](#) - duty to prepare a journalism code of practice

[DPA 2018 section 127](#) - legal effect of the code

[DPA 2018 section 178](#) - review of processing of personal data for the purposes of journalism

1. Balance journalism and privacy

At a glance

- Journalism plays a vital role in the free flow of communications in a democracy. It increases knowledge, informs debate and helps citizens to participate more fully in society. It also helps to hold the powerful to account.
- Journalism should be balanced with other rights that are also fundamentally important to democracy, such as data protection and the right to privacy.
- Data protection law specifically protects journalism and the special public interest in freedom of expression and information, reflecting its importance to society.
- In particular, the broad special purposes exemption under the DPA 2018 can dis-apply many of the usual requirements of data protection law.
- The special purposes are journalism, academic, artistic or literary purposes. This code is about journalism, however parts of this code will help you to consider the other special purposes.
- In relation to journalism, the exemption applies if you:
 - are processing personal data for journalism;
 - are acting with a view to publication;
 - reasonably believe publication is in the public interest; and
 - reasonably believe that compliance with a data protection provision would be incompatible with journalism.
- You can rely on the special purposes exemption even if you are processing personal data for another purpose, as well as journalism, such as campaigning.
- This code explains which data protection requirements are covered by the exemption.

In more detail

- [What is journalism?](#)
- [Why is it important to balance journalism and privacy?](#)
- [What is the special purposes exemption?](#)
- [What do we need to do to rely on the special purposes exemption?](#)

What is journalism?

Although data protection law does not define journalism, it's helpful to consider its everyday meaning, the underlying purpose of protecting freedom of expression and information, and relevant case law. In line with key case law, you may interpret 'journalism' to mean "the disclosure to the public of information, opinions or ideas by any means" (see [Satamedia case C-73/07](#)).

Taken together with art and literature, it is likely that the special purposes as a whole cover everything published in a newspaper or magazine, or broadcast on radio or television. In other words, the entire content of the print and broadcast media, with the exception of paid-for advertising. This is in line with the Supreme Court's decision in [Sugar \(Deceased\) v BBC \[2012\] UKSC4](#), which found that "journalism, art or literature" covers the whole of the BBC's output to inform, educate or entertain the public.

However, journalism is not limited to professional journalists and organisations. It may also involve other individuals and members of the public publishing information. This can cover citizen journalism, for example, when individuals publish journalistic material, typically online. Factors that may help to determine whether an individual is engaging in journalism include:

- the purpose of the publication, including any reasons provided by the individual for publishing the information. For example, informing the public;
- how closely the activity resembles activities that the media carry out;
- the content of the information, including any public interest in publication;
- the means by which the information was published;
- the extent to which the information has been promoted to the public, and any restrictions on its use.

Journalism is not so broad that it has the same meaning as communication or every activity that concerns conveying information or opinions (see [NT1 & NT2 v Google LLC and ICO \[2018\] EWHC 799 \(QB\)](#) para. 98). For example, in this case the judge said that the operation of Google's search engine was for purposes other than journalism.

As a rule of thumb, the more closely an individual's activity resembles activities traditionally carried out by the print and broadcast media or other clear sources of journalism, the more likely it is to be journalism. For example, if a private individual films an event of public interest, such as a demonstration or the aftermath of a natural disaster, and places the footage online, they may be engaging in journalism.

Of course, many people put material on the internet for reasons other than journalism. People frequently use the internet to express their views, converse or exchange information without necessarily engaging in journalism. This includes debate on substantive public interest issues. For example, a private individual who expresses their views on Twitter for or against a particular matter.

Personal data processed in the course of a purely personal or household activity, with no connection to a professional or commercial activity, falls outside the UK GDPR's scope. This may apply to material on the internet depending on its purpose, content, and the restrictions on its publication.

Case example

[Buivids case \(C-345/17\)](#)

Mr Buivids published a video he had taken in a police station on You Tube. He said that he wanted to draw attention to what he considered was unlawful conduct.

The European Court of Justice (ECJ) said that:

- Mr Buivids could not argue that the personal data was purely for personal or household activities because he had published the video on the internet without any restrictions;
- Mr Buivids could still be engaged in journalism, even though he is not a professional;
- although the interpretation of journalism was broad, it did not extend to all information published on the internet; and
- in determining whether Mr Buivids is processing personal data for journalism, Mr Buivids' reasons for publication could be taken into account. However, it is not necessary to prove that there had been any unlawful conduct.

Non-media organisations may process personal data for journalism as well as other purposes, such as campaigning (see *Steinmetz v Global Witness* [2014] EWHC 1186 (Ch)). As with private individuals, it is helpful to consider this on a case-by-case basis, taking into account similar factors to those set out above.

Further reading

[Guide to the UK GDPR: Exemptions](#)

Why is it important to balance journalism and privacy?

It is widely accepted that a free press, especially a diverse press, is a fundamental component of a democracy. It is associated with strong and important public benefits worthy of special protection. This in itself is a public interest.

Most obviously, a free press plays a vital role in the free flow of communications in a democracy. It increases knowledge, informs debates and helps citizens to participate more fully in society. All forms of journalistic content can perform this crucial role, from day-to-day stories about local events to celebrity gossip to major public interest investigations.

A free press is also regarded as a public watch-dog. It acts as an important check on political and other forms of power, and in particular abuses of power. In this way, it helps citizens to hold the powerful to account.

However, the right to freedom of expression and information should be balanced with other rights that are necessary in a democratic society, such as the right to privacy. The public interest in individual freedom of expression is itself an aspect of a broader public interest in the autonomy, integrity and dignity of individuals.

The influence and power of the press in society, and the reach of the internet, means that it is particularly important to balance journalism and people's right to privacy.

This code provides guidance about balancing these two important rights by helping you to understand what data protection law requires and how to comply with these requirements effectively.

What is the special purposes exemption?

The special purposes exemption under the DPA 2018 is specially designed to protect freedom of expression and information in journalism, academic activities, art and literature. It is a broad exemption, reflecting the importance of freedom of expression in society.

This code is about processing personal data for journalism. The other special purposes are outside the code's scope, but parts of this code will help you when considering the other special purposes.

When the special purposes exemption applies, you do not have to comply with certain provisions of the UK GDPR, including:

- the key data protection principles, apart from the security and accountability principles;
- the requirement to provide privacy information to individuals; and
- individual rights, apart from the rights regarding automated processing.

For a full list of the provisions of the UK GDPR that the exemption dis-applies, see Annex 1 of this code.

Although the special purposes exemption is broad, there are some fundamental provisions of data protection law which you always need to comply with as follows:

- Accountability, including the requirement to carry out a DPIA for certain types of processing (see [Be able to demonstrate your compliance](#)).
- Security (see [Keeping personal data secure](#)).
- The right to opt-out of direct marketing.
- Individuals rights regarding automated processing.
- Individuals' right to compensation for material or non-material damage.
- Criminal offences under the DPA 2018 (See [Disputes and enforcement](#)).
- [Registration](#) with the ICO.

What do we need to do to rely on the special purposes exemption?

You can rely on the special purposes exemption if you process personal data for the purposes of journalism. It applies if:

- the processing is carried out with a view to the publication by a person of journalistic, academic, artistic or literary material;
- you reasonably believe the publication of the material is in the public interest; and
- you reasonably believe that compliance with a relevant data protection provision is incompatible with journalism.

You can rely on the special purposes exemption even if you are processing personal data for purposes other than journalism, such as campaigning. This is a change from the DPA 1998 when the special purposes exemption applied only when you were processing personal data for journalism.

To rely on the exemption, you have to demonstrate a reasonable belief that publication is in the public interest, rather than proving that it definitely is in

the public interest. This distinction is less restrictive than other exemptions under the DPA 2018, reflecting the importance of protecting the special public interest in freedom of expression and information. It is designed to respect the independent judgement and expertise of the controller regarding the public interest. In other words, your judgement on the public interest is not to be disregarded lightly.

You can rely on the exemption by satisfying its requirements as explained below. Being able to demonstrate that this is the case will put you in a stronger position.

What does “with a view to the publication of journalistic material” mean?

“With a view to publication” means that you are processing personal data with the intention or hope of publishing journalistic material. In this context, ‘publish’ means you are making it available to the public.

You do not necessarily need to have a particular publication in mind. For example, if you collect personal data to publish a story, you can retain it to use it in a different story in the future or update a story that you have already published.

You can rely on the exemption to cover all the background information you collect, use or create as part of your journalistic day-to-day activities, even if you:

- do not include those details in any final article or programme; and
- do not actually publish a story, as long as there remains “a view to publication” in the future.

As long as the information you originally collected and used was for the ultimate aim of publication, the exemption protects you both before and after publication (See [Campbell v MGN Limited \[2002\] EWCA Civ 1373](#)). This is because the relevant processing is not each processing operation in isolation, but the end-to-end process involved in publishing journalistic material. For this reason, we accept that the exemption allows you to retain and re-use information, even after publication.

If you subsequently get a complaint about a story, and you are considering the complaint in the context of whether to print a correction or a retraction for example, this is processing “with a view to the publication of journalistic material”. However, if you are processing personal data to address a complaint and there is no possibility of the outcome affecting the publication

of journalistic material, this processing is not done “with a view to the publication of journalistic material”.

What does “reasonable belief” mean?

You can rely on the exemption if there is a reasonable belief that publication is in the public interest. This involves both a subjective and an objective element (see [NT1 & NT2 v Google LLC and ICO \[2018\] EWHC 799 \(QB\)](#) para 102).

Firstly, you simply need to demonstrate that you considered whether publication is in the public interest and formed a view (a subjective belief). Keeping a record can make this easy to do.

You are able to rely on the exemption if the belief you hold is objectively reasonable. This provides necessary latitude for journalism because the belief formed only has to be one that a reasonable person could hold in the circumstances. It does not need to be the only reasonable view or the most reasonable view. The ICO, a court or a tribunal may not agree with your assessment but that does not mean your belief is not reasonable.

In considering whether your belief is reasonable, the Commissioner’s role is not to substitute their own belief about what is reasonable in place of yours. It is only to consider the reasonableness of your belief on an objective basis.

It may be helpful to consider defamation law when considering whether a belief is objectively reasonable. The Defamation Act 2013 includes a defence when there is a reasonable belief publication is in the public interest. For example, it may be relevant to consider:

- attempts made to verify the truth of what is being published;
- the nature of the sources of information; and
- the extent to which the individual was given an opportunity to respond or comment.

It is the belief of the controller that is relevant in this context, rather than an individual journalist. However, you can delegate responsibility for decisions to individual journalists as appropriate. In many day-to-day stories it may be appropriate for individual journalists to use their own judgement. More high-profile, intrusive or damaging stories may require more formal consideration and more editorial involvement.

Where there is significant delegation, and particularly where there is a higher level of risk, clear policies and procedures will help you to minimise the risks (see [Be able to demonstrate your compliance](#)). Policies help to clarify responsibilities and what authority people have to act on your behalf. This

will help you to demonstrate that a reasonable belief was held when decision-making is delegated.

What does “in the public interest” mean?

You can rely on the exemption if you reasonably believe that publication is “in the public interest”. This involves:

- considering the circumstances;
- balancing relevant factors for and against publication; and
- deciding whether the public interest is best served by publication.

Doing this will help you to demonstrate that you formed an objectively reasonable belief about whether publication is in the public interest.

There is a general public interest in freedom of expression and information itself which should be balanced proportionately against other factors. This involves considering the arguments in favour of publishing information and those in favour of not publishing it in the circumstances of the particular case. Try to do this objectively and flexibly, recognising that there are always arguments to be made on both sides and that these will vary from case to case. In the most significant cases, it may be helpful to draw up a list showing the arguments on both sides. This will help you to assess their relative weight and decide what is proportionate.

You are required to consider specific industry codes of practice or guidelines that are relevant. The DPA 2018 specifies that relevant codes for you to take into account are:

- [Independent Press Standards Organisation \(IPSO\) Editors’ Code of Practice](#);
- [BBC Editorial Guidelines](#); and
- [Ofcom Broadcasting Code](#).

Although not listed in the DPA 2018, it is appropriate for members of IMPRESS to take the [IMPRESS Standards Code](#) into account.

Industry codes include guidance about the public interest. If you are able to demonstrate that you have complied with industry codes, this will support your assessment of the public interest when relying on the special purposes exemption.

You may also find it helpful to consider [complaint outcomes by IPSO](#) involving the balance of the public interest.

General public interest arguments

The public interest can cover a wide range of values and principles relating to the public good or what is in the best interests of society. It may take many forms and the following are non-exhaustive possibilities. For example, there is a general public interest in:

- upholding standards of integrity;
- ensuring justice and fair treatment for all;
- promoting transparency and accountability;
- encouraging public understanding and involvement in the democratic process; and
- securing the best use of public resources.

The special purposes exemption in the DPA 2018 protects the balance of the general public interests in freedom of expression and privacy. We have described in this code why both are important and the public interest benefits that derive from these rights ([see Why is it important to balance journalism and privacy?](#)).

There may also be a public interest in the general subject matter of the information. This depends on the circumstances of the case. For example, there may be a public interest in:

- protecting public health and safety;
- preventing people from being misled;
- exposing or detecting crime or anti-social behaviour; or
- exposing corruption, injustice, incompetence, negligence or unethical behaviour.

In general, there may be a stronger public interest for publishing information where an individual:

- is a public figure (individuals who have a degree of media exposure due to their functions or commitments); or
- has a role in public life more broadly, where the public has an interest in having access to some information about them. Politicians, public officials, business people and members of regulated professions are examples of individuals with this type of role.

Specific public interest arguments

As well as considering general public interest factors, you also need to consider the specific circumstances and the relative weight of the arguments both in favour and against publication. This will help you to balance the arguments proportionately.

Certain factors can add weight to the arguments on either side of the public interest balance. These factors include:

- the likelihood and severity of any harm to individuals or other public interests;
- the nature of the information and the contribution it would be likely to make in the public interest; and
- whether information is already in the public domain.

Likelihood and severity of harm

The likelihood of harm to an individual varies. There may only be a remote possibility of harm, it may be likely, or it may be more probable than not. This is not an exact science, but it will help you to consider the weight to apply when balancing the public interest.

The severity of any harm is another key factor in deciding how much weight to apply. If there would be a severe impact on individuals or other public interests, then this will carry significant weight in the public interest. This is relevant if, for example, there is any risk of physical or mental harm to an individual.

The nature of the specific information

Considering the nature of the specific information will help you to decide whether there is a sufficient public interest that would justify its publication. The information may enhance public debate or understanding, which may strengthen the public interest in publication. Alternatively, it may not actually add that much to public understanding.

In the case of public figures or those with a public role, while there may be a general public interest in publication, considering the nature of the information will help you to arrive at a balanced view. You are usually entitled to put the record straight if a public figure or individual with a role in public life chooses to present a false image or make untrue comments about their life. However, there may be a public interest in publishing some of the information, but not necessarily all of it. The key is to act proportionately.

Case example

[Campbell v MGN Ltd \[2004\] UKHL 22](#)

The Mirror newspaper published a story about Naomi Campbell's drug use and therapy.

In this case, there was a public interest in setting the record straight by publishing the fact that Miss Campbell had used drugs because she had repeatedly denied doing so in the media.

However, the Supreme Court found that there was not a sufficient public interest to justify the publication of other information. This included information that Miss Campbell was receiving treatment at Narcotics Anonymous, the details of her treatment, and a photograph of her leaving a meeting.

Whether some information is already in the public domain

The public interest in protecting the right to privacy is not automatically weaker because some information or similar information is already in the public domain. This is always a matter of fact and degree, so carefully comparing the specific information with what is already in the public domain will help you.

There may be a public interest in presenting a full picture to increase public understanding or to remove any suspicion of manipulating the facts or spin. If information is already in the public domain that is misleading or misrepresents the true position, this may increase the public interest in publication of the full picture. There may be a weaker public interest in publication if similar information is already available and the information you wish to publish would not significantly add to it.

What does “incompatible with journalism” mean?

You can rely on the exemption by demonstrating a reasonable belief that complying with a particular provision is incompatible with the purposes of journalism. In other words, it is necessary to not comply with data protection law in order to achieve your journalistic purpose.

Deciding what is proportionate may involve considering whether an alternative method is reasonably practicable. There may be resource implications, for example. Even if you cannot comply fully, you should still comply to whatever extent you believe is proportionate in order to achieve your journalistic purpose.

Case example

[True Vision Productions \(TVP\) v ICO \(EA 2019 0170\)](#)

This case before the First-Tier Tribunal concerned whether the ICO was right to impose a monetary penalty on TVP. Although not a binding precedent, this case shows how the judge considered whether compliance with data protection was incompatible with journalism.

The case was about filming in a maternity ward for the purpose of making a documentary about still births using CCTV. The fact that filming was taking place was not adequately brought to the mothers' attention. The intention was to capture a woman's reaction upon being told the news.

The judge decided that there was a reasonable way that TVP could have collected the data it required in accordance with the principle of fairness. This meant that TVP had not correctly relied on the special purposes exemption because compliance with the data protection principle was not incompatible with journalism.

The judge considered editorial judgement and "whether there was any possibility of different but reasonable views". He said, "...the use of hand held cameras would at least have made every mother aware that they were being filmed and their voices recorded" and "this was a modest, practical and reasonable alternative method...".

Demonstrating your decision

You are responsible for making sure you comply with data protection law and that you can demonstrate your compliance (see [Be able to demonstrate your compliance](#)).

It will be easier to show that you reasonably believed publication was in the public interest and that compliance with a data protection provision was incompatible with journalism if you:

- have clear policies and procedures covering who makes such decisions and how the decisions are made;
- can demonstrate that those policies were followed, as well as any relevant industry codes or guidelines; and
- can provide evidence, depending on the circumstances, of your considerations at the time to support the conclusions you reached.

Most, if not all, journalistic organisations already have suitable broader policies and procedures which can be easily adapted if necessary to include data protection considerations. This is because there are similar requirements in industry codes.

One of the most obvious ways to demonstrate your compliance is to keep a record of decisions you have taken and why. Whilst this may not always be necessary, doing so will help you to demonstrate your compliance more effectively.

We recognise that modern, digital newsrooms, are fast-paced and the speed to publication in a digital environment is also highly competitive. We also recognise that media organisations need to design record keeping processes that can feasibly work within this environment. Simple checklists and templates, in both digital and paper formats, can also assist fast decision-making.

Using risk as a guiding factor can help you to exercise your judgement to keep proportionate records of your decisions. In cases where there is less risk, it may be appropriate to keep a brief record of key points, or details of who made the decision and when. Where there is a greater risk, it is more likely to be appropriate for you to keep a record of your decision to rely on the special purposes exemption and the factors that support it. For example, there are greater risks when processing special category or criminal offence data.

Ideally, keep a record around the time you make your decision to rely on the exemption. Doing this means that it will be easier for you to recall the facts and show that you considered the public interest at the time. We recognise that urgency and public interest may mean that this is not always possible at the time of decision, but you could consider recording your decision at a later stage when it is more appropriate.

The key point is that you are able to account for the action that you took. This will put you in a much better position if you are challenged and need to defend against complaints or litigation.

Case example

[Sicri v Associated Newspapers Ltd \[2020\] EWHC 3541 \(QB\)](#)

Commenting on a lack of evidence to demonstrate editorial decision-making on the public interest in line with the Editor's Code (the requirements of which this ICO code echoes), the judge said:

"...the evidence falls well short of what the Code requires. It does not demonstrate that those responsible held a reasonable belief that identifying the claimant would serve and be proportionate to the public interest, or how such a belief was arrived at...There is no documentary evidence to support

such a conclusion...There is no reliable evidence, either, that there was even a conversation on the matter”.

The judge said that he accepted that such decisions do not need to be made formally or recorded but if there is no record, and nobody can recall when or how it happened, “...a defendant may find it hard to ‘demonstrate’ any of the things which the Code requires to be demonstrated”.

Key legal provisions

[UK GDPR article 85](#) – Duty to reconcile data protection with the right to freedom of expression, including processing for journalistic purposes

[DPA 2018 schedule 2, part 5, para. 26](#) – special purposes exemption for journalistic, academic, artistic or literary purposes

[DPA 2018 schedule 2, part 5, para. 26\(5\)](#) – requirement for controller to take into account specific industry codes

[DPA 2018 schedule 2 Part 5 paragraph 26\(9\)](#) – provisions of the UK GDPR that can be dis-applied by the special purposes exemption

2. Be able to demonstrate compliance

At a glance

- Accountability is a key principle of data protection law. Being able to show that you have appropriate data protection measures in place puts you in a much stronger position if challenged. It also helps to build and sustain public trust in journalism.
- Journalism often involves working at pace, under pressure and delegating significant responsibilities. Policies and procedures can support this type of work. For example, a good policy can clarify responsibilities around how decisions are made.
- You can comply with the accountability principle by acting proportionately and considering the risks of what you are doing with personal data.
- Many media organisations, in line with industry codes, will already have suitable broader policies and procedures in place that can be easily adapted to include data protection considerations.
- You do not need to carry out a data protection impact assessment (DPIA) for every story that is likely to involve high risk processing. A single DPIA that applies to the overall type of processing (eg investigative journalism) is very likely to be sufficient. A DPIA sets out how you manage the risks of the different types of processing you carry out.
- Reviewing the effectiveness of the data protection measures you have in place will help you to demonstrate you are complying with the law.
- You always need to comply with the accountability principle. It will stand you in good stead to comply with all aspects of data protection legislation.

In more detail

- [What does “being able to demonstrate compliance” mean?](#)
- [Why is it important that we are able to demonstrate compliance?](#)
- [How can we make sure that we are able to demonstrate compliance?](#)

What does “being able to demonstrate compliance” mean?

Accountability is one of the key principles set out in the UK GDPR. It involves putting in place proportionate and risk-based data protection measures to comply with data protection law.

Being accountable enables you to show others what practical measures you have put in place, including the steps you take to keep personal data safe. It is important to review these measures regularly to check that they continue to be appropriate.

You always need to comply with the accountability principle, even though you may rely on the special purposes exemption for other aspects of data protection law.

Further reading

[Guide to the UK GDPR: Accountability and governance](#)

[ICO Accountability Framework](#)

[Guide to Data Protection: Key data protection themes – children](#)

Why is it important that we are able to demonstrate compliance?

All of the data protection principles are legal requirements. There are also strong benefits. Being accountable helps you to minimise the risks of handling personal data, taking into account your circumstances, the nature of the personal data, and what you are doing with it.

In the journalism industry, particularly when under pressure, you may delegate significant responsibility to employees at different levels. Where the 'journalist on the ground' is making the decision at pace, implementing appropriate measures goes a long way towards reducing risks. For example, good policy will help individuals to be clear about their responsibilities.

Good accountability is key to building and sustaining public trust. It enhances your reputation and enables swifter resolution of complaints, investigations, and legal proceedings.

How can we make sure that we are able to demonstrate compliance?

Accountability is a flexible concept. As a general rule of thumb, what you do should be proportionate to the risks you are taking with personal data.

You can demonstrate what you are doing to comply with documentation or records. Accountability is also about what you do in practice, so it will help if

you regularly review how everything is working. A policy or procedure that is actually followed in practice is clearly most effective.

The ICO's [Accountability Framework](#) sets out our key expectations for accountability. It is divided into 10 main categories describing good accountability.

For example, it's fundamental to have strong leadership and oversight, with a positive tone from the top. Proportionate policies and appropriate training and support are also helpful. Most large media organisations are required to have a data protection officer (DPO). If you are not sure whether you need a DPO, you can use our [interactive tool](#) to help you decide.

People need to receive clear information from you about exercising their rights and know how to do so through straight-forward processes (see [Individual rights](#)). Children, in particular, benefit from clear and timely privacy information (see [Justifying your use of personal data](#)).

Processes for managing records will help to ensure you are accountable. You are required to keep a specific record of your processing activities (ROPA) and the lawful basis or bases you rely on (see [What does processing personal data lawfully mean?](#)). People should be able to find this easily in your privacy notice.

Good accountability also includes having clear processes for managing data sharing and written contracts with all processors (see [Be clear about roles and responsibilities](#)).

Data protection by design and by default

You are required to integrate data protection into what you do whenever you design a new system, process or policy, and use only the personal data that is necessary. This is known as data protection by design and by default. This is particularly important if you are processing children's personal data.

Data protection impact assessments

Having appropriate measures in place helps you manage data protection risks. In particular, you need to do a DPIA for any type of processing that is likely to result in a high risk to individuals. Much of the day-to-day work of journalists will not involve high risk processing. However, there will be some processing that does involve greater risks, such as:

- personal data about vulnerable individuals;
- sensitive or highly personal data; or
- special category or criminal offence data.

You can use our [screening checklist](#) to help you decide when to do a DPIA. It's helpful to do a DPIA for any major project that requires you to process personal data.

You do not need to carry out a DPIA for every individual story that is likely to involve high risk processing. The ICO recognises that DPIAs need to be practical in the journalism context. A more general DPIA, or series of DPIAs, that apply to the overall type of processing (eg special investigations journalism) is very likely to be sufficient in most cases, as long as it:

- covers the different types of processing you carry out;
- identifies the associated risks; and
- identifies where those risks can be mitigated.

Generally, organisations covered by UK GDPR must inform the ICO prior to processing if a DPIA identifies that a type of processing is likely to result in a high risk which cannot be mitigated. Although you always need to do a DPIA for any processing that is likely to result in a high risk to individuals, you do not necessarily need to inform the ICO when you are unable to mitigate the risk.

The DPIA process is intended to provide an extra layer of risk management when data protection risks cannot be mitigated. Consulting the ICO about your DPIA may not be necessary or proportionate. It may even be impossible or unrealistic in the circumstances. The special purposes exemption is the main mechanism that protects journalism in the DPA 2018. You may consider that this exemption applies to the specific requirement to inform the ICO when a DPIA concludes that there are risks you cannot mitigate (see [What is the special purposes exemption?](#)).

Key legal provisions

[UK GDPR article 5, para. 2](#) – the accountability principle

[UK GDPR article 24](#) – responsibility of the controller

[UK GDPR article 25](#) – Data protection by design and by default

[UK GDPR article 28](#) – processor requirements

[UK GDPR article 30](#) – records of processing activities

[UK GDPR articles 35 and 36](#) – Data protection impact assessment and prior consultation

[UK GDPR articles 37, 38, 39](#) – Data protection officers

3. Keep personal data secure

At a glance

- Security is a key principle of data protection law. It involves protecting personal data against unauthorised or unlawful processing and accidental loss, destruction or damage.
- You can protect personal data by putting in place appropriate and risk-based organisational and technical security measures. This involves cyber-security as well as how your staff handle paper records, for example.
- Your security arrangements should take into account the heightened security risks that may arise as a result of the work that journalists do. For example, risks concerning remote working, the use of portable devices, such as laptops and smart phones, and portable media, such as USB memory sticks.
- Asking processors acting on your behalf to show that they can keep personal data secure also helps you to protect people's personal data.
- You always need to comply with the security principle. As with the accountability principle, it provides strong foundations to help you to comply with other aspects of data protection law.

In more detail

- [What does processing personal data securely mean?](#)
- [Why is it important to process personal data securely?](#)
- [How do we process personal data securely?](#)

What does processing personal data securely mean?

The “integrity and confidentiality”, or security principle, is one of the seven key principles in the UK GDPR. It requires you to keep personal data secure. This includes protecting it from unauthorised or unlawful processing and accidental loss, destruction or damage. This principle includes cyber-security as well as physical and organisational security measures.

You must always comply with the security principle, although you may rely on the special purposes exemption relating to other data protection provisions (see [What is the special purposes exemption?](#)).

Further reading:

[Guide to the UK GDPR: Security](#)

[ICO Accountability Framework](#)

[Working from home](#)

[Bring your own device – what should we consider?](#)

Why is it important to process personal data securely?

Information security is a crucial legal requirement. It is also important because poor information security leaves your systems and services at risk and may cause real harm and distress to individuals.

Information security also supports good data governance more broadly. It helps you to demonstrate that you are complying with other aspects of the UK GDPR in accordance with the accountability principle (see [Be able to demonstrate your compliance](#)).

Getting security right will help you to minimise risks and maintain people's trust when you handle personal data. It will also help you to build a good reputation.

How do we process personal data securely?

You can comply with the security principle by considering the circumstances and the risks of what you do with personal data, in order to put in place appropriate and proportionate measures.

We have included security in the ICO's [Accountability Framework](#). This will help you to consider appropriate organisational and technical security measures.

Working practices

Journalism often involves working flexibly in different environments, including a strong reliance on mobile devices. A good security policy will help you to take into account the fast-paced nature of the industry and all the different types of portable devices and media that you could use to record personal data. Notebooks, mobiles, dictation machines, tablets, laptops and memory sticks are some examples. It's helpful for policies to demonstrate how you manage the associated security risks.

Where you have a business need to store personal data on removeable media, you are required to minimise it (see [Using the right amount of personal data](#)).

You can take into account the available technology and the costs of implementation. There are a wide range of solutions that allow you to implement security measures easily. You can consider widespread techniques such as encryption and password protection. This is important for all the devices you use, including mobile phones.

As controller, you are responsible for ensuring any processors you use are compliant with the UK GDPR (see [Be clear about roles and responsibilities](#)). You are required to have a written contract with processors that you are confident can comply with data protection law. You may find it helpful to use a third party processor to help you to demonstrate that you are complying with the security principle.

Whatever security measures you decide are appropriate, reviewing their effectiveness regularly will help to make sure personal data remains safe. It prevents risks developing and your security being compromised. For example, software may become unsupported and there may be an increased risk of unauthorised access to your systems.

Reporting personal data breaches

You are required to report personal data breaches to individuals when there is likely to be a high risk to the individual concerned. The special purposes exemption can apply to this requirement where necessary (see [What is the special purposes exemption?](#)). For more information about reporting breaches, see the [UK GDPR: Personal data breaches](#).

Key legal provisions

[UK GDPR article 5, para. 1\(f\)](#) – the security principle

[UK GDPR article 25](#) – data protection by design and by default

[UK GDPR article 28](#) – requirement for processors to provide “sufficient guarantees”

[UK GDPR article 32](#) – security of processing

[UK GDPR article 33 and 34](#) – notification of personal data breaches

4. Justify your use of personal data

At a glance

- Processing personal data lawfully, fairly and transparently is a key principle of data protection law. It helps you to make sure that individuals are treated according to commonly accepted general standards in a way that is free from dishonesty and injustice.
- This principle also helps you to balance different interests, which is often a key part of a journalist's role.
- You can process personal data lawfully using one of the lawful bases under the UK GDPR. You can also process special category or criminal offence data if you can satisfy one of the conditions concerning this type of personal data.
- One of the conditions concerns the disclosure of information for the purposes of journalism in connection with unlawful acts and dishonesty. This condition allows controllers to disclose these types of sensitive personal data to journalists in some circumstances.
- You can process personal data fairly by considering what a person would reasonably expect in the circumstances and whether the processing would cause any unwarranted harm.
- You can comply with people's right to be informed by providing privacy information when you collect their personal data.
- If you have collected personal data about an individual from someone else, you do not have to provide privacy information if doing so would be impossible or would seriously impair your work.
- The special purposes exemption provides additional protection for journalism where necessary.

In more detail

- [What does "lawful" processing of personal data mean?](#)
- [Why is it important to process personal data lawfully?](#)
- [How do we process personal data lawfully?](#)
- [What is special category data?](#)
- [How do we process special category data lawfully?](#)
- [What is criminal offence data?](#)
- [How do we process criminal offence data lawfully?](#)
- [What does "fair" processing of personal data mean?](#)
- [Why is it important to process personal data fairly?](#)
- [How do we process personal data fairly?](#)
- [What does "transparent" processing of personal data mean?](#)

- [Why is transparency important?](#)
- [How do we process personal data transparently?](#)

What does “lawful” processing of personal data mean?

Under data protection law, you can process personal data under a specific lawful basis. There are six lawful bases:

1. Consent
2. Contract
3. Legal obligation
4. Vital interests
5. Public task
6. Legitimate interests

There are also conditions for processing particularly sensitive types of data.

You can process personal data lawfully by checking that you are acting in line with other laws as well, including statutory and common law obligations, whether criminal or civil.

Further reading:

[Guide to the UK GDPR: Principles – Lawfulness, fairness and transparency](#)

[Guide to the UK GDPR: Lawful basis for processing](#)

[Guide to Data Protection: Key data protection themes – children](#)

[Age appropriate design: a code of practice for online services](#)

Why is it important to process personal data lawfully?

The requirement to have a lawful basis or bases when you process personal data is one of the key principles of data protection law. As part of an individual’s right to be informed, you are required to tell people which lawful basis you are relying on in your privacy notice (see [What does transparent processing of personal data mean?](#)). Individuals have the right to have personal data erased if you have processed it unlawfully. The lawful basis you rely on can also affect other rights available to individuals.

How do we process personal data lawfully?

As a first step, consider which lawful basis or bases are most appropriate for your purposes before you begin processing, and record it. We have an

[interactive tool](#) to help you to decide. The lawful bases most likely to be relevant to processing for the purposes of journalism are as follows:

Legitimate interests

You can rely on this lawful basis when the processing is necessary to pursue legitimate interests and where those interests are not outweighed by any harm caused to an individual.

It may be helpful to ask yourself the following questions:

1. Am I pursuing a legitimate interest?
2. Is it necessary to process the personal data to pursue that legitimate interest?
3. Do the individual's interests outweigh the legitimate interests I am pursuing?

Legitimate interests can be your own or third party interests. They may be commercial in nature or focused on wider societal benefits. For example, there is a legitimate interest in journalism because of the special public interest in freedom of expression and information.

Processing the personal data to pursue the legitimate interests you identify must be necessary. In this context, "necessary" means sufficiently targeted. To make sure your processing is sufficiently targeted, consider whether there is another reasonable and less intrusive way to achieve the same result.

This lawful basis also involves considering whether the individual's interests outweigh your legitimate interests. In other words, what would be proportionate.

You are required to take extra care when dealing with children's personal data and to consider their best interests in accordance with the [United Nations Convention on the Rights of the Child](#).

Consent

You can rely on consent if you give individuals genuine choice and control over when and how you use their personal data.

If you ask individuals to consent to the processing, make sure your request for consent is prominent and separate from other terms and conditions. The UK GDPR sets high standards for consent. To comply:

- ask people to positively opt-in, rather than assuming they have consented unless they opt-out;

- use language that is easy to understand;
- specify why you want the data and what you're going to do with it;
- provide options for people to consent separately to different purposes and types of processing;
- name your organisation and any third party controllers who will be relying on consent;
- tell individuals that they can withdraw their consent; and
- tell individuals that they are able to refuse consent without detriment.

If you are processing children's personal data, consider the child's competence and ability to understand consent. When offering an online service directly to children, only children aged 13 or over are able to consent. For children under 13, get consent from whoever holds parental responsibility for the child.

People can withdraw their consent at any time and you must make it easy for them to do so. If someone withdraws their consent, this does not affect the lawfulness of the processing up to that point. However, you will need to stop any processing that was based on consent.

Media organisations, particularly broadcasters, may rely on 'written releases' from actors and contributors to programmes. If your processing is based on consent, bear in mind that an individual could withdraw their consent at any point, including at a late stage. Consider relying on a different lawful basis from the start if this may cause problems, such as the contract lawful basis. For example, there may be financial consequences for a broadcaster if a contributor withdraws consent at a late stage.

Be clear about your lawful basis from the start before you begin any processing. Keep in mind that retrospectively changing your lawful basis is likely to breach the first data protection principle, which includes processing personal data fairly and transparently.

What is special category data?

Special category data is personal data revealing or concerning information about:

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

- sex life; or
- sexual orientation.

How do we process special category data lawfully?

Special category personal data needs more protection because it is sensitive.

Considering why you want to process the personal data will help you to choose one of the six lawful bases and one of the additional conditions for processing this type of data. There are 10 conditions under the UK GDPR for processing special category personal data. Those most likely to be relevant to journalism are:

Explicit consent

As well as meeting the high standard of consent that is required by the UK GDPR generally, explicit consent must be expressly confirmed in words.

Manifestly made public by the data subject

This condition applies if the processing of personal data relates to personal data which is “manifestly made public by the data subject”.

The individual concerned must have made the information public, and it must be clear that this is the case. The data must also be realistically accessible to a member of the general public. Disclosures to a limited audience are not necessarily “manifestly public”.

It is best to be cautious when applying this condition to information obtained from social media posts, taking into account:

- the nature of the information;
- whether it is available freely or only to a limited number of people on social media;
- how long ago was it put on social media;
- if there is evidence that it was put on social media by someone other than the individual concerned; and
- whether they were they a child when it was put on social media.

Individuals may not be aware of their default settings and may make their personal data public without realising it. Considering whether you are acting fairly in line with the first data protection principle will help you to handle appropriately online personal data you want to use. You may also find it helpful to consider [IPSO's Guidance for journalists: Using material from social media](#).

As acknowledged in [HM Courts and Tribunal Service guidance on media access](#), the media have an important role in facilitating public transparency about justice. As a consequence of the general principle of open justice, an offender may be deemed to have manifestly made information about his or her offending public. Criminal trials take place in public, and the verdicts returned and sentences imposed are public acts. It is generally lawful to report on these matters at the time of the trial and subsequently, subject to certain restrictions.

Rehabilitation of Offenders Act

An individual may reasonably expect privacy as a result of the passage of time, even when personal data was initially manifestly made public. Considering the circumstances will help you to decide whether an individual's expectations are reasonable. Whether or not a conviction is "spent" under the Rehabilitation of Offenders Act 1974 (ROA 1974) is generally a weighty factor (see [NT1 & NT2 and Google LLC and ICO \[2018\] EWHC 799 \(QB\)](#)).

The ROA 1974 provides that some convictions become spent after the end of a specified rehabilitation period. There is a strong public interest in the rehabilitation of offenders that is recognised by the ROA 1974. However, this does not mean that the information automatically becomes private when a conviction is spent under the legislation. You can consider each case on its own merits by taking into account the rights of privacy and freedom of expression to decide what outcome is proportionate (see [What does "in the public interest" mean?](#)).

Case example

[NT1 & NT2 and Google LLC and ICO \[2018\] EWHC 799 \(QB\)](#).

NT1 and NT2 asked Google to remove links of media reports about spent convictions regarding business activities.

The judge said:

"The starting point, in respect of information disclosed in legal proceedings held in public, is that a person will not enjoy a reasonable expectation of privacy. But there may come a time when they do... As a matter of general principle, the fact that a conviction is spent will normally be a weighty factor against the further use or disclosure of information about those matters, in ways other than those specifically envisaged by Parliament...But the specific rights asserted by the individual concerned will still need to be evaluated, and weighed against any competing free speech or freedom of information

considerations, or other relevant factors, that may arise in the particular case”.

Reasons of substantial public interest (with a basis in law)

You can rely on the “reasons of substantial public interest” condition under the UK GDPR to process special category data by satisfying one of the 23 additional substantial public interest conditions in Part 2 of Schedule 1 of the DPA 2018. Satisfying one of these conditions means that you have a valid “basis in law” allowing you to process the personal data.

Journalism in connection with unlawful acts and dishonesty

One of the 23 specific substantial public interest conditions in the DPA 2018 is “journalism in connection with unlawful acts and dishonesty”. This condition applies if the processing consists of the disclosure of personal data for the purposes of journalism and is carried out in connection with the following (whether alleged or established):

- the commission of an unlawful act by a person;
- dishonesty, malpractice or other seriously improper conduct of a person;
- unfitness or incompetence of a person;
- mismanagement in the administration of a body or association; or
- a failure in services provided by a body or association.

In a similar way to the tests that form part of the special purposes exemption for journalism, you can rely on this condition by showing that:

- the processing is necessary for reasons of substantial public interest;
- carried out with a view to the publication of the personal data by any person; and
- you reasonably believe that publication of the personal data would be in the public interest.

“Substantial public interest” reflects the extra protection that applies to special types of personal data. You can process this type of personal data by identifying a public interest that is considerably important and sufficient to justify your processing.

The condition concerns the disclosure of personal data for the special purposes. For this reason, you can consider the special purpose exemption to allow you to process any personal data that is disclosed to you by a controller using this condition (see [What is the special purposes exemption?](#)).

This condition can be used to justify the disclosure of personal data by a controller of personal data to a journalist when the relevant tests set out above are met. In other words, the condition can be used by the person or organisation that discloses information to you to allow them to do this lawfully, such as in a whistle-blowing scenario, for example.

It is a criminal offence to disclose personal data without a controller's consent, although there are public interest defences (see [Disputes and enforcement](#)).

What is criminal offence data?

Data protection law gives extra protection to personal data relating to criminal convictions and offences or related security measures. We refer to this as criminal offence data.

This covers a wide range of information about:

- criminal activity;
- allegations;
- investigations; and
- proceedings.

It includes data that is obviously about a specific criminal conviction or offence and also any other personal data relating to it. This includes:

- unproven allegations;
- information relating to the absence of convictions; and
- personal data of victims and witnesses of crime.

It also covers a wide range of related security measures, including:

- personal data about penalties;
- conditions or restrictions placed on an individual as part of the criminal justice process; or
- civil measures which may lead to a criminal penalty if not adhered to.

How do we process criminal offence data lawfully?

Considering why you want to process criminal offence data will help you to choose one of the six lawful bases set out in data protection law (see [What does "lawful" processing of personal data mean?](#)) and a relevant additional condition.

There are 28 conditions available for the processing of criminal offence data set out in schedule 1 of the DPA 2018. Those most likely to be relevant to journalism are:

- journalism in connection with unlawful acts and dishonesty;
- consent; or
- manifestly made public by the data subject.

These conditions apply in the same way as they do in the context of special category data, with the exception of consent which does not need to be explicit in the case of criminal offence data.

Criminal allegations

The general starting point regarding criminal allegations is that a suspect has a reasonable expectation of privacy regarding investigations, including the fact that there is an investigation. This is the case both in relation to police investigations (see [Sir Cliff Richard OBE v the BBC \[2018\] EWHC 1837 \(Ch\)](#) para. 251) and investigations by “an organ of the state” (see [ZXC v Bloomberg LP \[2020\] EWCA Civ 611](#) para. 82).

This is relevant if you are:

- relying on the legitimate interests lawful basis;
- considering fairness (see [What does it mean to process personal data fairly?](#)); or
- considering the public interest part of the special purposes exemption for journalism (see [What does “in the public interest” mean?](#)).

Generally, it is reasonable for a suspect not to wish others to know about an investigation because of the stigma attached and the damage that could be caused to their reputation. There may also be a risk of prejudice to the course of justice (see [Attorney-General v MGN Limited and News Group Newspapers Ltd \[2011\] EWHC 2074 \(Admin\)](#)).

[College of Policing guidance on Relationships with the Media](#) acknowledges that privacy is the general starting point during investigations. At paragraph 3.5.2 it says:

“Decisions must be made on a case-by-case basis but, save in clearly identified circumstances, or where legal restrictions apply, the names or identifying details of those who are arrested or suspected of a crime should not be released by police forces to the press or the public. Such circumstances include a threat to life, the prevention or detection of crime or a matter of public interest and confidence”.

While assuming that a suspect has a general expectation of privacy is a legitimate starting point, it is not an absolute rule. There may be a reason why an expectation of privacy is not reasonable in the circumstances. For example, the alleged activity may have taken place in a public place in circumstances where it would not be reasonable to expect privacy eg rioting. It may also be the case that an originally reasonable expectation no longer exists. The police may disclose information for operational reasons, for example.

There may be some limited circumstances where the public interest may justify identifying a suspect. However, you should carefully consider the weight of this (see [What does "in the public interest" mean?](#)). As the harmful consequences of identifying a suspect are likely to be substantial, having strong public interest conditions in your favour will help you to justify publication of criminal offence data. This involves asking yourself whether publication is necessary to best serve the public interest.

When considering where an arrest took place and any resulting impact on the right to privacy, keep in mind that reporting an arrest in the media can attract substantially more attention than would otherwise be the case. This is different to the level of public exposure that results from a small or limited group having knowledge, such as neighbours.

You may need to consider a suspect's public profile in some cases. Considering the specific circumstances will help you to judge the bearing that the individual's profile has on the balance of the public interest. When dealing with allegations about someone with a public profile, it may be relevant to consider that individuals with a public profile may be more vulnerable to false allegations (see [Sir Cliff Richard OBE v the BBC \[2018\] EWHC 1837 \(Ch\) para. 244](#)). An allegation that causes reputational harm may also be more damaging to such individuals because of their public status.

Case example

[Sir Cliff Richard OBE v the BBC \[2018\] EWHC 1837 \(Ch\)](#)

This case concerned the BBC's decision to broadcast the police search of Sir Cliff Richard's home and to name him specifically as the subject of a police investigation into an allegation of sexual abuse.

The judge agreed that Sir Cliff Richard's promotion of his Christianity "might make disclosure of actual conduct which might be regarded as unchristian something to which he has rendered himself vulnerable by virtue of his public

position. However, that does not mean that unsubstantiated allegations or investigations, into unproved conduct, fall into the same category”.

The judge added that “...it is precisely because of that contrast that the publication of the material is capable of being so intrusive...and so damaging to his reputation and life...”.

What does “fair” processing of personal data mean?

You are required to process personal data fairly in accordance with the data protection principle.

You can process personal data fairly by processing:

- personal data in ways that people would reasonably expect, without misleading them when you obtain the data; and
- personal data in ways that do not cause unwarranted harm to an individual.

This also means you are required to make sure that you treat individuals fairly when they seek to exercise their rights over their data, and help them to exercise their rights.

Further reading

[Guide to the UK GDPR: Principles – Lawfulness, fairness and transparency](#)

Why is it important to process personal data fairly?

All of the data protection principles are legal requirements. We all expect and hope to be treated fairly when our personal data is used. The concept of fairness in data protection law is designed to make sure that people are treated according to commonly accepted standards in a way that is free from dishonesty and injustice generally. It also seeks to make sure that there is a proper balancing of conflicting interests, which is central to a functioning democracy (see [Why is it important to balance journalism and privacy?](#)).

How do we process personal data fairly?

Processing personal data fairly is closely linked to processing it lawfully and transparently, which is why they are part of the same data protection principle. You can comply with this principle by processing personal data lawfully and providing people with appropriate privacy information.

Reasonable expectations and unwarranted harm

To process personal data fairly, it is helpful to first consider whether processing the personal data would be within the reasonable expectations of an individual, taking into account all the circumstances.

When in doubt about whether people may have a reasonable expectation of privacy, points that may help you include:

- the individual concerned (eg are they an adult or a child? Are they a public figure or do they perform a public role?);
- the nature of the activity in which the individual is engaged; and
- the place where the activity is happening.

As well as considering reasonable expectations, it is also relevant to consider any unwarranted harm the processing may cause. Not all harm is unwarranted however. You can process personal data by being clear about how you justify it even if it causes some harm.

Public figures and public role

Even though there may be a stronger public interest for publication of information about individuals with a public profile, they may still have a reasonable expectation of privacy in the specific circumstances. A public figure may attract or seek publicity about some aspects of their life without necessarily losing the right to privacy regarding other matters.

In [Sir Cliff Richard OBE v the BBC \[2018\] EWHC 1837 \(Ch\)](#), the judge said:

“...the very act of making certain aspects of oneself public means...that there is a corresponding loss of privacy in those areas which are made public. However, it does not follow that there is some sort of access the board diminution of the effect of privacy rights...It depends on the degree of ‘surrender’, the area of private life involved and the degree of intrusion into the private life.”

Information in the public domain

If the information, or similar information, about the individual is already in the public domain, the impact on any reasonable expectation of privacy is a matter of fact and degree.

Information will not necessarily lose its private character simply because an individual:

- has already disclosed personal data relating to the same or similar parts of their life;
- (or another person) has already disclosed certain facts relating to the personal data;
- intends to publish the personal data in the future; or
- (or another person) may or would be able to publish the personal data in another country according to different laws.

Photographs or filming, especially in public

You can consider whether publication of photographs is fair in the same way as any other information, although it is helpful to keep in mind that photographs or film of an individual may be particularly intrusive. The impact may be greater if an individual is continually photographed or recorded, or if it wasn't clear to them what you were doing (see [Covert surveillance, subterfuge and similar intrusive methods](#)).

Individuals should reasonably expect that they may sometimes be photographed or caught on film in public in an incidental way. If an individual's image is captured in public and they are the subject of the photograph or film, you can comply with data protection law by considering whether the processing would be fair in the circumstances, even though the activity is happening in a public place. Acting proportionately will help you to do this. For example, it may not be necessary for your story to publish all the information you have if this would cause unwarranted harm (see [Naomi Campbell v MGN Ltd. \[2004\] UKHL 22](#)).

Covert surveillance, subterfuge and similar intrusive methods

The use of covert surveillance, subterfuge and other intrusive methods as the means of uncovering stories may cover a range of different techniques. Such techniques include the use of private detectives, covert recording, disguise, and long-lens photography. Such methods may be deployed in the context of investigative journalism.

Under data protection law, it is likely to be unfair to mislead people about a journalist's identity or intentions. However, you can consider the special purposes exemption if you plan to use undercover or intrusive covert methods to get a story (see [What is the special purposes exemption?](#)). Before doing so, it is helpful to consider whether it is necessary to use these methods.

If you do decide to rely on the special purposes exemption, bear in mind that the intrusive (in some cases extremely intrusive) nature of this activity may

mean that it is more difficult to justify it in the public interest. If you are processing special category data, such as details about an individual's sex life, or criminal offence data, there is a much greater risk of harm (see [What does "in the public interest" mean?](#))

It is more likely to be appropriate to keep a record of your decision-making if you decide to use these methods because of the higher level of risk.

There are criminal offences in the DPA 2018, including to knowingly or recklessly obtain personal data from another controller without its consent. This includes blagging (obtaining private or confidential information by impersonation or another method), hacking, or other covert methods. However, there are public interest defences available. We will also consider any other potentially relevant defence under the DPA 2018 (see [Disputes and enforcement](#)).

What does "transparent" processing of personal data mean?

Transparency is fundamentally linked to fairness. It means that you are clear, open and honest with people from the start about who you are and how and why you use their personal data.

Individuals have the right to be informed about the collection and use of their personal data. This type of information is known as privacy information.

You are normally required to provide privacy information to people when you collect their personal data. When obtaining personal data from other sources, you do not need to provide individuals with privacy information if:

- the individual already has the information;
- providing the information would be impossible;
- providing the information would involve a disproportionate effort;
- providing the information would render impossible or seriously impair the achievement of the objectives of the processing;
- you are required by law to obtain or disclose the personal data; or
- you are subject to an obligation of professional secrecy regulated by law that covers the personal data.

You can provide effective privacy information by checking that the information you provide is concise, intelligible and easily accessible. It is particularly important to use clear and plain language for children.

It will help you to be transparent if you regularly review, and where necessary, update your privacy information. Before you process personal data, bring any new uses of personal data to the individual's attention.

Further reading

[Guide to the UK GDPR: Principles – Lawfulness, fairness and transparency](#)

[Guide to the UK GDPR: Right to be informed](#)

Why is transparency important?

All of the data protection principles are legal requirements. Being clear and informing people about what you are doing in a way that is easy for them to understand is important. This enables individuals to exercise control over what is happening to their personal data, where appropriate. You need to take particular care when dealing with children or vulnerable individuals and where processing is complex or automated. Transparency will also help to build and sustain people's trust.

How do we process personal data transparently?

Providing privacy information to individuals

You can provide privacy information to people by putting it online, on your website for example (known as a privacy notice). Privacy information needs to be easily accessible and individuals should be aware of it.

Privacy information must be clear for everyone but in particular for children. Age-appropriate privacy information will help children to exercise their data protection rights.

If you have collected an individual's personal data from them directly, you always need to provide privacy information, unless the individual already has the information. You can consider the special purposes exemption if you believe that providing privacy information would be incompatible with journalism (see [What is the special purposes exemption?](#)). For example, if you are conducting an investigation that requires you not to disclose to individuals what you will be doing with their personal data, you may wish to rely on the special purposes exemption (see [Covert surveillance, subterfuge or similar intrusive methods](#)).

If you have collected an individual's personal data from other sources, there are exceptions from the obligation to provide privacy information that could protect journalism. For example, you can rely on an exemption if providing the information would involve disproportionate effort or seriously impair or render impossible the achievement of your objectives (see [What does transparent processing of personal data mean?](#)).

In the context of journalism, we accept that it is not always reasonable (or even possible) to provide an individual with privacy information. This could be because it is not practical to do so, for example because you don't have their contact details. It could also be because informing the individual would undermine your journalistic purposes in some way. An investigation may be undermined if an individual finds out about it, for example.

If none of these exemptions apply, you can also consider whether the special purposes exemption applies, which offers protection when a data protection provision is incompatible with journalism. You need to demonstrate a reasonable belief that publication is in the public interest to rely on the special purposes exemption. In determining whether you have a reasonable belief, it may be relevant to consider the extent to which you gave the individual concerned the opportunity to respond or comment (see [What is the special purposes exemption?](#)).

You should consider if the stage a story or investigation is at could make a difference to whether you provide privacy information and when you provide it. For example, if you are conducting an investigation, it may be justifiable not to inform the individual at first if doing so would prevent you from conducting the investigation. However, it may be fair to provide privacy information at a later stage. You may find it helpful to consider the [BBC's Editorial guidelines](#) on offering a right to reply.

Whether or not you provide privacy information to individuals, privacy information should be kept up-to-date.

Key legal provisions

[UK GDPR article 5\(1\)\(a\)](#) – the lawfulness, fairness and transparency principle

[UK GDPR article 6](#) – lawfulness of processing

[UK GDPR article 9](#) – processing of special category data

[UK GDPR article 10](#) – processing of criminal offence data

[UK GDPR articles 13 and 14](#) – right to be informed

[UK GDPR article 17\(1\)\(d\)](#) – right to erasure when personal data has been processed unlawfully

[DPA 2018 Schedule 1, paragraphs 1-37](#) – conditions for processing criminal offence data

[DPA 2018 part 2 of schedule 1](#) – substantial public interest conditions for special category data

5. Take reasonable steps to ensure personal data is accurate

At a glance

- Accuracy is a key data protection principle. Taking reasonable steps to make sure that personal data is accurate is fundamental to both journalism and data protection.
- Complying with this principle complements journalism by helping to maintain public trust. It will also help you to protect the public from harm caused by inaccurate personal data, which can be magnified and spread quickly online.
- You can comply with the accuracy principle by taking reasonable steps to correct or erase personal data where necessary.
- Clearly distinguishing between fact and opinion, and taking the context into account, will help you to make sure personal data is accurate.
- You should be able to comply with the accuracy principle in the majority of cases because it complements the public interest served by journalism. Where necessary, the special purposes exemption also protects journalism.

In more detail

- [What does being accurate mean?](#)
- [Why is it important for personal data to be accurate?](#)
- [How do we make sure the personal data we hold is accurate?](#)

What does being accurate mean?

The requirement to make sure that the personal data you hold is accurate is one of the data protection principles. Where necessary, you are required to keep personal data up-to-date and take every reasonable step to correct or erase personal data.

You can comply with the accuracy principle by:

- taking reasonable steps to make sure that personal data is accurate;
- making sure that the source and status of the personal data is clear;
- carefully considering any challenges to the accuracy of information; and
- considering whether it is necessary to periodically update the information.

Further reading:

[Guide to UK GDPR: Principles – Accuracy](#)

Why is it important for personal data to be accurate?

As well as being a key legal requirement, accurate use of personal data is at the core of a journalist's work and industry codes of practice. Maintaining public trust by using accurate personal data protects the important public interest served by journalism and can boost your reputation as a reliable source of news.

Processing personal data accurately helps to protect individuals from harm, such as reputational damage. This is particularly important considering how inaccurate information can be magnified and spread quickly online.

How do we make sure the personal data we hold is accurate?

Having appropriate measures in place helps you to comply with the accuracy principle. Some simple practical measures that you could consider include:

- policies to set out a clear process for checking facts and sources;
- an accuracy checklist or flowchart to support journalists in their work;
- or
- systems to record inaccuracies and monitor recurring themes.

Reasonable accuracy checks

Given the quantity and pace of journalistic output, and the judgement which it often requires, some accidental inaccuracies are inevitable. However, even in lower profile stories, you are required to take reasonable steps to check the personal data you are processing is accurate.

Considering the circumstances will help you to decide what checks are reasonable, including the urgency of the particular story and the risks of harm to individuals. More robust checks are likely to be appropriate where there is a greater risk of harm.

You may find it helpful to refer to the [BBC's Editorial guidelines](#) about accuracy and gathering material. These say that, where possible, you should:

- "gather material using first-hand sources;
- check facts and statistics, identifying important caveats and limitations;

- validate the authenticity of documentary evidence and digital material;
- corroborate claims and allegations made by contributors;
- weigh, interpret and contextualise claims, including statistical claims”.

There may be circumstances where you decide that it is in the urgent public interest to publish personal data without carrying out your normal accuracy checks. This may be a challenge when broadcasting live, for example.

You still need to be able to show that thought was given by someone at an appropriate level to whether the publication is reasonable. Relevant factors may include:

- what checks might be possible;
- whether publication could be delayed; and
- the nature of the public interest at stake.

If you go ahead with publication in the above circumstances, you should be as clear as possible that you are reporting on unconfirmed facts, and any potential inaccuracies. In any decision you make, you should factor in the risk of the information you report spreading quickly online, without appropriate context. You may find it helpful to consider [IPSO's guidance on reporting major incidents](#).

Facts, opinions and context

You can comply with the accuracy principle by clearly distinguishing between fact and opinion when reporting information about individuals. Some programmes may involve a blend of factual and fictional elements about individuals, so you need to make the extent of the facts clear.

While deciding what editorial position to take when reporting the news, it is important to make sure that personal data continues to be presented accurately. You may need to clarify the nature or context of some content specifically to avoid compromising the accuracy of the personal data. For example, check that headlines are supported by the text.

The courts sometimes take into account defamation law when considering the distinction between facts and opinions, and the importance of context (see [Aven and Others v Orbis Business Intelligence Limited \[2020\] EWHC 1812 \(QB\)](#)). It may be helpful for you to consider how the words would strike the ordinary reasonable reader, taking into account their context and the subject matter when determining whether personal data is a fact or an opinion.

Sources of information

There is a strong public interest in the public being confident in the accuracy of personal data. If possible and the details are not confidential, being clear about the source will help the public to be confident in the accuracy of personal data by allowing them to judge the source's status.

When you need to protect a source, there is also a strong level of confidence associated with the source's identity and a strong public interest in respecting confidences. To comply with the accuracy principle, try to provide what information you can about the source, if appropriate, and not say anything inaccurate about their status.

Wherever possible, keeping records about your sources and other research that you use to report an individual's personal data will allow others to verify the accuracy of the information you use, where necessary.

Take care with material supplied by third parties, including other news providers. If personal data within a story was originally inaccurate, the harm can be perpetuated and magnified if the same story is repeated elsewhere. It is best not to assume that reasonable checks have already been done by third parties, even by news organisations that you judge to be reputable. Seeking assurance that reasonable accuracy checks have been done helps to protect your reputation as a reliable news source and builds public trust.

Social media

There may be a higher risk when using internet sources, social media or other user-generated content. For example, inaccuracy on social media may be deliberate and can be very damaging to an individual. Individuals, particularly children, may not realise the extent to which information has been shared and the possible consequences. You may find it helpful to consider [IPSO's Guidance for journalists: Using material from social media](#).

Dealing with complaints

You are required to help and support people to exercise their individual rights under data protection law (see [Individual rights](#)). Proportionate policies and clear routes for people to get in touch will help you to comply.

If an individual complains that you have processed inaccurate personal data, policies and procedures will help you to investigate and correct or erase it where necessary. Individuals have the right to have incorrect personal data rectified (see the [Right to rectification](#)). Individuals do not have the right to

erasure just because personal data is inaccurate, but it may be reasonable to erase the data in some cases (see the [Right to erasure](#)).

Corrections

You can comply with the accuracy principle by keeping records of mistakes, where proportionate. You may need to add a note to make clear that you made a mistake or a correction. This may take a variety of forms, for example, an advisory line at the top of an online article, or a printed correction area in a newspaper (see [Right to rectification](#)).

Accuracy and the special purposes exemption

You should be able to comply with the accuracy principle in the majority of cases because it is also fundamental to journalism. Where necessary, the special purposes exemption specifically protects journalism.

There may be occasions when you need to refer to inaccurate personal data because this itself is part of the story. As long as it is clear that you are reporting on an inaccuracy, this does not breach the accuracy principle and you do not need to rely on the special purposes exemption. However, re-publication of the inaccurate personal data should be necessary and in line with the other data protection principles, especially the principle to process personal data fairly, lawfully and transparently

There may be some scenarios where information is deliberately inaccurate, such as satirical or parody articles. Where this is obvious, this does not breach the accuracy principle and it is not necessary to rely on the special purposes exemption.

Key legal provisions

[Article 5\(1\)\(d\)](#) – the accuracy principle

[Article 16](#) – the right to rectification

[Article 17](#) – the right to erasure

6. Process personal data for specific purposes

At a glance

- Processing personal data for specific purposes that are “compatible” with your initial purpose is a key data protection principle.
- Being clear about why you are using personal data helps individuals to be informed and exercise their rights. It also helps you to avoid function creep. This is when personal data is used for new purposes which are not acknowledged.
- You can comply with the purpose limitation principle by specifying your reasons for processing in your privacy information.
- Regular review will help you to check whether your purposes change over time and to keep your records up-to-date.
- Where necessary, the special purposes exemption specifically protects journalism.

In more detail

- [What does using personal data for specific purposes mean?](#)
- [Why is it important to use personal data for specific purposes?](#)
- [How do we limit the purpose of our processing?](#)

What does using personal data for specific purposes mean?

Purpose limitation is one of the data protection principles. You can comply with this principle by processing personal data for specified, explicit and legitimate purposes that are “compatible” with your original purpose

Identifying clearly why you are processing personal data will help you to comply with this principle. You can process personal data in line with this principle if:

- your new purpose is compatible with the original purpose;
- you get consent (see [What does it mean to process personal data lawfully?](#)); or
- you have a clear obligation or function set out in law.

If you plan to use or disclose personal data for a new purpose, the new use should be fair, lawful and transparent (see [Justifying your use of personal data](#)).

Further reading

[Guide to the UK GDPR: Purpose limitation](#)

[Guide to the UK GDPR: Exemptions](#)

Why is it important to use personal data for specific purposes?

All of the data protection principles are key legal requirements. Being clear about why you are using personal data enables people to understand what you are doing and supports them to make informed decisions. For example, it helps them to consider whether to share their data with you. It also helps people to exercise their rights and exert more control over what happens to their data.

If you specify the reasons you are using personal data from the start, this helps you to be more accountable and to avoid function creep. This is when personal data is collected for a particular purpose but its use is gradually widened to include other purposes, which may not be explicitly acknowledged or recorded.

How do we limit the purpose of our processing?

You need to specify your purpose or purposes for processing within the documentation you are required to keep as part of your records of processing. You also need to specify your purposes for processing in the privacy information you provide to people.

Regularly reviewing your processing will help you to make sure that your purposes have not changed or evolved over time. This will enable you to keep your records up-to-date too.

Purposes that are compatible with journalism

You can use personal data for a new purpose in some circumstances. If your new purpose is compatible, you don't need a new lawful basis. The retention of material that you publish in the form of a news archive is material that is held for the purposes of journalism, which is a compatible purpose.

If you originally collected the personal data using the consent lawful basis, you usually need to get fresh consent to make sure that your processing is fair and lawful (see [How do we process personal data lawfully?](#)).

Purposes that are not compatible with journalism

As a general rule, if the new purpose is very different, unexpected, or would have an unjustified impact on an individual, it is likely to be incompatible with your original purpose.

If your new purpose is not compatible with the original purpose, in practice, you are likely to need specific consent to use or disclose the data (see [What does it mean to process personal data lawfully?](#)). You may also be able to rely on an exemption, such as the special purposes exemption (see [What is the special purposes exemption?](#)).

If you have collected data for a non-journalistic purpose, and it subsequently becomes of journalistic interest, this is unlikely to be a compatible purpose. However, you may be able to rely on the special purposes exemption to process the personal data for the purposes of journalism.

Key legal provisions

[UK GDPR article 5\(1\)\(b\)](#) – the purpose limitation principle

[UK GDPR article 6\(4\)](#) – determining compatibility

[UK GDPR article 30](#) – requirement to record the purposes of the processing

7. Use the right amount of personal data

At a glance

- You are required to make sure that you have sufficient personal data to do what you need to do, that it is relevant, and not excessive. This is known as the data minimisation principle.
- Limiting the amount of personal data that you hold helps you to manage risks. It will also make it easier for you to limit requests about the personal data and to deal with them more efficiently.
- You can comply with the data minimisation principle by reviewing the personal data that you have from time to time and deleting anything you no longer need.
- Where necessary, the special purposes exemption specially protects journalism.

In more detail

- [What is data minimisation?](#)
- [Why is it important to minimise personal data?](#)
- [How do we minimise personal data?](#)

What is data minimisation?

Minimising personal data is one of the data protection principles. It requires you to make sure that the personal data you hold is:

- **adequate** (sufficient to fulfil your stated purpose);
- **relevant** (has a rational link to that purpose); and
- **limited** (you do not hold more than you need for that purpose).

You can comply with this principle by identifying the minimum amount of personal data needed to fulfil your purpose and not keeping more personal data than necessary.

Further reading

[Guide to UK GDPR: Data minimisation](#)

[Guide to UK GDPR: Right to rectification](#)

[Guide to UK GDPR: Right to erasure](#)

Why is it important to minimise personal data?

All of the data protection principles are key legal requirements. Limiting the amount of personal data that you hold helps you to manage risks. It will also make it easier for you to limit requests about the personal data and to deal with them more efficiently.

If you hold more personal data than you actually need to fulfil your purpose, people may ask you to delete it (see [Right to erasure](#)). If you hold less data than you need, you may not have a complete understanding of the facts. People also have the right to ask you to complete any incomplete data (see [Right to rectification](#)).

How do we minimise personal data?

Having appropriate data protection processes in place will help you to make sure that you only collect and hold the personal data you need. In particular, being clear about what personal data you hold and why, and identifying this in your records of processing and privacy notice, will help you to comply with this principle.

Deciding whether personal data is adequate, relevant and not excessive

It may help you to decide whether the information you hold is adequate, relevant and not excessive if you consider:

- any specific factors that an individual brings to your attention when making a request to exercise their rights;
- whether you have all the personal data that you need for your story;
- whether you have only collected personal data that is relevant to your story; and
- whether you have collected any personal data that is only remotely connected to your story.

If personal data is not relevant to your specific purpose, it may still be relevant to your more general journalistic purpose. The key point is that you are able to justify why the information is relevant (see [Deciding how long to keep personal data](#)).

Reviewing the personal data you hold from time to time will help you to check that you are not keeping data you no longer need. In the context of journalism, it may be reasonable to keep personal data for long periods or indefinitely (see [Deciding how long to keep personal data](#)).

Key legal provisions

[UK GDPR article 5\(1\)\(c\)](#) – data minimisation principle

[UK GDPR article 16](#) – right to rectification

[UK GDPR article 17](#) – right to erasure

8. Decide how long to keep personal data

At a glance

- You are required to keep personal data for no longer than necessary. This principle helps you to reduce risks and comply with other aspects of data protection law.
- A retention policy or schedule will help you to justify how long to keep personal data, where this is possible.
- Where necessary, the special purposes exemption specifically protects journalism.

In more detail

- [What is meant by keeping personal data “no longer than is necessary?”](#)
- [Why is it important not to keep personal data for longer than is necessary?](#)
- [How do we avoid keeping personal data for longer than is necessary?](#)

What is meant by keeping personal data “no longer than is necessary”?

The requirement to keep personal data only as long as necessary is one of the data protection principles.

Data protection law does not set specific time limits for different types of data. This means that you need to consider why you are processing the personal data and then decide how long you think it is reasonable for you to keep it for that purpose.

Individuals have a general right to erasure but this only applies in certain circumstances (see [Right to erasure](#)).

Further reading

[Guide to the UK GDPR: Storage limitation](#)

[Guide to the UK GDPR: Right to erasure](#)

[Guide to the UK GDPR: Documentation](#)

Why is it important not to keep personal data for longer than is necessary?

All of the data protection principles are key legal requirements. Keeping personal data for no longer than is necessary reduces the risk that it will become irrelevant, excessive, inaccurate or out-of-date. It will therefore help you to be more efficient and comply with your other legal requirements to only use data for a limited purpose, minimise it, and make sure that it is accurate.

It will also help you to deal effectively with requests from individuals to exercise their rights. For example, it may be easier to respond to requests for subject access or erasure if you only have the information that you need.

Erasing data you do not need also reduces the risk that you will use the information in error, and perhaps cause harm to those concerned.

How do we avoid keeping personal data for longer than is necessary?

You can comply with this principle by being clear about what personal data you hold and why in the first instance, and recording this in your records of processing and in the privacy information you provide to individuals.

Retention policies or schedules

Where possible, justifying why you are keeping personal data will help you to comply with this principle. This means having a clear reason for keeping it and being able to explain why it is necessary to keep it for the length of time that you want to. A retention policy will help you to do this.

Retention policies or retention schedules list the types of information you hold, what you use it for, and how long you intend to keep it. They help you to establish and document standard retention periods for different types of personal data.

Having a clear system will help you to act in accordance with your retention policy or schedule. Your system should involve reviewing the personal data you hold at appropriate intervals. There may be occasions where it is appropriate to erase personal data earlier than planned. It is helpful to proactively consider this.

If it is not possible for you to document how long you expect to keep the personal data, it's still helpful to review it periodically to make sure you are not keeping any data that you no longer need.

Research and background materials

Research and background details, such as contact details, are vital to journalism and you may wish to keep them for a long, unspecified period of time or indefinitely.

Data protection law does not impose a specific time limit on how long you can retain personal data. In some cases it will be reasonable to keep certain information indefinitely. The key point is that you are able to justify why keeping the information is proportionate to your journalistic purpose.

Considering the circumstances will help you to decide how long to keep personal data. We accept that it may often be difficult to know if and when background information about a person may be relevant in the future, in the context of journalism. However, you may be able to consider how likely you are to need the information in the future. For example, are you likely to use out of date contact details?

In cases of doubt, it may be helpful to consider the nature of the public interest concerned or any risks associated with retaining or deleting the information. There may be legal reasons why you need to keep the information for a certain period of time, for example.

Retaining news archives

Individuals have a right to erasure but this right is not absolute. There is an exemption to protect journalism if the processing is necessary to exercise the right of freedom of expression and information.

There is a strong, general public interest in the preservation of news archives, which contribute significantly to the public's access to information about past events and contemporary history. This is generally a weighty factor in favour of not erasing personal data from news archives (see [Right to erasure](#)).

Key legal provisions

[UK GDPR article 5\(1\)\(e\)](#) – the storage limitation principle

[UK GDPR article 17\(1\)\(a\)](#) – the right to erase personal data when it is no longer necessary to hold it

[UK GDPR article 30\(1\)\(f\)](#) – requirement to record time limits for erasure of different categories of data where possible

9. Be clear about roles and responsibilities

At a glance

- When a third party is involved in processing personal data, consider whether they are a controller or a processor. Controllers determine the means and purposes of the processing of personal data, whereas processors act only on instructions.
- Understanding the respective roles of yourself and third parties will help you to be clear about responsibilities.
- You are required to have a written contract with processors and they must give sufficient guarantees that they can comply with data protection law.
- If you are acting as a joint controller with a third party ie you both determine the means and purposes of the processing, the law requires you to have a transparent arrangement in place setting out your respective responsibilities.
- When sharing personal data with another controller, a data sharing agreement will help you to be clear about arrangements and responsibilities. Considering whether a DPIA is needed will help you to manage associated risks.
- Carrying out appropriate checks when third parties share personal data with you that you want to use for journalism will help you to be confident that you are complying with data protection law. Relevant checks include confirming the source, how and when the data was collected, and checking that it is accurate.

In more detail

- [What are the possible roles and responsibilities of different parties?](#)
- [Why is it important to be clear about roles and responsibilities?](#)
- [How do we make sure that we are clear about roles and responsibilities?](#)

What are the possible roles and responsibilities of different parties?

Third parties can either be a controller or a processor under the UK GDPR. The key question is who determines the purposes and means of the processing?

Controllers are the main decision-makers exercising control over the purposes and means of the processing. If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. If they are processing personal data for different purposes, they are not joint controllers.

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

Further reading:

[Guide to UK GDPR: Key definitions – Controllers and processors](#)

[Guide to the UK GDPR: Accountability and governance](#)

[Data sharing: a code of practice](#)

If you are transferring personal data internationally, for the most up-to-date information, please read [Guide to the UK GDPR: International transfers after the UK exit from the EU Implementation Period](#).

Why is it important to be clear about roles and responsibilities?

Understanding your role and the role of third parties in processing personal data and the different responsibilities is key to making sure you comply with data protection law.

The ICO has powers to take action against both controllers and processors and individuals can bring claims for compensation and damages against both.

Putting the right measures in place helps to protect individuals when others are processing their personal data. It also protects your reputation, the trust people have placed in you, and the wider public interests served by journalism.

How do we make sure that we are clear about roles and responsibilities?

Deciding whether a third party is a controller, processor or joint controller

It is worth taking the time to assess and document the status of each individual or organisation you work with that processes personal data. Your Record of processing activities (ROPA) will help you to consider this.

To help you consider whether third parties are controllers or processors, it's helpful to consider the nature of the activities they are carrying out. For example, a private investigator is likely to be a controller rather than a processor. This is because they are likely to be making independent decisions about how to investigate and determining the means and purposes of the processing, albeit that you have provided some instructions.

If, on the other hand, you ask a third party to help you and they are only permitted to act on your instructions, they are a processor. You are required to have a written contract in place in accordance with the UK GDPR's requirements. Processors also need to provide sufficient guarantees they will implement appropriate measures to meet the UK GDPR's requirements and protect individual rights.

You may also act as a joint controller. This is when two organisations or individuals jointly control the purposes and the means of the processing. The UK GDPR requires you to put in place an agreement that sets out your respective responsibilities, particularly regarding transparency obligations and individual rights. This information needs to be made available to individuals.

Data sharing with third parties

When sharing personal data between controllers, you are required to comply with the data protection principles. A key requirement is to share personal data fairly, lawfully and transparently (see [Justifying your use of personal data](#)). Particular care is needed when children's personal data is involved.

You are required to keep certain records to comply with the UK GDPR's requirements. As part of this, assess what data you are sharing and record it as appropriate (see [Be able to demonstrate your compliance](#)). It's also helpful to have a data sharing agreement in place, especially when the sharing is regular, routine or scheduled. Data sharing agreements:

- set out the purpose of the data sharing;
- cover what happens to the data at each stage;
- set standards; and
- help all parties to be clear about their roles and responsibilities.

We've created separate guidance to help you to consider common elements for data sharing agreements. You may be required to conduct a DPIA, or it may be helpful to consider carrying one out.

Receiving personal data from third parties

You should bear in mind that you are responsible for complying with data protection law concerning your own processing if you receive any personal data from another controller. You may receive personal data when working with a freelance journalist or photographer, for example.

If you want to use the information for journalistic purposes, you should generally make appropriate enquiries and checks. Relevant checks include:

- confirming the source of the data;
- identifying the relevant lawful basis;
- verifying details of how and when the data was initially collected and checking records of consent if relevant;
- checking what individuals were told and what privacy information was provided;
- checking that the data is accurate and up-to-date; and
- making sure that the data you receive is not excessive or irrelevant for your purposes.

If complying with a provision of data protection law would be incompatible with journalism, the special purposes exemption specifically protects journalism where necessary (see [What is the special purposes exemption?](#)).

Key legal provisions

[UK GDPR article 28 and 29](#) – requirements regarding processors

[UK GDPR article 30](#) – requirements to record information about processors

[UK GDPR article 32](#) – requirements to make sure that personal data is processed securely by processors

10. Help people to exercise their rights

At a glance

- Individuals have general data protection rights which they can exercise on request. These include an individual's right to access their own personal data and to ask for it to be erased if certain conditions are met. You are required to help people to exercise these rights.
- However, you may refuse to comply with individual requests in certain circumstances.
- There is a very strong, general public interest in protecting the identity of journalists' confidential sources. It is very unlikely you would be required to disclose information identifying a confidential source in response to an individual's request for their own personal data.
- You can keep records of mistakes. To make sure that your records are clear, you may need to add a note or a correction.
- The right to erasure does not apply if your processing is necessary to exercise the right to freedom of expression and information.
- There is a strong, general public interest in the preservation of news archives, which contribute significantly to the public's access to information about past events and contemporary history. This is generally a weighty factor in favour of not erasing personal data from news archives.
- Where necessary, the special purposes exemption specifically protects journalism. This applies to all individuals' rights, except for rights relating to automated processing.

In more detail

- [What are individual rights?](#)
- [Why are individual rights important?](#)
- [How do we comply with individual rights?](#)

What are individual rights?

Individuals have a number of different rights concerning their personal data as follows:

- right to be informed;
- right of access;
- right to rectification;
- right to erasure;

- right to object;
- right to data portability; and
- right related to automated decision-making, including profiling.

We have focused below on the rights most likely to be relevant in the context of journalism. Therefore, we have not included specific commentary on the last two rights within this code (see [What does it mean to process personal data transparently?](#) for information about the right to be informed).

Further reading

[Guide to UK GDPR - Individual rights](#)

[Guide to the UK GDPR - exemptions](#)

[Guide to Data Protection - children](#)

Why are individual rights important?

As well as being legal obligations, individual rights enable people to understand why and how you are processing their personal data and gives them more control over what happens to their personal data. This is fundamental to building and sustaining public trust in the use of personal data.

Complying with individual rights reduces the risks you take on whenever you process people's personal data. It can also increase your reputation, and give you a competitive edge.

How do we comply with individual rights?

You can prepare for dealing with requests by putting in place appropriate data protection measures (see [Be able to demonstrate your compliance](#)).

Refusals

Generally, you are required to comply with a request without undue delay within one month. However, you can refuse to respond to a request if an exemption or restriction applies, or if the request is manifestly unfounded or manifestly excessive.

An exemption may exempt you in whole or only in part. You should avoid taking a blanket approach. Always consider whether you are able to disclose some of the information, even if some of it is exempt.

The special purposes exemption can apply to all of the individual rights, except for those regarding automated processing.

If you refuse to comply with a request, you should explain:

- why;
- that there is a right to complain to the ICO or another supervisory authority; and
- there is a right to seek court enforcement.

Right of access

Individuals have the general right to access and receive a copy of their personal data and other supplementary information. This is known as a subject access request or SAR.

The special purposes exemption specifically protects journalism where this is necessary (see [What is the special purposes exemption?](#)). Provide any information you are able to without undermining your journalistic activities. If an individual makes a complaint to us, we may ask you to explain your decision to use the special purposes exemption.

The special purposes exemption may apply to SARs made before or after publication of a story. For example, providing information may undermine a story by tipping someone off to forthcoming publication. Resource implications may also be a relevant factor. If so, consider the nature of the request and what would be proportionate in the circumstances.

You are not required to give an individual information personal data about another individual unless:

- the other individual has consented; or
- it is reasonable to disclose it without their consent.

In most cases, a confidential source is unlikely to consent to the disclosure of their personal data to a third party. They are also likely to have a strong expectation of confidentiality as the protection of sources is considered to be fundamental to a free press, which is reflected in legislation. For example, under section 10 of the Contempt of Court Act 1981, a publisher cannot be compelled to reveal the source of published information unless a court considers it to be in the interests of justice or national security, or for the prevention of crime.

It is therefore very unlikely that you would be required to disclose information about confidential sources in response to a subject access request from another person.

Right to restriction

Individuals have the general right to restrict the processing of their personal data in certain circumstances, including when:

- you have processed personal data unlawfully and an individual requests restriction rather than erasure (see [What does it mean to process personal data lawfully?](#));
- the individual contests the accuracy of their personal data and you are verifying it (see [Take reasonable steps to ensure personal data is accurate](#)); or
- the individual objects to your processing and you are considering whether your legitimate grounds override the individual's (see [Right to object](#)).

You need to have processes that allow you to restrict personal data, if required. There are a number of different ways you could restrict data, such as:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website.

If you have disclosed the personal data to others, you need to inform them (unless you are relying on the special purposes exemption). Consider whether it is possible or proportionate to contact each recipient to tell them about the restriction. If asked, tell the individual making the request who you have disclosed their personal data to.

In many cases, the restriction is only temporary. You need to tell the individual before you lift the restriction.

Right to rectification (correcting or completing data)

Individuals have a general right to ask you to correct their personal data if it is inaccurate, or to complete it if it is incomplete (known as the right to rectification).

Some practical examples of relevant accountability measures you could take include:

- a policy setting out the process to follow when an inaccuracy is reported;
- an online form to make it easy for people to report inaccuracies; and
- reporting on inaccuracies and corrections in one place, as well as individual stories.

It's helpful to restrict your processing of the personal data while you check its accuracy. This is regardless of whether the individual has exercised their right to restriction (see [Right to restriction](#)).

If you receive a request for rectification, take reasonable steps to satisfy yourself that the data is accurate and rectify it, if necessary. This includes informing other parties of the inaccuracy if the information was disclosed to them (unless you are relying on the special purposes exemption). It's helpful to consider:

- what the requester tells you; and
- any steps you have already taken to verify the accuracy of the personal data (see [Take reasonable steps to ensure personal data is accurate](#)).

Consider the nature of the personal data and what you will use it for to help you to decide what steps are reasonable. More effort is appropriate if you are using personal data to make significant decisions or it may cause severe harm.

Where you remain satisfied that the data is accurate, it is helpful to put a note on the system recording that the requester challenges its accuracy and explain why.

Opinions are, by their nature, subjective. It will often be sufficient to make sure that your record shows clearly that the information is an opinion and, where appropriate, whose opinion it is.

To make sure your records are clear, you may need to add a note about a mistake or a correction. This may take a variety of forms, for example, an advisory line at the top of an online article, or a printed correction area in a newspaper.

Many inaccuracies may only be minor, such as a typographical error. In those cases, it is usually reasonable to simply edit an online article to correct the inaccuracy. Most typographical errors do not involve data protection issues.

You may have published the personal data in multiple locations, such as in print and online. If so, consider what steps it is reasonable for you to take. On social media platforms it may be reasonable to encourage people who have shared the inaccurate information to help to circulate the correction.

Right to object

Individuals have the general right to object to the processing of their personal data. This right is absolute in the case of direct marketing.

You are required to clearly tell people about their right to object. You may be able to carry on processing if you have a compelling reason to do so.

If you are deciding whether you have compelling legitimate grounds which override the interests of an individual, it will help you to consider the reasons why an individual has objected to the processing and balance their interests, including any harm against your own legitimate interests or a third party's (see [What does "in the public interest" mean?](#)).

If you have no grounds to refuse the objection, stop processing the personal data. This may mean that you need to erase the personal data but this is not always appropriate. For example, you may need to retain the data for other purposes.

If you do decide to refuse an objection, you need to reply to the individual to tell them, explain your reasons, and inform them of their right to complain to the ICO and the courts.

Right to erasure

Individuals have the general right to have their personal data erased in certain circumstances, including if you:

- have processed the personal data unlawfully (see [What does it mean to process personal data lawfully?](#));
- are relying on the consent lawful basis and consent is withdrawn; or
- are relying on the legitimate interests lawful basis, the individual objects and there is no overriding legitimate interest to continue.

You need to give particular weight to any request for erasure if you are processing data based upon consent given by a child, especially any processing on the internet.

If you do erase personal data in response to an erasure request, you need to tell other organisations or individuals about the erasure if:

- it has been disclosed to others; or
- the personal data has been made public (for example on social networks, forums or websites).

Consider whether it is possible or proportionate to contact the recipients of the personal data. If asked, tell the individual making the request who you disclosed their personal data to.

Where personal data has been made public online, take reasonable steps to inform other controllers who are processing the personal data to erase any links, copies or replication of that data.

If compliance with these requirements is incompatible with journalism, the special purposes exemption can protect you, where necessary. In addition, the right to erasure does not apply if the processing is necessary to exercise the right to freedom of expression and information. In practice, your considerations are likely to be similar to those for the special purposes exemption when balancing public interest considerations (see [What does "in the public interest" mean?](#)).

There is a strong, general public interest in the preservation of news archives, which contribute significantly to the public's access to information about past events and contemporary history (see [Why is journalism important?](#)). This is generally a weighty factor in favour of not erasing personal data from news archives. It may be proportionate to rectify inaccurate or incomplete information in a news archive from time to time (see [Right to rectification](#)).

The extent to which material is amplified online may be a relevant factor to consider. This is why search engines may be required to remove links to material, even if it is lawful for the material itself to remain available online. (see [Google Spain SL, Google Inc v AEPD \(2014\)](#)).

Key legal provisions

[UK GDPR article 12](#) – requirements about providing information to individuals

[UK GDPR article 15](#) – right of access

[UK GDPR article 16](#) – right to rectification

[UK GDPR article 17](#) – right to erasure (or right to be forgotten)

[UK GDPR article 18](#) – right to restrict processing

[UK GDPR article 19](#) – requirement for controllers to notify recipients of personal data when personal data is rectified, erased or restricted

[UK GDPR article 21](#) – right to object

Disputes and enforcement

At a glance

- If someone has concerns about your handling of personal data, it helps to save the time and resources of all parties if you are able to resolve the matter directly with the individual in the first instance.
- If a complaint is made to the ICO, we will consider whether it is likely that there has been a breach of data protection and we may ask you to take steps to put things right.
- We exercise our enforcement powers, where necessary, in a proportionate way and the DPA 2018 significantly restricts their use to protect processing for the special purposes, offering additional protection for journalism.
- There are a number of criminal offences under the DPA 2018. However, there are public interest defences available for some of these. This includes a specific defence to protect journalism, where the person acted with a view to the publication of journalistic material and in the reasonable belief that publication would be in the public interest.
- The ICO may offer assistance to claimants in cases of substantial public importance.
- In certain circumstances you can apply for a stay to legal proceedings. This prevents data protection being used to block publication.

In more detail

- [How does the ICO handle complaints?](#)
- [How does the ICO enforce compliance with data protection law?](#)
- [What criminal offences are there and what are the most relevant defences?](#)
- [How may the ICO pursue criminal offences?](#)
- [What happens if an individual complains to a court?](#)

How does the ICO handle complaints?

In the first instance, we expect individuals with concerns about the handling of personal data to complain to the organisation concerned. To support this process, as part of our Your Data Matters series, we have published separate [guidance to help individuals to complain to media organisations](#) in line with the DPA 2018.

If an individual complains to you about how you have processed their personal data, review what has happened and consider carefully whether you

are able to resolve the issue at this stage. This can help to save the time and resources of all parties.

If a complaint is made to us, we may ask you to provide more information to help us to investigate. For example, if you are relying on the special purposes exemption, we may ask you to provide any records about your decision.

We will provide an opinion on whether data protection law has been broken and where necessary, we may ask you to take steps to put matters right. We may also highlight where improvements are required and ask you to take action to make your processes stronger for the future.

We will consult with industry bodies, wherever appropriate, and seek to work with them where our roles overlap. For example, compliance with an industry code of practice may be a relevant factor in our decision as to whether the special purposes exemption applies.

If a breach is serious enough or we consider that informal resolution will not be possible, we may take formal enforcement action. However, there are significant restrictions on our powers to make sure that the public interest in journalism is protected.

How does the ICO enforce compliance with data protection law?

Generally, the ICO has powers to take formal enforcement action for breaches of data protection law. These include powers to issue enforcement, information, assessment or penalty notices. We may also pursue criminal prosecutions.

However, in recognition of the importance of the public interest in freedom of expression, our enforcement powers are significantly more restricted in cases involving journalism or the other special purposes. The restrictions imposed on the use of our powers are intended to reconcile freedom of expression and privacy as necessary. Enforcement provisions are either necessary to enable the ICO to pursue investigations or are limited to breaches of substantial public interest.

In any event, we will always carefully consider the potential impact on freedom of expression before deciding to take any action in cases involving the special purposes. Any action we take will be targeted and proportionate. We are more likely to consider action in cases where there is, for example:

- a risk of significant damage or distress;

- poor accountability (see [Be able to demonstrate your compliance](#)), including attitude or conduct suggesting an intentional, willful or negligent approach; or
- a pattern of poor compliance over time.

More details about our enforcement powers generally, and the way in which we use them are in our [Regulatory Action Policy](#).

Enforcement notice

If we believe the breach is of substantial public importance, we can serve an enforcement notice. This requires you to take steps to comply if certain conditions are met (subject to a right of appeal to a tribunal). However, we cannot prevent publication, and there are significant procedural safeguards to protect journalism.

To serve an enforcement notice, we must make a written finding, and then appeal to the court for permission.

We must make a written finding that personal data is:

- not being processed only for the special purposes; or
- not being processed with a view to the publication by a person of special purposes material which has not previously been published by the controller.

There is an important restriction so that we can only take this action where personal data is being processed for another purpose, as well as journalism. We cannot take this action if the processing is only for the special purposes.

We must provide written notice of the finding to you containing details of the right to appeal. Our finding will not take effect until either:

- the appeal period ends without an appeal being made; or
- an appeal is made and decided (or otherwise ended), including any subsequent appeals, and the appeal period ends without an appeal being made.

After the written finding stage, we can then apply to the court for permission to serve an enforcement notice. The court must be satisfied that we have reason to suspect a breach of substantial public importance. Unless the case is urgent, you will be given notice of the request to the court. Generally, you will also be given the chance to defend the application.

Information notice

We may serve an information notice if we reasonably require information to help us with our investigations.

To serve an information notice, a written finding must take effect (as above), or we must have reasonable grounds for suspecting that a written finding could be made and require the information for that purpose.

We may serve an information notice, if necessary, to gather information to support our review of processing for the purposes of journalism as required under section 178 of the DPA 2018. This type of notice states our opinion that the information is needed for the review and the reasons why.

In these circumstances, the usual time for compliance does not apply. However, we cannot require you to provide information until 24 hours after we give the notice.

Assessment notice

We can only provide an assessment notice to review processing of personal for journalism in accordance with the review requirement under section 178 of the DPA 2018. An assessment notice may, for example, require you to give us access to premises and specified documentation and equipment.

The assessment notice must state that, in the Commissioner's opinion, it is necessary to comply with the notice in order to review journalism processing under section 178 of the DPA 2018. It must also explain why this is necessary.

The usual time for compliance does not apply. However, we cannot require you to comply with the requirement until seven days after we give the notice.

A written finding must take effect (as above) before we may give an assessment notice for this purpose.

Penalty notice

The ICO has the power to issue penalty notices, which may impose fines. To serve a penalty notice, a written finding must take effect (as above) and a court must also give permission.

The court must be satisfied that we have reason to suspect a breach of substantial public importance. Unless the case is urgent, you will be given

notice of the request to the court. Generally, you will also be given the chance to defend the application.

What criminal offences are there and what are the most relevant defences?

Criminal offences

There are a number of specific criminal offences under the DPA 2018. We have not set them all out here, so you should refer to the legislation for full details.

For example, it is an offence for a person to knowingly or recklessly:

- obtain or disclose personal data without the controller's consent; procure the disclosure of personal data to another person without the controller's consent; or after obtaining personal data, to retain it without the consent of the person who was the controller when it was obtained;
- re-identify information that is de-identified personal data without the consent of the controller; or
- process personal data that is reidentified information without the consent of the controller responsible for the reidentification and in circumstances in which the reidentification was an offence.

It is an offence for a person to sell, or offer to sell, personal data that has been, or will be, obtained unlawfully.

Defences

For the offences set out above, apart from those concerning selling personal data, it is a direct defence if the person charged can prove that there was a public interest justification in the circumstances, or that the person charged acted:

- for the special purposes;
- with a view to the publication by a person of any journalistic, academic, artistic or literary material; and
- in the reasonable belief that there was a public interest justification in the particular circumstances.

We will also consider any other potentially relevant defence under the DPA 2018.

How may the ICO pursue criminal offences?

We will only bring prosecutions when we consider it is in the public interest to do so, and we will always assess the public interest carefully, taking into account where appropriate:

- relevant ICO policies as set out in our [Prosecution Policy Statement](#);
- [the Code of Practice for Victims of Crime](#);
- [the Code for Crown Prosecutors](#); and
- the Crown Prosecution Service (CPS) guidance for [Assessing the Public Interest in Cases Affecting the Media](#).

The ICO has powers of entry and inspection. A judge may grant a warrant to the ICO if they are satisfied that:

- there has been non-compliance by a controller or processor (failures as described in section 149(2) of the DPA 2018); or
- an offence under the DPA 2018 has been or is being committed.

A judge must also be satisfied that there are reasonable grounds for suspecting that evidence of the failure or the commission of the offence is to be found on particular premises.

A judge must not issue a warrant regarding personal data processed for the special purposes unless a determination under section 174 of the DPA 2018 has taken effect (see above).

What happens if an individual complains to a court?

You may be able to reach an agreement with the individual to resolve the complaint (eg through arbitration). This can save time and resources. If you cannot reach agreement, individuals are entitled to take their case to court to:

- enforce their rights under data protection law if they believe they have been breached;
- claim compensation for any damage caused by any organisation if they have broken data protection law, including any distress the individual may have suffered; or
- a combination of the two.

The UK GDPR gives individuals a right to claim compensation from an organisation if they have suffered damage because of a breach in data protection law. This includes both “material damage” (eg the individual has lost money) or “non-material damage” (eg damage to reputation or distress).

ICO assistance for claimants

Any individual who is a party or prospective party to court claims in relation to journalism can ask the ICO for assistance.

We can only provide assistance if we think the case involves a matter of substantial public importance. This is likely to be the case where:

- there has been (or could be) a serious infringement causing substantial damage or distress; or
- the outcome of the case might significantly affect the interpretation of data protection law or other laws.

The assistance that we may provide includes:

- paying the applicant's costs; or
- indemnifying the applicant against their liability to pay costs, expenses or damages.

Stay to proceedings

The DPA 2018 includes a provision that may allow you to prevent legal proceedings taking place. This is intended to protect freedom of expression and avoid data protection law being used to block publication.

The court must stay the proceedings (or, in Scotland, sist the proceedings) if you claim that, or it appears to the court, that the personal data concerned:

- is being processed only for journalism (or one of the other special purposes);
- is being used with a view to the publication by anyone of special purposes material; and
- the personal data has not previously been published by the controller.

You should note that the provision applies when personal data is being processed only for journalism, in contrast to the special purpose exemption that can apply even when other purposes are involved, such as campaigning. If you wish to rely on the statutory stay, you need to be satisfied that you are only using the personal data for journalism, rather than any other purpose.

When considering whether personal data has been previously published by the controller, publication in the immediately preceding 24 hours is ignored.

This stay remains in place until:

- a written determination by the ICO takes effect (see [How does the ICO enforce compliance with data protection law?](#)); or
- the claim is withdrawn.

Key legal provisions

[DPA 2018 section 167](#) – compliance orders

[DPA 2018 section 168](#) – compensation for contravention of the GDPR

[DPA 2018 section 143](#) – Information notices: restrictions

[DPA 2018 section 152](#) – Enforcement notices: restrictions

[DPA 2018 section 156](#) – Penalty notices: restrictions

[DPA 2018 section 170 -173](#) – criminal offences

[DPA 2018 section 174](#) – the special purposes

[DPA 2018 section 175](#) – provision of assistance in special purposes proceedings

[DPA 2018 section 176](#) – staying special purposes proceedings

[DPA 2018 section 177](#) – guidance about how to seek redress against media organisations

[DPA 2018 section 178](#) – review of processing of personal data for the purposes of journalism

[DPA 2018 Schedule 15](#) – powers of entry and inspection

[DPA 2018 Schedule 17](#) – review of processing of personal data for the purposes of journalism

Annex 1 – UK GDPR provisions covered by the special purposes exemption

[Schedule 2 Part 5 paragraph 26\(9\)](#) of the DPA 2018 lists the parts of the UK GDPR that journalists can be exempted from. These are:

- Article 5(1)(a) to (e) – the UK GDPR’s principles, apart from the security and accountability principles.
- Article 6 – requirement to satisfy a lawful basis for processing.
- Article 7 – conditions for consent.
- Article 8(1) and (2) – conditions for children’s consent.
- Article 9 – rules relating to special category data.
- Article 10 – rules relating to criminal offence data.
- Article 11(2) – specific rules regarding informing individuals when their personal data has been anonymised.
- Article 13(1) to (3) – requirement to provide privacy information to individuals when you have collected data directly from the data subject.
- Article 14(1) to (4) – requirement to provide privacy information to individuals when you have not collected data directly from the data subject.
- Article 15(1) to (3) – right of access.
- Article 16 – right to have inaccurate or incomplete data rectified.
- Article 17(1) and (2) – right to erasure (the right to be forgotten).
- Article 18(1)(a), (b) and (d) – right to restrict processing.
- Article 19 – requirement to inform third parties to whom data has been disclosed of a rectification, erasure or restriction.
- Article 20(1) and (2) – right to data portability.
- Article 21(1) – right to object to processing (except for direct marketing).
- Article 34(1) and (4) – requirement to inform data subjects of a data security breach.
- Article 36 – requirement to consult the ICO prior to any high-risk processing.
- Article 44 – general principles for international transfers.