Second consultation on the ICO's draft Data protection and journalism code of practice

Start date: 9 September 2022
End date: 4 November 2022

Information Commissioner's Office

Introduction

We are seeking feedback on a revised version of our draft Data protection and journalism code of practice. This follows your feedback to a written public consultation that ran for 12 weeks from September 2021 and workshops.

You can read our summary of the feedback and individual responses on the ICO website – redacted in line with our privacy statement.

This is a draft of a statutory code of practice under section 124 of the Data Protection Act 2018 (DPA 2018). It will help those using personal data for journalism understand their legal obligations and comply with good practice.

The revised draft code is now out for further public consultation. Although the focus of this public consultation is the draft code, we would also welcome your views on the associated documents below. Please note that these documents do not form part of the statutory code.

- supporting reference notes for the code
- the code 'at a glance'
- 10 data protection tips for day-to-day journalism
- updated impact assessment

The public consultation will remain open until 4 November 2022.

Download this document and email to: journalismcode@ico.org.uk

Print off this document and post to:

Journalism Code of Practice
Regulatory Assurance
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

If you have any general queries about the consultation, please email us at journalismcode@ico.org.uk.

Privacy statement

For this consultation, we will publish all responses except for those where respondents are acting in a private capacity (eg a member of the public). We will remove email addresses and telephone numbers from all responses.

For more information about what we do with personal data please see our privacy notice.

Questions

When commenting, please bear in mind that the code does not aim to cover all of the legislation. Supporting reference notes contain key legal provisions, case law examples, and further reading.

Please also bear in mind that in line with your feedback, we plan to develop additional supporting resources, including guidance for smaller organisations and individuals.

Please let us know if you have any other comments about the code or associated documents in the general comment box at the end.

Section one: The statutory code

Guardian News and Media Limited's ("**GNM**") responses to the Second ICO Consultation on the revised draft data protection and journalism code of practice (the "**second draft Code**") are in blue for ease of reference.

Q1 Overall, to what extent do you agree that the revised code sufficiently reflects the feedback provided to the ICO?

To inform your answer please ensure you have read the consultation summary report. This sets out the changes we made in response to your feedback.

□ Strongly agree
□ Agree
□ Neither agree nor disagree
X □ Disagree
□ Strongly disagree

Q2 If you consider that the code does not sufficiently deal with the feedback, please specifically explain why and what you think we should change.

GNM welcomes the opportunity to respond to the ICO's consultation on the second draft Code. GNM responded to the first round of consultation on the draft code and while it appreciates the steps now taken to address the feedback from the first consultation, it still stands behind the substance of the points it made on that occasion. The second draft Code is shorter, less complex and written in simpler English that is easier for a layperson to understand. The adoption of the "*must*", "*should*" and "*could*" language helps differentiate between legal obligations and good practice in a way that should be of practical use. The journalism exemption is given a more central role in the second draft Code which GNM welcomes.

However, GNM considers that the second draft Code downplays the significance of legitimate interests as a lawful basis for processing personal data in the context of journalism. We believe that more work is needed to explain to journalists that a lot of their everyday use of data will be lawful on this basis. We go into more detail on this in point 1 in response to Q4.

GNM also considers that the second draft Code has some significant omissions that mean that it still does not provide a comprehensive guide for journalists using personal data for journalism. For example, it does not:

(i) provide details of the detailed defences that may be used by journalists to defend their use of data, often only referring journalists back to specific provisions of the legislation and in some cases not even summarising those. For example, there are a number of specific defences for the use of special category data and criminal offence data set out within the Data Protection Act 2018 ("**DPA 2018**"). The second draft Code is not comprehensive and only refers to those that it considers journalists will use most frequently without identifying or listing any of the others. It is possible that some of the others may be relevant in particular circumstances but without them being included in the second draft Code it is likely that most lay people will forget about them. The reference notes include details of the sections where the relevant statutory defences can be found but without links to the legislation and/or summaries of each of the provisions most lay people will find it difficult to locate these in either the UK General Data Protection Regulation ("**UK GDPR**") or the DPA 2018.

(ii) set out the criminal offences that may be committed under the DPA 2018 or the defences that may be available in response to those defences.

(iii) give guidance to journalists about how they and/or other individuals may use data protection law to obtain information in connection with their journalism. For example, journalists may be able to ask data subjects to make subject access requests and those data subjects may be able to provide journalists with the data disclosed as a result. It would be a missed opportunity for the second draft Code not to refer to ways such as this in which the DPA 2018 can be utilised for journalism.

(iv) provide details of how the statutory stay mechanism will work, perhaps by reference to *Steinmetz v Global Witness*.

GNM also notes that although much of its feedback has been incorporated in the second draft Code, some key aspects have not been adequately reflected. The second draft Code remains longer than necessary (60 pages), repetitive and overly-focussed on policies and record keeping that simply do not reflect the realities of modern journalism.

Modern journalism is a 24-hour operation, spanning multiple time zones, across a range of territories with different legal regimes and often with tangible personal risks to journalists. That working environment requires quick decisions to be made in response to developing situations so that news can be reported accurately and in a timely manner. Although the second draft Code is supposed to be of practical use to its stated audience, journalists, it does not give enough practical advice on the applicability of the exemption that would be useful for them.

GNM is a member of the Media Lawyers' Association and endorses its general submissions. We also attach copies of the second draft Code, the reference notes and the top 10 tips with suggested amendments and notes.

In terms of specific comments:

1. **Regulatory**. GNM is concerned that the second draft Code still does not sufficiently take into account the very real dangers of over regulation of areas in which there is already considerable statutory and case law. The law has been developed over many years, seeking to strike a careful balance between the rights of individuals with those of freedom of expression, the right to fair trial, freedom of religion and the right to

life. Placing a new section at the beginning of the document called "*Complaints, enforcement and investigations*" could be seen as attempting to regulate press conduct and standards. This section should logically be presented at the end of the document as it covers situations where the code has not been complied with. There is little reference in the second draft Code to the way in which the ICO and media regulators are likely to interact or what will happen when both industry codes and the final version of this ICO code are engaged (since there is significant overlap between them it is likely this will happen frequently). Considering how accuracy is a matter referred to in all of the media codes there should be some reference as to how the ICO is intending to deal with complaints about accuracy of data which are already being or have been examined by media regulators. There is a reference to the ICO's Regulatory Action Policy but this does not give practical guidance on these topics.

2. **Public interest**. GNM considers that the definition of the public interest (1.24-1.35) still does not give enough recognition to the value in public interest in freedom of expression and information in itself, in addition to any specific factors relevant to the circumstances. The approach taken in the second draft Code is narrow and focuses on cases that are likely to involve misconduct/wrongdoing. However, there are wider public interests that need to be recognised to ensure that the exemption truly protects the whole spectrum of journalism. For example, the public interest extends from an in-depth investigation to a sports interview, to a feature whose purpose is to amuse a reader. All of this varied content is produced in the public interest and contributes to the business of a news organisation. The second draft Code suggests "*reporting on local events*" may be an area in which it would be more difficult to establish a public interest, again implying a narrow approach to the definition of the public interest. This may be accidental, but it should be amended in the revised version.

3. **Policies and record keeping: "Take steps to protect personal data"**.

    a. The second draft Code is still not sufficiently clear that most accountability requirements are themselves dependent on the operation of the data principles, which may not apply if a journalist can apply the special purposes exemption in respect to those principles. If the principles do not apply because of the exemption, then there is no need to demonstrate compliance in respect of those principles. This is fundamental to the operation of data protection law in relation to journalism and needs to be reflected. The summary at the front of section 2 gives the impression that the exemption only applies in relation to the usual requirement to consult the ICO if a Data Protection Impact Assessment identifies a high risk. It does not explain that journalists cannot be required to comply with accountability requirements for provisions of data protection law if they have disapplied those provisions by virtue of the exemption. This also needs to be referred to on p10, where it states "*You **must** always comply with the key data protection principles of accountability and security*" (emphasis added). Again, this misleads the reader, as accountability obligations may also be subject to exemptions or may be fulfilled by complying with specific data protection principles.

    b. The second draft Code still frequently recommends that journalists should have data protection-focussed policies in place and keep records, particularly in section 2. GNM considers their need and significance continue to be overstated. Even if expressed as a 'should' rather than a 'must', references to specific records/documents in this context are likely to create a *de facto* expected standard that does not necessarily reflect the reality of the law as it applies to a modern-day newsroom. As set out in GNM's first response,

devising and implementing specific policies applicable to all of the various fast-moving situations that present themselves and producing specific audit trails is simply not realistic. It will either restrict and slow down the production of news or create standards which in practice cannot be fulfilled. There is a high risk that creating unrealistic expectations in a statutory document published by the ICO will lead to them being used against news organisations by those seeking to use any and all legal routes to undermine their journalistic output.

c. At various points the second draft Code refers to the need for written contracts (see, for instance, 3.18, p51 and 11.6). Written agreements are only mandatory under data protection law where a third party is acting as a processor. The second draft Code acknowledges that freelance photographers and journalists are likely to be acting as controllers in their own right (see 11.3), and therefore there is not an absolute need for a written agreement. In the journalism context the use of processors is likely to be relatively limited - for example, to when a third party is being used for the provision of software. It would be useful if the second draft Code made this clear and perhaps gave a practical example of a third-party processor in paragraphs 3.16-3.18 or 11.5/11.6. Paragraphs 3.16-3.18 should also use the language of "processor" given that its meaning is explained in section 11.

d. 11.4 of the second draft Code states: "*If acting as a joint controller, you **must** have an agreement with the other party or parties that sets out your respective responsibilities, particularly about transparency and individual rights. You must **make** this information available to people*" (emphasis added). GNM considers this overstates the requirements of data protection law and that "*agreement*' should be replaced with "*means of arrangement*" to avoid giving the impression a written contract is needed, when responsibilities can be transparently allocated in other ways. The second draft Code should also make clear that in certain circumstances the journalism exemption may apply to data sharing. For example, it could apply to data sharing between media organisations/freelancers collaborating on an investigation by exempting them from the obligation to make available "*the essence of the arrangement*" between one another. If media organisations were obliged to provide this information to third parties it would be likely to undermine their journalism. The availability of the exemption should also be made clear to the intended audience, journalists, at 11.7 where it states: "*When sharing personal data between controllers, you must comply with the data protection principles. In particular, you must share personal data lawfully, fairly and transparently*".

e. The 'At a glance' summary of what the accountability principle means for journalists states *"you must take steps to protect personal data and be able to demonstrate you comply"* (p17). Likewise, the word "*demonstrate*" is used in relation to the journalism exemption as the draft states *"you must be able to demonstrate your belief was reasonable"* (1.17 and 1.23). As referred to in GNM's first consultation response, the word "*demonstrate*" may be used to imply that records have to be kept with the expectation that they must be shown at some future point. GNM would recommend the word demonstrate is replaced with the word **show**.

4. **Repetitive.** The second draft Code remains repetitive. To take an example, the section "*what does "reasonable belief" mean?"* (1.16-1.22) refers twice to the fact a decision must be objective and twice to the fact that a decision can be delegated. It

also makes three very similar points about the ICO/judges: (i) "*Nor do you need to arrive at the same conclusion as the ICO or a judge*"; (ii) "*it is not the role of the ICO or a judge to disregard your decision lightly or substitute their own belief in place of yours*"; and (iii) "*It is also not the role of the ICO or a judge to disregard the important editorial discretion that you have to decide how to edit, present and convey the information*". There is a similar level of repetition throughout the second draft Code. The repetition may be intended to ensure that the intended reader, journalists, are reassured that they have discretion in how they make their decisions. The effect, however, is to bloat the second draft Code without providing any additional clarity for the reader.

5. **Privacy law**. As stated in our last response, references to "*privacy*" need to be carefully considered given the second draft Code is a data protection code and there are significant differences between privacy and data protection law. It may be helpful for the second draft Code to flag the difference in threshold between the applicability of data protection law versus privacy law, particularly because information in which there is a reasonable expectation of privacy is protected under Article 8 of the ECHR and must therefore be balanced with Article 10 rights protecting freedom of expression and information. Personal data does not necessarily benefit from these same protections. The second draft Code should also make it clear that, even in cases where there is no reasonable expectation of privacy, there may still be data protection implications.

6. **Use no more personal data than you need**. The explanation of using "*adequate*", "*relevant*" and "*limited*" data (pp46-47) seems to be in reference to a single specific story. As noted in GNM's previous response, data-led investigations can involve terabytes of data and it is not clear, and may not be clear for some time, which data is particularly relevant for a particular story. The second draft Code should make it clear that the special purposes exemption gives sufficient latitude for journalists to investigate and identify stories in this context.

7. **Practical examples**. There is an absence of practical examples in the second draft Code. GNM considers that it would be helpful if the second draft Code set out examples to illustrate the breadth of circumstances in which the journalism exemption may be relied on. Although the exemption is referred to in the 'At a glance' sections at the beginning of each section, it would be helpful to set out specific practical examples of how it could be applied to the requirements set out in each section of the second draft Code. GNM would suggest that the ICO speaks to media organisations to develop practical and diverse examples that relate to a wide variety of stories published by news organisations.

Q3 To what extent do you agree that the code provides useful guidance on the use of personal data for journalism?

□ Strongly agree
□ Agree
X □ Neither agree nor disagree
□ Disagree
□ Strongly disagree

Q4 If you do not think it is useful, please explain why specifically and what you think we should change.

1. **Journalism exemption and legitimate interests.**

   a. GNM welcomes the clearer explanation of the special purposes exemption and the fact that it has its own section. However, it may not be clear to journalists that, in many cases, they will not need to rely on the exemption for their activities, as they will be processing personal data lawfully on the basis of their own legitimate interests (and/or, in some circumstances, with the consent of the data subject). The second draft Code explains legitimate interests in the section on using personal data lawfully; that is approximately halfway through the draft (see 4.8-4.13). It gives the impression that legitimate interests should only be relied upon for routine journalism with "*minimal privacy impacts*". GNM considers the applicability of this lawful basis for processing to be much wider, particularly given the special public interest in freedom of expression and information. GNM suggests the second draft Code is revised to better explain the significance of legitimate interests to journalists, so that they can understand that it may be relied upon as a lawful basis for processing. At the very minimum, legitimate interests needs to be sign-posted for journalists in the journalism exemption section, so that they do not get the wrong impression that the default position should be trying to apply the exemption.

   b. In terms of where the section on the exemption sits within the second draft Code, GNM would suggest that it may make sense to first introduce the usual requirements of data protection law for a data controller, before describing how the exemption may disapply some of the requirements.

   c. There is an error in law regarding how the journalism exemption is explained. The second draft Code states "*The exemption can cover all the personal data you use for journalism as long as you have the intention or hope of publishing it*". This suggests that, in order to rely on the exemption, a journalist needs to have the intention of publishing the specific data that it is using. However, the exemption can cover the use of personal data for journalism if it is being carried out "*with a view to the publication by a person of journalistic, academic, artistic or literary material*". There is no requirement you have to be considering publishing the specific data that you are using. This is illustrated by considering the example of a phone number - your processing of that number should be protected by the journalistic exemption regardless of the fact you never intend to publish it. GNM considers the second draft Code should be amended to reflect that. We believe it would be a significant restriction on freedom of expression if journalists were given the impression that they needed to be able to justify that they were considering publishing all of the personal data they were processing prior to publication.

   d. The second draft Code summarises elements of the journalism exemption in plain English, using language that could be interpreted differently to the statutory tests. For example, acting with a "*view to publication*" is re-framed as acting "*with the intention or hope of publishing journalistic material*". This is unhelpful as the language could be interpreted differently to the statute. Further, the incompatibility provision is expressed in a number of different ways, including with the following reference in 1.38: "*In some cases, it will be obvious that you cannot carry out your journalistic activity and comply with data protection at the same time*". GNM considers these summaries overstate the requirements of the journalism exemption. In the case of *Campbell v MGN Ltd* [2003] QB 633 (CA), the Court of Appeal

summarised the test as one of practicality. GNM believes the code should adopt the language of "*reasonable practicability*" so that it reflects the relevant case law. The second draft Code should make clear to journalists that if it is not "*reasonably practicable*" to comply with an element of data protection law when using data for journalism, then it can be waived if the other elements of the exemption are satisfied.

e. Although the 'At a glance' bullet points at the beginning of sections 2-12 contain a brief summary of how the journalism exemption may apply to it, almost no practical guidance is provided within the sections as to the applicability of the exemption. This lack of practical guidance within sections 2-12 of the second draft Code means its practical relevance to journalists will inevitably be limited.

2. **Compulsory obligations**. GNM welcomes the use of the words "*must*", "*should*" and "*could*" in the second draft Code. However, it is not always clear that the journalism exemption can exempt journalists from obligations expressed as "**must**" obligations. We would suggest that the second draft Code is amended to distinguish between "*must unless an exemption applies*" and "*must in all circumstances (i.e. the data security obligations)*". For example, where the journalism exemption cannot be applied to a "*must*" obligation, the word "*could*" is underlined and a relevant explanatory key provided at the beginning in the section entitled "*How will this code help us*" (p5).

3. **Complaints, enforcement and investigations**. There is a new section at the beginning of the second draft Code entitled "*Complaints, enforcement and investigations*". As referred to above, GNM is concerned that this section could be used to treat the ICO as a media regulator. In addition to those concerns, this section is confusing as, although it primarily relates to complaints made to the ICO, it also touches on privacy information and how to deal with complaints directly.

a. Privacy information is already covered in section 6, meaning that the complaints section is repetitive. Section 6 is also clear that the journalism exemption may be used to disapply this provision, yet this is omitted from the complaints section. It is confusing for journalists if one of the first things they are faced with in the second draft Code is the unqualified statement that "*You must tell people about their right to complain when you provide privacy information*" without any explanation of what privacy information is or any acknowledgement that an exemption can remove this usual requirement.

b. The second bullet says "*You must also tell people how to contact your Data Protection officer (DPO), if you have one*". This gives the impression that (where an organisation has a DPO) journalists should be telling individual subjects of stories how to contact the DPO on a day-to-day basis, for example when speaking to the subject of an interview. However, such onerous obligations are not compatible with journalism. Media organisations have privacy policies online which tell individuals how they can contact its DPO or relevant data privacy contact point. For example, GNM's privacy policy states: "*If you would like to exercise any of your rights specified above, please email dataprotection@theguardian.com or write to the Data Protection Officer at Guardian News & Media Limited, Kings Place, 90 York Way, London N1 9GU.*" The second draft Code should make it clear that it is sufficient to provide privacy information in this form.

c. The references to how to deal with complaints directly appears to have some overlap with section 12 on helping people to use their rights. GNM would

suggest that complaints should be dealt with in one place in the second draft Code. The best place for this would be in the context of helping people to use their rights as that is how data protection complaints tend to be framed.

4. **Take steps to protect personal data**. The section on accountability has been renamed "*Take steps to protect personal data*". GNM welcomes the move away from the word "*accountability*" given it has different meanings to different people. However, the new title is confusing as it gives the impression that this section relates to data security, which is not the case. GNM suggests it is renamed as "*Be responsible for your use of personal data*". GNM also notes that a lot of this section seems to be general guidance for organisations about using data that is not tailored to journalism. Such material is already available on the ICO website in the Guide to Data Protection and does not need to be replicated here. GNM has a DPO to monitor the organisation's overall compliance with the UK GDPR, advise on its data privacy obligations (accountability obligations), conduct audits, provide training, respond to data incidents and breaches, and respond to data subject rights requests. This section looks more appropriate for data privacy colleagues than for the intended audience of the second draft Code, journalists. GNM believes that the non-journalism specific guidance should be removed from the second draft Code and replaced with links to the generic guidance. This would both reduce the length of the second draft Code and provide clarity by ensuring that it is a practical document tailored to the specifics of journalism.

5. **Allegations of criminal activity**. GNM recognises that, as reflected in the second draft Code, the "*alleged commission of offences by the data subject*" is subject to specific protections under the DPA 2018/UK GDPR. However, "*allegations of criminal activity*" are singled out as an area where journalists must consider a person's reasonable expectation of privacy, reflecting the recent Supreme Court case of *Bloomberg LP v ZXC* [2022] UKSC 5 (4.47-4.55). This section essentially re-states the legal principles of misuse of private information established in *ZXC*. There is a difference between privacy law and data protection and GNM does not consider it appropriate for the second draft Code - a statutory code on data protection - to go into this level of detail on privacy law. It is also not clear why "*allegations of criminal activity*" are singled out as there are many other areas where individuals would generally be able to establish a reasonable expectation of privacy (for example, in relation to their sex life or the contents of private correspondence) and these are not considered in detail - but rather would just need to be considered within the section on reasonable expectations (5.4-5.9).

6. **Accuracy**. The section on accuracy contains a section called 'sources of information' which distinguishes between "*primary*", "*generally reliable*" and "*secondary sources*". There is then some general guidance on how one may consider the reliability of such sources. This seems to be straying into areas of editorial discretion. We would suggest that the section is pared back.

Q5 Is there anything else you would like to tell us about the code?

See above answers to Q2 and Q4.

Section two: Supporting documents

Q6 To what extent do you agree that the supporting reference notes are helpful?

□ Strongly agree

□ Agree
X □ Neither agree nor disagree
□ Disagree
□ Strongly disagree

Q7 To what extent do you agree that the code 'at a glance' is helpful?

□ Strongly agree
□ Agree
□ Neither agree nor disagree
X □ Disagree
□ Strongly disagree

Q8 To what extent do you agree that the quick guide to support day-to-day journalism is helpful?

□ Strongly agree
□ Agree
X □ Neither agree nor disagree
□ Disagree
□ Strongly disagree

Q9 Is there anything else you would like to tell us about the supporting reference notes, the code 'at a glance',quick guide for day-to-day journalism or impact assessment?

Reference notes:

1. GNM suggests that for ease of reference hyperlinks are provided to all of the sections of the DPA 2018 referred to within the reference notes.

2. The reference notes highlight a number of privacy cases. Although there are similarities between data protection law and privacy law, it would also be helpful at the beginning of the reference notes to make it clear that there are significant differences between the two and that there is relatively little case law in relation to data protection. Some of the cases contained in the reference notes are first instance decisions which, as referred to in our previous response, GNM does not consider should be included given such decisions do not establish precedent and may be superseded by higher authorities.

3. No explanation is given as to how the ICO intends to keep the reference notes up to date with the latest developments in case law. This would be helpful to know given the nature of the document.

4. It would be useful to cross reference the case examples to the relevant paragraphs of the second draft Code. For example, to make clear that case examples 1-4 are relevant to 1.8-1.12. It is not always clear how specific cases fit into the second draft Code - for example case 7 (which we assume from looking at the previous draft Code is relevant to 1.19) and case 10 (which we assume from looking at the previous draft Code is relevant to 1.34).

5. Case example 12 relates to the case of *ZXC*. The header within the box states "*Criminal allegations under state investigation*". This may give the impression that the case establishes that individuals have a reasonable expectation of privacy in *allegations of criminal activity* rather than the fact of a criminal investigation. We would therefore suggest this is amended to read: "*Criminal investigations by the state*".

6. Case examples 10 and 16 re-state the same principle from the same case to illustrate two different points - "*public interest and proportionality*" and "*unwarranted intrusion*". We suggest this is amended to avoid repetition within the notes.

7. GNM considers the use of the words "*third-party*" in case example 19 to be potentially confusing - although publisher websites were 'third parties' in the context of the ECJ case, the use of the phrase could suggest something else (i.e. user-generated content) and we would suggest clearer language is used to make clear the distinction is between search engines and websites such as a news website.

8. The second draft Code no longer includes a specific reference to the ICO's decision in *Steinmetz v Global Witness*. GNM considers this should be included as a case example in the reference notes or referred to within an explanation of the statutory stay mechanism.

At a glance:

It looks like the 'At a glance' wording is the same as the bulleted text at the front of each section. Please therefore refer to the above responses in relation to the text - for example, please see point 1c in response to Q4 regarding the wording "*The exemption can cover all the personal data you use for journalism as long as you have the intention or hope of publishing it*"

Top 10 tips:

The language in this document is not always consistent with the main second draft Code. We have prepared a marked up copy of the text which seeks to address this to avoid the same thing being explained in different ways that could conflict and/or be confusing for a journalist seeking practical guidance.

The "At a glance" and "Top 10 tips" documents are both high-level summaries of the second draft Code. It is unclear whether these documents are intended to have different purposes. We would suggest that they could perhaps be combined into a single summary document.

Section three: About you

Q10 What is your name?

Gillian Phillips

Q11 If applicable, what is the name of your organisation and role?

Director of Editorial Legal Services, Guardian News and Media Limited

Q12 Are you acting: (Please select)

□ in a private capacity (eg someone providing their views as a member of the public)?
☑ in a professional capacity?
☑ on behalf of an organisation?
□ other

If other, please specify.

Q13 Are you a: (Please select most appropriate)

□ member of the public
□ citizen journalist
□ public figure (eg people who have a degree of media exposure due to their functions or commitments) or individual with a public role (eg politician, public official, business people and members of regulated professions)
☑ representative of a newspaper or magazine
□ representative of a broadcaster
□ representative of an online service other than those above
□ representative of the views and interests of data subjects
□ representative of a trade association
□ representative of a regulator
□ representative of a third sector/civil society body (eg charity, voluntary and community organisation, social enterprise or think tank)
□ freelance journalist
□ private investigator
□ photographer
□ academic
□ lawyer
□ other

If other, please specify.

Further consultation

Q14 Would you be happy for us to contact you about our work relating to the Data protection and journalism code of practice?

☑ Yes
□ No

If so, please provide the best contact details.

[redacted]

Q15 Would you be happy for us to contact you about the review of processing for journalism under section 178 of the DPA 2018?

☑ Yes
☐ No

If so, please provide the best contact details.

[redacted]

Thank you for taking the time to share your views and experience.

Information Commissioner's Office

Draft data protection and journalism code of practice

ico.
Information Commissioner's Office

Contents

NOTE: This document, like its predecessor, lacks a comprehensive index at the end of the code

About this code

At a glance

- This code contains practical guidance for organisations and people using personal data for journalism under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).
- Personal data is any information about a living and identifiable person, that is, or will be, stored on a digital device or kept in an organised way.
- This code is mainly for media organisations and journalists.
- It will help you to comply with your legal obligations and follow good practice.
- You **must** balance freedom of expression and information with other fundamental rights in a democratic society~~, such as data protection, which is part of the broader right to privacy~~.
- This code is about data protection. It does not concern press conduct or standards in general, which are covered by industry codes. However, it may help you comply with industry codes and other privacy laws.
- This code is a statutory code of practice under the DPA 2018.
- The Information Commissioner's Office (ICO), courts and tribunals must take this code into account, where relevant.
- The ICO must review how personal data is used for journalism. This code will help us to consider this. We must also keep the code itself under review.

In more detail

Note: The paragraphs in this section and the complaints section should be numbered for ease of reference.

Who is this code for?

This code contains practical guidance for organisations and people using personal data for journalism under the UK GDPR and the DPA 2018. We may refer to this in the code as data protection law.

What does using personal data mean?

Personal data **is** any information:

- about an identifiable living person; and
- that is, or will be, stored on a computer or other digital device, or in an organised way.

It does not need to be private. Anything about a person can be personal data – even information that is public knowledge or about someone's professional life. For example, a job title.

Personal data does not need to be factual. For example, opinions about a person can be personal data.

Information is **not** personal data if it is:

- a paper record that you do not plan to put on a digital device or organised file (eg handwritten notebooks);
- information about a deceased person; or
- truly anonymous – if you can still identify someone from the details or by combining it with other information, it is personal data.

In the code, we refer to "using" personal data, which means the same as "processing" personal data. Processing is the legal description used in data protection law. Using personal data means anything that you do with it, including collecting, recording, storing, publishing, sharing or deleting it.

This code applies to organisations using personal data that operate within the UK. It also applies to organisations outside the UK that offer goods or services to people in the UK.

The code is mainly for media organisations and journalists, such as the press, broadcast media and online news outlets. This includes press agencies and freelance journalists providing stories to media organisations.

When we say 'you' in the code, we are mainly addressing the person with the main legal responsibility for complying with data protection law (eg the head of the media organisation). However, in practice, various people within an organisation have some data protection responsibilities, so this code will help anyone using personal data for journalism, including journalists.

We also recognise that journalism is not limited to media organisations or the journalists they employ. So the code also applies more broadly to other groups and people, including campaign groups or members of the public using personal data for journalism.

How will this code help us?

This code will help you to understand important parts of data protection law and think about how to apply it in practical ways. It focuses on seven key principles, which are largely flexible and based on risk. It says that you **must**:

1. take steps to protect personal data; NOTE: As referred to in the response, this title is confusing and should be renamed. We would suggest "Be responsible for your use of personal data"
2. keep it secure;
3. use it lawfully, fairly and transparently;
4. use accurate personal data;
5. use it for a specific purpose;
6. use no more than you need; and
7. only keep it for as long as you need it.

To help you to understand the law and good practice as clearly as possible, we explain in the code what you must, should or could do to comply.

- When we use the word **must** in the code, this refers to legal requirements. NOTE: The Code needs to distinguish between must obligations that may be subject to the exemption and those that are applicable in all circumstances. We would suggest that the latter must obligations are underlined and explained here
- When we use the word **should** in the code, this does not refer to a legal requirement, but what we consider is important to help you to comply effectively with the law. You **should** do this unless there is a good

reason not to. If you choose to take a different approach, you need to be able to demonstrate that your approach complies with the law.

- When we use the word **could** in the code, this refers to an option or options that you could consider to help you comply effectively. There are likely to be various other ways you could comply.

There are also Reference notes to support the code. Although not part of the code itself, these notes contain case law examples and refer to legal provisions and further reading.

How does this code take into account the special public interest in freedom of expression and information?

There is a strong public interest in a free press because it is vital to democracy. A free press can increase knowledge; inform debate; entertain and help citizens to participate in society. All forms of journalism can perform this crucial role, including local stories, entertainment news, and major investigations.

A free press is also a public watchdog that holds the powerful to account. It acts as an important check on political and other forms of power, particularly abuses of power.

Given the special role of freedom of expression and information and a free press, there is a broad exemption for those using personal data for journalism in data protection law. However, you **must** also consider this alongside other fundamental rights, including the right to privacy.

~~A degree of privacy, and limits on intrusion by the state and others with power, is needed to protect citizens' private and family life, their home and correspondence. This is fundamental to their physical, psychological and social well-being.~~

The protection of personal data ~~is an important part of the broader right to privacy. It~~ enables people to understand and exercise proportionate control over what happens to their personal data. Data protection and privacy cannot however be confused as some personal data may not be private. Private information is protected by article 8 of the European Convention on Human Rights (right to respect for private and family life, home and correspondence) and, where it is engaged, it needs to balanced with article 10 (right to freedom of expression and information).

This code explains how to apply the key principles of data protection law flexibly and proportionately when considering these fundamental rights in a journalism context. This includes practical guidance about specific provisions to protect freedom of expression and information.

This code also takes into account consultation responses from industry and representative groups about the realities of news environments, which are often fast-paced, pressured and competitive.

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

This code does not concern media conduct or journalistic values in general. It is about data protection law and good practice. Media standards 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 industry codes and is designed to complement industry guidance. Where relevant to data protection, we will take industry codes of practice into account and work with industry bodies.

NOTE: As referred to in our response, This code does not however describe what will happen when both industry codes and the ICO code are engaged (and since there is significant overlap between them it is likely that this will happen quite a lot). There is no reference here to how the ICO will treat industry regulatory decisions (except that this Code does refer to the Regulatory Action Policy (https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf) which is similarly unclear).

Complying with industry codes will also help you comply with data protection law, as well as other privacy laws.

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

This is a statutory code of practice under the DPA 2018. If someone complains about how you have used their personal data, the ICO, courts and tribunals must take this code into account once it is in force so far as it appears to be relevant.

If you do not do what this code says you should do, you will need to be able to show ~~persuade~~ the ICO or the courts that you have nevertheless complied with the law. Courts and tribunals will generally follow the guidance in codes and give weight to it unless there is a good reason not to.

How will the ICO review this code?

The ICO must keep this code under review. The ICO must review how personal data is used for journalism. This is not limited to the code, but the code will help us to consider compliance. We may also use the findings of the statutory reviews to help us update the code.

Complaints, enforcement and investigations

At a glance

- ~~You **must** tell people about their right to complain when you provide privacy information.~~
- ~~You **must** also tell people how to contact your Data protection officer (DPO), if you have one.~~ NOTE: Delete as repetitive and misleading given that no reference is made to the possibility of the exemption applying to either of these 'must' obligations. It is not the role of journalists to be telling individual subjects of stories how to contact the DPO on a day-to-day basis and it should be made clear in section 6 that information in a media organisation's privacy policy is sufficient.
- Try to resolve complaints with the complainant ~~person concerned~~ because this is likely to save you time and resources.
- If someone complains to the ICO, we can tell them whether it is likely you have complied with data protection law.
- There are several bodies who provide a complaints process about the media. We have published separate guidance to help complainants ~~people~~ consider the most appropriate way to resolve their concern.
- People also have the right to enforce their data protection rights in court or claim compensation for damages, or both.
- Courts must stay (or in Scotland, sist) legal proceedings in some cases so data protection is not used to block publication.
- Any regulatory action we take will be ~~is~~ proportionate to the risks of harm involved. We also carefully consider the potential impact on freedom of expression before taking any action.
- To protect journalism, there are significant restrictions on our powers and procedural safeguards. There are also defences to criminal offences concerning journalism and the public interest. NOTE: In order to be comprehensive for journalists, the code should set out the criminal offences associated with the misuse of data and the defences available to journalists in respect of them.

In more detail

- How should we deal with complaints about how we use personal data?
- What happens if someone complains to the ICO or a court?
- What is the ICO's approach to enforcement or investigations and how is journalism protected?

How should we deal with complaints about how we use personal data?

You **must** give people clear information about their rights and help them to use them. This includes details of their right to complain to the ICO and the courts (See Use personal data transparently).

If you have a DPO (see Take steps to protect personal data), you **must** make it clear how to contact them.

You **could** consider an online complaints form or publish a complaints policy to make it easier for people to contact you. If someone complains, you **should** consider it carefully. If you are able to resolve it directly, this may save you time and resources.

What happens if someone complains to the ICO or a court?

Before complaining to the ICO, we expect people to raise their concerns with you or your organisation first. If we receive a complaint, we will consider whether it is likely you or your organisation have complied with data protection law and we may ask you to take certain steps to comply if we think you have not. ~~take steps to put things right~~.

Our role is about data protection rather than general press standards. We recognise that there are a number of industry codes of practice relating to both print, on-line and broadcast journalists, which may overlap with some of the matters in this document, for example accuracy, and we encourage anyone with concerns in areas of overlap to raise them with the appropriate internal or external standards body, where one exists. However, where there is overlap, we will work constructively with other regulators and industry bodies to resolve issues effectively and efficiently in line with our Regulatory action policy. NOTE: The Regulatory Action Policy (https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf) does not really give guidance on what will happen if there are industry regulators. According to this it appears that the ICO will select the relevant regulator on the basis of the seriousness of the breach (p10). It is not clear however how that will affect the media regulator. It would be useful for the ICO to provide explicit reference to what they will do as guidance to the regulators and those regulated (ie will they have to fight two fronts simultaneously or consecutively on the same issue, will the ICO form an appeal forum or will it order the internal regulator to cease their investigations?)

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

People may be able to ~~can~~ enforce their data protection rights in court or claim compensation for damages, or both. When the case concerns journalism, the person pursuing court action can ask the ICO to assist, if the ICO considers that the case is of substantial public importance.

Courts must stay (or in Scotland, sist) some legal proceedings if certain criteria are met, which protect~~s~~ publication. Note: Typo as criteria is plural.

What is the ICO's approach to enforcement and investigations and how is journalism protected?

We have powers to take formal enforcement action for breaches of data protection law. However, there are specific and strong protections for journalism and various restrictions and safeguards built into the law.

Any action we take will be targeted and proportionate in line with our Regulatory action policy. We reserve our strongest measures for incidents of serious harm. We also carefully consider the potential impact on freedom of expression before deciding to investigate or take any action in cases involving journalism.

We may also prosecute criminal offences. We only do this when we consider it is in the public interest in line with our Prosecution policy statement. There are specific defences available relating to the public interest and journalism.

NOTE: In order to be a comprehensive guide for journalists, the code should set out the relevant criminal offence provisions of the DPA (including s170) and the way that journalists may defend themselves from such a prosecution.

This code does not include any reference to the provisions of s170 of the DPA 2018 which makes it an offence to knowingly or recklessly and without the consent of the data controller to obtain or disclose personal data. There is no information in this guide about this criminal offence and the way that journalists may defend themselves from such a prosecution.

The Reference notes contain~~s~~ more details about the key legal provisions.

1. Apply the journalism exemption

NOTE: GNM suggests it would make sense to include a brief introduction to the usual requirements of data protection law before explaining how the exemption may disapply some. It would also be helpful at this point to include reference to the legitimate interests as a basis for lawful processing.

At a glance

- There is an exemption in data protection law to protect freedom of expression and information in journalism, academic activities, art and literature.
- When the criteria for using the exemption is met, you do not have to comply with many of the usual requirements of data protection law.
- You **must** always comply with the key data protection principle~~s~~ of ~~accountability and~~ security. NOTE: This is not correct. Accountability only applies in respect of those principles that are not subject to the journalism exemption.
- The exemption applies if you:
  - use personal data for journalism;
  - act with ~~the intention or hope of~~ a view to publishing journalistic material; NOTE: Risk of the 'intention or hope' being interpreted differently to the statute
  - reasonably believe publication is in the public interest; and
  - reasonably believe that complying with ~~a specific~~ part~~s~~ of data protection law is incompatible with journalism.
- ~~You **should** interpret~~ Journalism is interpreted broadly.
- The exemption can cover all the personal data you use for journalism as long as you act with a view to publishing journalistic material ~~have the intention or hope of publishing it~~.
- A "reasonable belief" is one you are able to justify in a reasonable way. NOTE on definition of reasonable belief: The definition of what is a reasonable belief should not be tied to publication. Surely it means a belief that a reasonable person in the same position is capable of holding?
- Deciding what is "in the public interest" involves considering the special importance in freedom of expression and information and any specific codes of practice or guidelines relevant to you. ~~considering the circumstances, balancing arguments for and against, and judging how the public interest is best served overall.~~ NOTE: Amended to reflect that statutory requirements rather than public law principles of proportionality that are inappropriate here.

- The exemption applies if you reasonably believe that it would be impracticable to comply with ~~a specific~~ parts of data protection law ~~must or should be set aside because complying with it disproportionately restricts~~ whilst carrying out your journalistic activity.

In more detail

What does the journalism exemption do?

1.1 There is an exemption in data protection law to protect freedom of expression and information in journalism, academic activities, art and literature. For ease, we refer to this throughout the code as the journalism exemption.

1.2 When the criteria for using the exemption is met, you do not have to comply with many of the usual requirements of data protection law. For example, the exemption can remove the usual requirements to:

- have a lawful reason or basis for using data (see Use personal data lawfully);
- provide privacy information (see Use personal data transparently); and
- comply with individual rights that people have about their personal data (see Help people to use their rights).

1.3 For a full list of the parts of the UK GDPR that the exemption applies to, see key legal provisions in the Reference notes.

1.4 Although the journalism exemption is broad, you **must** always comply with some fundamental parts of data protection law, as follows:

- the principle of accountability, including the requirement to carry out a data protection impact assessment (DPIA) for certain types of processing (see Take steps to protect personal data); NOTE: As above, Accountability only applies to those provisions of the DPA principles that are not incompatible with journalism (in compliance with the journalism exemption) and security of data.
- security (see Keep personal data secure);
- the right to opt-out of direct marketing;

- people's rights about automated processing;
  NOTE: The inclusion of the right to opt-out of direct marketing/people's rights about automated processing confuses journalism with the business of journalism - i.e. running a newspaper as a commercial entity. Eliding the two is not helpful because the principle of accountability applies to the commercial operation of media organisations but does not apply in the same way to the editorial operations. We would suggest omitting these or making clear that they relate to the commercial side of the business.
- people's right to compensation for material or non-material damage; and
- registering with the ICO. NOTE: More detail should be given on this legal requirement.

When can we use the journalism exemption?

1.5 The journalism exemption applies if you:

- use personal data for journalism;
- act "with a view to publication";
- reasonably believe that publishing would be ~~is~~ in the public interest; and
- reasonably believe that complying with ~~a specific~~ part**s** of data protection law is incompatible with journalism.

1.6 In the following sections, we explain what each of these requirements means in practice.

1.7 In many cases, we anticipate that you will not have to rely on the journalistic exemption to comply with data protection law when using personal data for journalism. However, there are some circumstances where, although you reasonably believe publication is in the public interest, data protection law may make it impractical for you to carry out your journalism ~~prevent or disproportionately restrict journalism~~. The exemption protects journalism in such circumstances.

When are we using personal data for journalism?

1.8 To rely on the journalism exemption, you **must** first decide whether you are using personal data for journalism. In many cases this will be obvious.

1.9 Journalism may involve a wide range of activities that may be loosely grouped into production (including collecting, writing and verifying material), editorial, publication or broadcast, and management of standards (including staff training, management and supervision). You **should** interpret journalism broadly to include:

- everything published in a newspaper or magazine, or broadcast on radio or television excluding paid-for advertising and equivalent content published online (eg on the websites and social media channels of newspaper and magazine publishers or broadcasters, and similar publishers who operate online-only services); NOTE: Amendment also needed to incorporate pre- and post- publication activities rather than these bullets just being a reference to actual published content
- content published by non-professional journalists, including members of the public (eg citizen journalism such as bloggers, eye witnesses or social networkers); and
- material that is journalistic but is also being used for another purpose, such as campaigning.

1.10 If you are not sure whether you are using personal data for journalism, you **should** consider the specific circumstances. Factors you **could** consider include:

- the purpose of the processing ~~publication~~, including any reasons for publishing the information (eg informing the public); NOTE: Publication is only relevant later in the exemption.
- how closely the activity aligns with the media's traditional functions (eg holding the powerful to account); NOTE: This should be amended to refer to wider definitions of the public interest and not just make reference to 'holding the powerful to account'
- whether you have made some attempt to align with typical journalistic standards or values (eg checking accuracy);
- the content of the information, including any public interest in publication; and
- the extent to which you have, or will, promote the information to the public.

1.11 The above factors are not exhaustive and whether they are relevant, and the extent to which they are relevant, varies from case to case.

1.12 For third party content or online "user-generated content", you **could** consider whether you have applied any editorial judgement to the third party content (eg to decide whether to include a reader's response). NOTE: This definition of third-party content would suggest that material that is published pre-moderation would not come within the definition of journalism. This does not take account of the fact that editorial judgement may be exercised in determining which content should be made available for readers to comment on.

The more editorial control exerted, the more likely it is that you are using personal data for the purposes of journalism.

When are we acting "with a view to publication"?

1.13 To rely on the exemption, you **must** also ~~intend or hope to publish~~ act with a view to publication of journalistic material. You publish material when you make it available to the public, even if it is not accessible to all members of the public (eg there is a subscription or pay wall).

1.14 Where you ~~intend or hope to publish~~ act with a view to publication of journalistic material, the journalism exemption can apply to all the personal data you collect, use, retain or create as part of your journalistic activity.

1.15 It does not matter whether you have a particular story in mind, or you actually publish the story you had in mind using the personal data. You can retain that personal data to use in a different story in the future, or update a story that you have already published (see Keep personal data only for as long as you need it).

What does "reasonable belief" mean?

1.16 To rely on the exemption, you **must** reasonably believe that:

- publication is in the public interest; and
- complying with the relevant provisions ~~specific part~~ of data protection law is incompatible with journalism.

1.17 You do not have to prove that publication is in the public interest or that complying with the relevant provisions ~~specific part~~ of data protection law is incompatible with journalism. Nor do you need to arrive at the same conclusion as the ICO or a judge. Different and opposing views may both be reasonable but you **must** be able to show ~~demonstrate~~ the reasonableness of your decision.

1.18 In considering whether your belief is reasonable, it is not the role of the ICO or a judge to disregard your decision lightly or substitute their own belief in place of yours. They will only consider the reasonableness of your belief on an objective basis.

1.19 It is also not the role of the ICO or a judge to disregard the important editorial discretion that you have to decide how to gather, edit, present and convey the information.

1.20 You **should** make an objectively reasonable decision. This is one that you are able to justify on reasonable grounds ~~to another person in a reasonable way~~. You can make the decision yourself, where proportionate, or delegate as you see fit.

1.21 To make a reasonable decision, you **should** consider:

- whether you have enough relevant and reliable information to make a reasonable decision; and

- what weight to give to the information you take into account ~~to help you make a proportionate decision~~.

1.22 It is the belief of the controller that is relevant rather than an individual journalist. However, you can decide to delegate responsibility for decisions to individual journalists depending on the level of risk.

Show ~~Demonstrate~~ your reasonable belief

1.23 You **must** be able to show ~~demonstrate~~ that your belief was reasonable. In some cases this will be obvious. There are different ways to do this, so you **should** decide what is appropriate depending on the circumstances. For example, you **could**:

- have a clear policy or process explaining who can make the decision and how;
- be ready to demonstrate that you followed your policy or process, as well as any relevant industry codes or guidelines; and/or NOTE: Addition of "or" because these are not mandatory provisions.
- keep a record of your decision. The level of risk involved will help you decide how detailed your records should be (see Take steps to protect personal data). You **could** do this at a later stage, if more appropriate.

What does "in the public interest" mean?

1.24 To rely on the exemption, you **must** reasonably believe that publication is "in the public interest".

NEW PARA: When considering whether publication would be in the public interest you must take into account the special importance of the public interest in the freedom of expression and information.

1.25 To decide what is in the public interest, you **must** consider specific industry codes of practice or guidelines that are relevant to you. The DPA 2018 specifies the following codes:

- Independent Press Standards Organisation (IPSO) Editors' Code of Practice;
- BBC Editorial Guidelines; and
- Ofcom Broadcasting Code.

1.26 Although not listed in the DPA 2018, the IMPRESS standards code applies to its members.

~~1.27 To judge what is in the public interest, you **should**:~~

~~• consider the circumstances;~~
~~• balance relevant factors for and against publication; and~~
~~• judge how the public interest is best served.~~

1.28 You **should** consider whether the arguments in favour of publication are stronger than any foreseeable harm to a person. Where there is a high risk, you **could** draw up a list showing the arguments on both sides to assess their relative weight.

General public interest arguments

1.29 There is a general public interest in freedom of expression and information ~~and protecting people's right to privacy and data protection~~ (see About this code).

1.30 The general public interest can take many forms. Examples you **could** consider include:

- 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.

1.31 This does not mean that there cannot be a public interest in reporting on local events. What is ultimately "in the public interest" is determined by balancing factors in favour of publication against any harm to a person.

1.32 There may be a public interest in the general subject matter of the information. Examples you **could** consider include:

- 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.
- Protecting national security
- Disclosing information the public need to know

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

1.33 In general, there may be a stronger public interest for publishing information where a person:

- is a public figure (people 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, some business people and members of regulated professions are examples of people with this type of role.

Specific public interest arguments

1.34 As well as considering general public interest factors, you **should** also consider the specific circumstances and arguments both in favour and against publication.

1.35 Certain factors can add weight to the arguments on either side of the public interest balance. Factors you **could** consider include:

- how likely and severe any harm could be. If there would be a severe impact on people ~~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 information and how likely it is to contribute to the public understanding. The information may enhance public debate, which may strengthen the public interest in publication; and
- whether information is already in the public domain. Information that is already being published in the public domain may be less damaging to publish again. There may be a public interest in presenting a full picture or to remove any suspicion of manipulating the facts or spin. However, 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?

1.36 You **must** comply with data protection law if there is a straight-forward way to do so whilst still achieving your journalistic objective.

1.37 However, a part of data protection law may be "incompatible" with journalism if you reasonably believe that it is impracticable to comply with it whilst still carrying out ~~must or should be set aside to enable~~ your journalistic activity. As explained in section 1.20 of this code, a reasonable belief is one that you can objectively justify in a reasonable way.

1.38 In some cases, it will be obvious that it would be impracticable for you ~~to you cannot~~ carry out your journalistic activity and comply with data protection at the same time. For example, you cannot use personal data fairly and transparently if you decide to use covert methods as part of an undercover investigation (see Use personal data fairly).

~~1.39 If you are not sure whether part of data protection law is incompatible with your journalistic activity, you **should** consider what actions are~~

~~proportionate in the circumstances. Generally, this means trying to achieve a fair balance between what you want to achieve and the interests of the individual.~~

~~1.40 Factors you **could** consider to help you to make a proportionate decision include:~~

- ~~the extent to which your journalistic activity is restricted by complying with the specific part of data protection law;~~
- ~~The public interest in the publication;~~
- ~~the extent to which your journalistic activity could harm the individual concerned;~~
- ~~whether you could take steps to mitigate the impact on your journalistic activity whilst still complying with data protection law;~~
- ~~whether you could reduce the impact of harm to the person whilst still achieving your journalistic objective; and~~
- ~~overall, whether you believe that complying with the specific part of data protection law disproportionately affects your journalistic activity~~

NOTE: This has been deleted as the DPA does not refer to a proportionality balancing exercise.

2. Take steps to protect personal data

NOTE: This code is supposed to be a comprehensive guide to personal data and journalism. A lot of this section relates to the commercial side of the business and will not be relevant for journalists. GNM considers this section should be renamed "Be responsible for your use of personal data" and that the non-journalism specific guidance should be removed and replaced with links to the generic guidance. Contextually it sits very oddly with the previous section on the wording of the exemption, when it starts with the words "you must take steps to protect …" which is just confusing - it needs to explain when this obligation - "must" - arise for a journalist

At a glance

- You **must** take steps to protect personal data and be able to show ~~demonstrate~~ that you comply.
- You **must** decide what steps to take to protect personal data. This varies depending on how you are using personal data for journalism and any risk of harm to people.
- You **must** review the steps you take to protect data and update them when you need to. Media organisations **could** take an organised approach to managing data protection by putting in place a system, sometimes known as a privacy management programme. This involves
  - strong leadership and oversight;
  - policies where proportionate;
  - training and awareness;
  - knowing what personal data you use; and
  - risk management.
- You **could** combine your approach to managing data protection with your existing management and governance systems.
- You **must** consider data protection when you do anything that involves personal data.
- You **must** identify and minimise risks when you use personal data. When there is likely to be a high risk, you **must** carry out a DPIA.
- **When the criteria applies, the journalism exemption can remove the usual requirement to consult us if a DPIA identifies a high risk that you cannot mitigate.** NOTE: Amendment needed to reflect that the accountability principle is dependent on the operation of the underlying data principle

In more detail

- What does "take steps to protect personal data" mean?

- How can we make sure that we take the right steps to protect personal data?

What does “take steps to protect personal data” mean?

2.1 This simply means you **must** proactively protect personal data and be able to demonstrate that you comply. This is sometimes known as the accountability principle.

2.2 There is no one-size-fits-all approach. It is for you to consider your circumstances and the level of risk to decide what steps are appropriate and proportionate. Where proportionate to do so, you **should** ~~**must**~~ put in place data protection policies. NOTE: This is confusing because it imposes a mandatory requirement to put in place data protection policies 'where proportionate to do so' without specifying where the ICO considers that it will be proportionate to do so. It is not clear if this is intended to apply to data held for the purposes of journalism or data held by media organisations for other purposes eg commercial uses. It would be an onerous requirement to impose on media organisations to develop data protection policies applicable to all the data that they use in a journalism context.

2.3 When you have got measures in place, you **must** also review and update them when needed.

How can we make sure that we take the right steps to protect personal data?

Decide what is appropriate and proportionate

2.4 It is your responsibility to decide what measures are appropriate and proportionate in the circumstances. How much risk is involved is very important. You **must** consider:

- what personal data you are using, what you plan to do with it and why, the public interest in freedom of expression and journalism, as well as the wider context; and
- the risks of using the personal data – the higher the risks (eg of harm to people), the more important it is that you can clearly demonstrate how you comply.

2.5 Considering the wider context **could** involve taking into account:

- the size of your organisation;
- its overall structure;
- the resources available to you;
- your ways of working; and
- the special public interest in freedom of expression and information.

2.6 To consider the risks of using personal data for journalism, you **must** consider how much harm it could cause, and how likely it is to cause harm. This refers to harm to specific people as well as harm to wider society. NOTE: These risks must be considered in light of the public interest in freedom of expression. e.g. Harm is caused to a politician who is exposed to have committed a fraud but the public interest in that exposure clearly outweighs the harm caused to an individual. This section seems to place more emphasis on the protection of the personal data at the expense of the public interest in publication and investigating- it should always be regarded as a balancing exercise in this code.

2.7 You **should** take into account significant risks, such as:

- discrimination, financial loss, damage to reputation or loss of confidentiality;
- stopping people from accessing their rights or controlling their personal data;
- using sensitive types of personal data known as special category data or criminal offence data (see Use personal data lawfully);
- physical harm;
- using personal data of vulnerable people, especially children; or
- using a large amount of personal data affecting a large number of people.

Show ~~Demonstrate~~ that you comply

2.8 To demonstrate what you do to comply with data protection law, you **should:**

- be able to give a clear and practical explanation of the steps you take to comply; and
- where appropriate and proportionate, provide evidence of what you do to comply and the measures you have put in place to ensure that this happens.

  NOTE on 2.8: This is really vague. It appears to be imposing an obligation on media organisations to develop wide ranging data protection policies to all of their journalistic output. It is not clear where this requirement is set out in the legislation which only applies the accountability requirements to those parts of the data principles which are not exempt as part of the journalistic exemption.

2.9 This code is generally well-aligned with industry codes so complying with them is likely to help you demonstrate that you comply with data protection.

2.10 You **could** adapt existing measures to take account of data protection requirements. For example, corporate risk, security and records management policies and existing editorial processes.

2.11 Where proportionate, you **must** put in place data protection policies, although this does not necessarily mean separate documents dealing solely with data protection. As above, you can incorporate data protection into your existing policies and processes.

2.12 You **must** also review what is happening in practice at appropriate intervals. You **should** consider not just what documentation you may have, but also how it is working for people.

2.13 Governance is often the name given to the framework of measures organisations use to comply with data protection and hold people to account. There are lots of different ways of doing this but you **could** consider adapting the ICO's Accountability framework and the main building blocks of an effective governance system or privacy management programme, as described below.

Many of these points do not appear to have any bearing on journalistic rather than commercial content: if they are intended to apply to journalistic content then it should be clearly stated.

2.14 Smaller organisations or individuals are more likely to benefit from a smaller scale approach. See further reading in the Reference notes.

Leadership and oversight

2.15 Strong leadership and oversight of data protection are important to make sure you hold people to account appropriately.

2.16 You **should** set a positive tone and culture from the top by leading by example and making sure that your organisation complies with data protection.

2.17 You **must** have a DPO, if legally required. You **should** also be clear who is responsible for practical day-to-day data protection compliance at a senior level and below. For example, in job descriptions.

Policies

2.18 The UK GDPR specifically says that you **must** have policies, where proportionate. This is likely to be more important in environments where there is significant delegation from the top and where decisions are often made at pace, such as news environments.

NOTE: This appears to suggest that there should be policies in place determining what happens to data on the news desks. In practice this would be a very onerous obligation and likely to adversely affect freedom of expression.

2.19 What you may have policies for and their level of detail varies depending on what you think is proportionate. You **should** take the risk of harm into account amongst other relevant factors (see above).

2.20 For example, you **could** have a policy (either standalone or part of another policy) to help people understand how to use the journalism exemption. Your policy **could** set out:

- what the special purposes exemption does;
- when to apply it;
- how to apply it; and
- the roles and responsibilities people have when using it.

Training and awareness

2.21 You **should** make sure that staff receive the training on data protection that they need tailored to their role, including induction and refresher training.

2.22 You **should** also regularly raise awareness of data protection. For example, you **could**:

- create quick-reference guides;
- run internal campaigns; or
- draw attention to important information through your usual internal communication channels.

Know what personal data you use

2.23 Taking stock of what information you have, where it is and what you do with it, makes it much easier to put the right measures in place to protect personal data.

2.24 If you have 250 or more employees, you **must** record your use of personal data in line with legal requirements.

2.25 There is a limited exemption for smaller organisations with fewer than 250 employees. These organisations only need to record when they use personal data in ways that:

- are not just occasional;
- could result in a risk to people's rights and freedoms; or
- involve using special category or criminal offence data.

2.26 You **should** make sure that you adequately support data protection within your organisation by good records management**.**

Manage risk

2.27 You **must** integrate data protection into any system, service, product, policy or process you design that uses personal data. This is sometimes known as taking a data protection by design approach.

2.28 You **must** incorporate data protection into your normal practice, including:

- implementing the data protection principles effectively (see About this code);
- protecting individual rights (See Help people to use their rights); and
- using only the personal data that you need (see Use personal data for a specific purpose, Use no more data than you need and Keep personal data only for as long as you need it).

NOTE on 2.28: This makes no reference to the journalism exemption that applies to most of these provisions. It should do if this is intended to be applied to journalistic data rather than commercial data. This is referred to as a mandatory provision but the journalism exemption means it is not in respect of data held for the purpose of journalism where the exemption applies.

2.29 You **should** have appropriate measures in place to identify, record and manage personal data risks. For example, you **could** have a risk policy that is either a separate document or part of your wider corporate policy.

Data protection impact assessments

2.30 A DPIA is simply a type of risk assessment. The UK GDPR provides significant flexibility to decide what structure and form it takes so that it fits with your existing processes. As a minimum, a DPIA **must**:

- describe how you plan to use the personal data and why;
- assess whether it is necessary and proportionate to use the personal data;
- assess the risks to the rights and freedoms of the people whose personal data you wish to use; and
- set out how you intend to manage these risks.

2.31 You do not need to do a DPIA every time you use personal data for journalism, but you **must** do a DPIA whenever you use personal data in a way that is likely to result in a high risk to someone. You **could** also do a DPIA for any other major project involving personal data.

NOTE on 2.31: This is not very useful since there is no indication given here about when processing is likely to result in a high risk to someone.

s64 DPA 2018 states that '(1)Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment.' but in

'(4)In deciding whether a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must take into account the nature, scope, context and purposes of the processing.'

There is no reference in this section to the context and purpose of the processing which may include the public interest in the proposed publication.

2.32 You do not need to carry out a DPIA for individual stories. You **could** do a more general DPIA that covers the ways you may use personal data in high risk ways (eg using personal data for investigative journalism).

2.33 Assessing risk involves considering how likely it is that using personal data will cause harm and how severe any harm could be (see Take steps to protect personal data). Much of the day-to-day work of journalists does not involve a high risk to people. If you think there may be a high risk, you **must** consult your DPO, if you have one.

3. Keep personal data secure

At a glance

- You **must** keep personal data secure. This involves protecting personal data against unauthorised or unlawful use and accidental loss, destruction or damage.
- Security measures are not limited to cyber-security. They also include organisational measures and physical security.
- You **must** be able to restore personal data if there is a security incident. NOTE: It is unclear that this has to apply to all journalistic content. It is possible that in order to keep personal data secure that it is only stored in one location. We assume that this provision applies to commercial data held by media organisations and not to the data that journalists hold.
- You **must** review and keep security measures up-to-date.
- You **must** decide what security measures are appropriate and proportionate to protect personal data, taking into account the circumstances, the risk of harm, and available technology.
- Your security arrangements **should** take into account the security risks of using mobile devices and remote working.
- You **must** ask anyone acting on your behalf to demonstrate they can keep personal data secure. You **must** also have a written contract with them dealing with security.
- A DPIA can help you assess security risks when others act on your behalf or you share personal data with them.
- You **must** record all personal data breaches, and tell the ICO if the breach is likely to cause harm to someone.
- If there is a high risk, you **must** also tell the people affected. NOTE: Bearing in mind the provisions set out below 'must' seems an inappropriate classification of this instruction.
- **When the criteria applies, the journalism exemption can remove the usual requirement to tell people where there is a high risk of harm that they have been affected by a data breach ~~when there is likely to be a high risk~~.**

In more detail

- What does keeping personal data secure mean?
- How do we keep personal data secure?

What does keeping personal data secure mean?

3.1 You **must** keep personal data secure. This involves protecting it against unauthorised or unlawful use and accidental loss, destruction or damage.

3.2 To do this, you **must** have appropriate and proportionate security measures. This involves cyber-security, as well as physical and organisational security measures.

3.3 You **must** be able to restore personal data if there is a security incident as soon as possible (eg a backup system). NOTE: It does not seem appropriate that there is a requirement that all journalistic data should capable of being restored since this appears to impose an obligation that there should be at least two copies of all personal data held by journalists just in case something happens to one of them. This is unrealistic and actually may pose a greater security risk to that data if it is imposed since with each copy it doubles the obligations to keep such data secure. This provision seems to make more sense in applying it to commercial data held by media organisations.

3.4 You **must** also review and update your security measures. For example, scanning for network vulnerabilities to prevent risks developing that compromise your security.

How do we keep personal data secure?

Decide what security is appropriate and proportionate

3.5 In a similar way to the accountability principle, you **must** consider all the circumstances and the risks of harm to keep personal data secure (see Take steps to protect personal data). You **must** also take into account what technology is available and the costs of security measures.

3.6 You **should** consider factors such as:

- your organisation's premises and computer systems;
- who has access to personal data and how; and
- any personal data a third party is using on your behalf.

Harm

3.7 Amongst other factors, you **must** consider how likely it is that using the data could harm someone, and how severe any harm could be.

3.8 When choosing security measures, you **should** consider significant risks. You **must** also carry out a DPIA, if there is likely to be a high risk. This will help you decide on appropriate security measures to manage the risks.

3.9 For example, there is a high risk involved in personal data that could identify a journalist's confidential sources. In some cases, a security breach

could pose a risk to someone's physical health or safety. Where that is the case, you **should** have strong security measures to protect the personal data, including strict measures controlling access.

Working practices

3.10 Journalism often involves working flexibly in different environments, including a strong reliance on remote working and portable devices. You **should** therefore consider how you keep your IT equipment secure, especially portable devices, such as laptops, tablets, and smart phones.

3.11 There are a wide range of low-cost and easy to implement cyber-security solutions. You **should** consider common techniques such as encryption and password protection. This is important for all the devices you use, including mobile ones.

3.12 Where you have a business need to store personal data on removeable media (eg a memory stick), you **must** minimise it (see Use no more data than you need).

3.13 You **should** consider the increased security risks if you allow employees to use their own devices for work purposes.

3.14 You **should** train your employees to follow fundamental security advice if travelling with personal data, including:

- check Foreign Office travel advice, if going overseas;
- only take what you need;
- keep devices and papers with you and store them securely; and
- lock or power off your device when not in use.

3.15 You **should** also raise awareness of common security issues when travelling, such as discussing confidential information, allowing people to overlook a screen and writing down or telling someone a password.

Third parties using data on your behalf

NOTE: This should clarify that freelancers or independent media companies are unlikely to be acting as processors and so do not come within the provisions of this section about third parties. It would be useful if a practical example of a third party processor in the journalism context could be given here.

3.16 You **must** make sure that any third parties acting as a data processor on your behalf ~~and using personal data~~ comply with the UK GDPR (see Be clear about roles and responsibilities).

3.17 In particular, you **must** only use third parties as a data processor to act on your behalf that can give you sufficient guarantees about their security measures to protect personal data.

3.18 You **must** have a written contract with the third party processor, making it clear that they must provide the same level of security for personal data as you do. The contract **should** allow you access to all the information you need to demonstrate that the personal data is secure.

Sharing personal data

3.19 You may share personal data with a third party who is not acting on your behalf. For example, you may ask a freelance journalist to write a story or take a photograph, where they have the freedom to act beyond your instructions. In this scenario, the third party is also legally responsible for keeping the personal data secure in the same way as you are.

3.20 Even if you are not legally required to do a DPIA, you **could** do one when sharing personal data to help you to identify security risks and how to mitigate them. This may be particularly helpful if the data sharing is routine or planned, when you may have more time available.

Personal data breaches

3.21 You **must** keep a record of personal data breaches and how you deal with them. A personal data breach means a breach of security leading to the accidental or deliberate destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

3.22 If a personal data breach is likely to cause harm to someone, you **must** tell the ICO as soon as possible, and generally within 72 hours. If you do not think the breach is likely to cause harm, you **should** record the reason.

3.23 You **must** tell people affected by a breach when there is likely to be a high risk to them. NOTE: unless the exemption applies

4. Use personal data lawfully

At a glance

- You **must** use personal data lawfully. [NOTE: The term 'must' is inappropriate in respect of conditions that only apply if the journalism exemption does not. If the same language is used as when the provision is mandatory for everyone it will cause confusion.]
- You **must** have a ~~specific~~ lawful reason under the UK GDPR to use personal data.
- The lawful reasons most likely to be relevant to journalism are legitimate interests and consent.
- You have a legitimate interest in using personal data, if there is not a less intrusive way of achieving the same result, and your interests are not outweighed by harm to a person.
- Consent is often not the most appropriate lawful reason for a journalist to use, unless you are giving people genuine control over how you use their data. If you rely on consent, you **must** comply with the high standards of consent in the UK GDPR. NOTE: The Code should specify what these are.
- Special category or criminal offence data needs more protection because it is sensitive. You can use this type of data, if you have a lawful reason **and** can satisfy the relevant conditions and safeguards under the DPA 2018.
- If the criteria is met, there is a condition to enable sources to disclose these sensitive types of data about unlawful acts and dishonesty for journalism.
- Criminal offence data includes allegations of criminal behaviour. You **should** consider all the circumstances to decide if a suspect has a reasonable expectation of privacy. ~~If a suspect is under investigation by the state, there is usually a reasonable expectation of privacy.~~ NOTE: This is about privacy and not data protection.
- You **should** make sure you can defend ~~justify~~ identifying a suspect, taking into account the public interest in publication and the harmful consequences for the person.
- **When the criteria applies, the journalism exemption can remove the usual requirements to:**
  - **use personal data lawfully in line with the data protection principle;**
  - **satisfy a lawful basis for using the data;**
  - **comply with conditions for consent and children's consent; and**

- **comply with the rules about special category data and criminal offence data.**

In more detail

What does use personal data lawfully mean?

4.1 You **must** have a ~~specific~~ lawful reason for using personal data. This is known as a lawful basis, or bases, if more than one applies. NOTE: The use of the word 'must' is misleading as when the journalism exemption applies these provisions do not apply. The availability of the exemption in relation to 'must' obligations should be clear to the reader throughout, including in relation to 4.2 and 4.3

4.2 You can use sensitive types of data known as special category data and criminal offence data, if you can satisfy the relevant conditions and safeguards.

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

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

4.5 You **must** check that you are acting in line with other laws as well, including statutory and common law obligations, whether criminal or civil. For example, using personal data may be unlawful if it is a breach of confidence, infringement of the Human Rights Act 1998, or in contempt of court.

How do we use personal data lawfully?

4.6 You **should** use the most relevant lawful reason and consider if more than one applies. Changing your mind about which lawful reason applies is likely to breach the data protection principle to use personal data fairly and transparently.

4.7 The lawful reasons most likely to be relevant to journalism are legitimate interests and consent. Although, legitimate interests is often more appropriate than consent in most cases.

Legitimate interests

4.8 You can rely on this lawful reason when it is necessary to use personal data to pursue legitimate interests **and** where those interests are not outweighed by any harm caused to a person.

4.9 This lawful reason is likely to be most appropriate when you use people's personal data in ways they would reasonably expect with minimal privacy impacts. For example, in day-to-day reporting on local events. However, even if there is a more significant risk of harm, it can still apply if you can justify the harm.

4.10 If you want to use this lawful reason, you **should** identify what your legitimate interests are. Legitimate interests can be your own or third party interests and can include commercial interests. For example, there is a legitimate interest in journalism because of the special public interest in freedom of expression and information (see About this code).

4.11 You **must** only use the personal data if it is necessary to pursue those legitimate interests. This means that you **should** consider whether there is another reasonable and less intrusive way to achieve the same result. If there is, this lawful reason does not apply.

4.12 You **must** consider whether your legitimate interests are outweighed by harm to a person. Where your legitimate interest is journalism, any harm would need to be sufficiently serious to justify interfering with the fundamental right to freedom of expression and the pubic interest in maintaining the freedom of the press. You **should** consider their reasonable expectations and any unwarranted harm (see Use personal data fairly). You **could** complete a Legitimate interest assessment to help you balance different interests.

4.13 In many cases it will be obvious or self-evident that processing for the purposes of normal journalistic activity will be lawful because off your legitimate interests. You **should** take extra care when dealing with children's personal data or other vulnerable groups. You **must** consider a child's best interests in accordance with the United Nations Convention on the Rights of the Child.

Consent

4.14 The consent lawful reason may sometimes be used for journalism. For example, you can use special category data with explicit consent (see below).

4.15 However, consent is often not the most appropriate lawful reason to use for journalism, unless you are giving someone genuine choice and control over how you use their personal data.

4.16 If you want to use a child's personal data, you **should** consider the child's competence and ability to understand consent. If you have doubts, the

legitimate interests lawful reason may be more appropriate to show that you have properly protected the child's rights.

4.17 When offering an online service directly to children, only children aged 13 or over are able to consent.

4.18 If you are relying on consent as a lawful reason for using personal data, you **must** comply with the high and specific standards for consent in the UK GDPR. You **could** keep a record of who consented, when, how and what you told them to help demonstrate that you have complied (See Take steps to protect personal data). NOTE: These requirements should be set out in the Code.

What is special category data?

4.19 Data protection law gives extra protection to sensitive types of personal data. Some of this type of data is known as special category data.

NOTE: it would be helpful to explain where legitimate interests/consent/special exemption sits with regard to special category data. The reference at 4.21 could be clearer on this - see suggestion.

4.20 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.

4.21 You can use special category data for journalism if you have a lawful reason for doing so - such as a legitimate interest or consent - **and** you meet one of the conditions in the UK GDPR. For some of these, you **must** also meet further conditions and safeguards set out in Schedule 1 of the DPA 2018. Where the journalism exemption applies you do not have to comply with the additional further conditions and safeguards.

How do we use special category data lawfully?

4.22 First, you **should** decide whether you are using special category data. The UK GDPR is clear that the information does not need to specify these

details. Information that reveals or concerns special category data is also covered. NOTE: It is not clear what this means.

4.23 There may be times when you are not sure whether the information is special category data. For example, you may be able to infer an individual's religion or ethnicity from names, photographs or film. Where there is doubt, you **should** consider:

- whether it is possible to infer or guess special category data from the information you want to use;
- how certain that inference is; and
- whether you are deliberately inferring the data.

4.24 If you use the personal data specifically because it reveals one of the details above, you are using special category data. However, if you can only infer or guess these details, you do not need to meet extra conditions to use the data. Although you **must** still consider whether it is fair to use the information in context (see Use personal data fairly).

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

4.26 There are 10 conditions under the UK GDPR that provide extra protection for special category data and can give you a valid reason for using it. Below, we refer to those most likely to be relevant to journalism. NOTE: All the conditions should be stated either in this guide or in the accompanying material.

Explicit consent is given to use it

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

The data is manifestly made public by the person it is about

4.28 This condition applies if personal data is obviously made public by the person concerned. Personal data is made public if it is realistically accessible to a member of the general public, including if that is only to part of the general public because there is, for example, a subscription or paywall to access news content. This condition does not apply if an individual has indicated an intention to make it public in the future or is in the process of doing so.

4.29 You **should** be cautious when applying this condition to information obtained from social media posts or other user-generated content. You **must** always consider whether it is fair to use the data, bearing in mind that people may make their personal data public without realising it.

4.30 In the context of criminal trials, an offender may obviously make information about their offending public in line with the principle of open

justice. However, you **must** consider whether using the personal data again remains fair at a later date. Subject to certain exceptions, some of which are set out below, An offender may reasonably expect privacy as a result of the passage of time, even if information is initially made public.

4.31 You **should** also consider whether using the personal data would cause unwarranted harm. There is a ~~strong~~ public interest in the rehabilitation of offenders recognised in the Rehabilitation of Offenders Act 1974 (ROA 1974). Although this is generally a strong factor in favour of not publishing or broadcasting data once a conviction is spent, whether or not it is fair depends on all the circumstances.

NEW PARA: Even where using data manifestly made public might be unfair to a data subject, it may be permissible to use it if the Journalism Exemption applies.

There is a substantial public interest with a reason in law

4.32 You can use special category data if there is a substantial public interest and you have a valid legal reason to do so. This means that one of the substantial public interest conditions **must** apply that is set out in paragraphs 6 to 28 of Part 2 of Schedule 1 of the DPA 2018. NOTE: These provisions are essential to set out in the Code so that it is a one-stop guide to data protection for journalists.

Eg It is in connection with the commission or an unlawful act, dishonesty, malpractice or other seriously improper conduct, unfitness or incompetence or mismanagement in the administration of or failure in service by a body or association.

4.33 There are 23 substantial public interest conditions. We refer below to the two conditions most likely to be relevant to journalism.

It is necessary for the administration of justice

4.34 This condition is met if using personal data is necessary for the administration of justice.

4.35 The open justice principle is a long-standing feature of our legal system that recognises the strong benefits to society of open justice. For example, promoting public confidence in, and respect for, the administration of justice.

4.36 If you use this condition, you **must** have an Appropriate policy document. You **must** keep this for six months after you stop using the data. You **could** publish it to help people understand how you protect personal data.

It is disclosed for journalism about unlawful acts and dishonesty

4.37 This condition is most likely to be used to allow a person or an organisation, such as a whistle-blower, to send data to you for the purposes of journalism.

4.38 It applies if special category data is **disclosed** for journalism by the person with legal responsibility for complying with data protection law known as the controller **and** it relates to:

- a person acting unlawfully;
- dishonesty, malpractice or other seriously improper conduct of a person;
- the unfitness or incompetence of a person; or
- mismanagement or service failure by a body or association.

4.39 The controller of the personal data can disclose personal data to you for journalism if there is a substantial public interest, it is necessary to disclose the data, and they:

- are disclosing it with a view to publication; and
- reasonably believe that disclosure of the personal data would be in the public interest.

4.40 If a third party controller uses this condition to disclose personal data to you, you need to apply the journalism exemption, if you want to use the data for journalism yourself (see Apply the journalism exemption).

What is criminal offence data?

4.41 Data protection law gives extra protection to personal data about criminal convictions and offences or related security measures. This is sometimes known as criminal offence data.

4.42 Criminal offence data covers a wide range of information about:

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

4.43 It also covers related security measures, including:

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

4.44 You can use criminal offence data for journalism if you have a lawful reason for doing so and you meet one of the conditions in Schedule 1 DPA or if the journalism exemption applies.

How do we use criminal offence data lawfully?

4.45 Before you use any criminal offence data, you **should** consider why you want to use it. This will help you identify ~~choose~~ a relevant lawful reason and condition or if necessary to apply the Journalism exemption.

4.46 There are 28 conditions that allow you to use criminal offence data that are set out in paragraphs 1 to 37 of Schedule 1 of the DPA 2018. Those most likely to be relevant to journalism are the same as those set out above about special category data. The only difference is that consent does not need to be explicit.

Allegations of criminal activity [NOTE: Too much detail on privacy law here - would suggest this section is trimmed down]

4.47 Before you use personal data about allegations of criminal activity, you **must** consider a person's reasonable expectations of privacy and the likely impact on them ~~serious risk of harm~~, in particular, reputational harm. You **must** do this if you are considering whether:

- the legitimate interests lawful reason applies;
- using the data would be fair; and/or
- the journalism exemption applies.

4.48 In some cases, there may be a risk of prejudice to the course of justice. You **must** only use criminal offence data if it would not breach any other law. For example, you may be in contempt of court if you publicly comment on a court case on social media or in a story.

4.49 In privacy law, a ~~A~~ suspect under state investigation usually has a reasonable expectation of privacy up to the point of charge, including about the fact that there is an investigation. Although it depends on the specific facts of each case~~, the facts will often point to a conclusion that there is a reasonable expectation of privacy~~.

4.50 Whether or not someone is under a state investigation, you **should** consider whether they have a reasonable expectation of privacy in all the circumstances (see Use personal data fairly). There may be reasons why an expectation of privacy is not reasonable. For example:

- the activity may take place in a public place where it is not reasonable to expect privacy (eg rioting);
- an expectation, that was initially reasonable, may no longer be so (eg if the police decide to disclose information for operational reasons).

4.51 When considering where an activity, such as an arrest, took place and any resulting impact on privacy expectations, you **should** take into account that media reporting can attract substantially more attention than would otherwise be the case.

4.52 You **should** make sure you can justify any decision to publish information identifying a suspect, taking into account the public interest in publication and if there are possible harmful consequences for the suspect (see Apply the journalism exemption). NOTE: actual harm should not be presumed

4.53 You **should** act proportionately and consider whether you can sufficiently serve the public interest without identifying the suspect. For example, you may be able to highlight weaknesses in an investigation by a public authority without identifying a suspect.

4.54 If there is a duty of confidence associated with the personal data, you **should** take into account that there is a ~~strong~~ public interest in observing duties of confidence. For example, documents about a public authority's investigation of criminal activity.

~~4.55 It **could** be relevant to consider the impact of a person's public profile because they may be more vulnerable to false allegations. An allegation that causes reputational harm may also be more damaging to such people because of their public status and the specific circumstances.~~ [NOTE: Delete as this seems to imply that if a person has a higher public profile they are more likely to be accused of an offence falsely.]

5. Use personal data fairly

At a glance

- You **must** use personal data fairly. [NOTE:The term 'must' is inappropriate in respect of conditions that only apply if the journalism exemption does not. If the same language is used as when the provision is mandatory for everyone it will cause confusion.]
- You **should** consider what someone reasonably expects in the circumstances and whether using the data is likely to cause any unwarranted harm.
- You **should** consider the specific circumstances to decide what someone reasonably expects. Various factors may be relevant including:
  - the extent to which the information is in the public domain;
  - a person's public profile; and
  - the risk of harm.
- There are certain types of sensitive data that will normally, but not always, be private, such as data about a person's physical or mental health and sex life.
- When someone is charged with a crime, the open justice principle means there is generally an expectation of transparency, although this data may become private with the passage of time.
- You **should** make sure you can justify your decision to use any personal data in view of the risk of harm and publish data that is proportionate to the public interest.
- Photographs or filming may be particularly intrusive. You **must** consider whether it is fair to use the data, even if the person is in a public place.
- Using covert surveillance, subterfuge or similar intrusive methods may be justified in the context of journalism, but you are likely to need to use the journalism exemption.
- **If the criteria applies, the journalism exemption can remove the usual requirement to use personal data fairly.**

In more detail

What does using personal data fairly mean?

5.1 You **must** use personal data fairly. This involves using it lawfully and transparently, which are part of the same data protection principle (see also Use personal data lawfully and Use personal data transparently).

How do we use personal data fairly?

5.2 You **should** use personal data in ways that:

- people reasonably expect; and
- do not cause unwarranted harm to them.

5.3 Not all harm is unwarranted. You can use personal data even if it may cause harm but you **should** be able to justify it. The greater the harm, the stronger your justification should be.

Reasonable expectations

5.4 You **should** consider whether using personal data is within someone's reasonable expectations, taking into account all the circumstances. NOTE: It may be helpful to explain the difference in threshold between the applicability of data protection law versus privacy law here.

5.5 When considering a person's reasonable expectations, it is often important to decide whether a reasonable person would consider the information to be private.

5.6 When in doubt about whether someone has a reasonable expectation of privacy, you **could** consider the following factors:

- the person 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 and where it happens;
- how and why you plan to use the data;
- your lawful reason for processing the data;
- the impact on the person; and
- how and why you obtained the personal data.

5.7 If a person is acting in the context of professional or business activities, there may be no reasonable expectation of privacy or it may be reduced significantly. However, they may still reasonably expect privacy, so you **should** consider all the circumstances.

5.8 Information that was private may become so well-known that it is no longer private. If the information, or similar information, about the person is already in the public domain, the impact on any reasonable expectation of privacy varies depending on the facts and circumstances.

5.9 A public figure may attract or seek publicity about some aspects of their life without necessarily losing the right to privacy in other matters. You **should** consider all the circumstances. Factors you **could** take into account include:

- the extent to which someone has made their personal data public;
- what personal data they have made public; and
- how you are planning to use their personal data.

Sensitive types of personal data

5.10 While you **should** always consider all the circumstances, there are certain types of information which are usually, but not always, considered private. For example:

- special category data is a sensitive type of data that is given extra protection under the UK GDPR (see Use personal data lawfully);
- personal data about someone's home life, correspondence or personal finances; and
- personal data about someone's involvement in crime as a victim or a witness.

5.11 Criminal offence data is also given extra protection in the UK GDPR. However, the principle of open justice means that the media can generally report on criminal trials (see Use personal data lawfully).

5.12 You **should** make sure you can defend ~~justify~~ any harm caused to someone. In particular, there is a greater risk of harm when using special category data because it is more likely to harm a person's fundamental rights. For example, it could cause discrimination.

5.13 Any time you use personal data, whether or not it falls within the sensitive types protected by the UK GDPR, you **must** consider the risk of harm to people weighed against the public interest in freedom of expression and information (see Take steps to protect personal data).

Children and other vulnerable people

5.14 You **must** take extra care when dealing with children's personal data (anyone under 18). The child's best interests **must** be your main consideration in accordance with the United Nations Convention on the Rights of the Child.

5.15 You should also take into account other groups who may be vulnerable, such as some elderly people or those with certain disabilities.

5.16 All these groups may be less able to understand how you will use their data and the risks involved. ~~In these circumstances, publication is less likely to be fair.~~ Publication in these circumstances must be approached carefully to make sure that it is fair.

5.17 A child does not have a lower expectation of privacy simply because their parents have a public profile.

Photographs or filming, especially in public

5.18 You **should** keep in mind that photographs or film may be particularly intrusive. The intrusive impact may be greater if someone is continually photographed or recorded, or if it was not clear to them what you were doing.

5.19 People should reasonably expect that they may sometimes be photographed or caught on film in public in an incidental way. However, if a person's image is captured in public and they are the subject of the photograph or film, you **must** consider whether using their personal data is fair in the circumstances, even if the activity is happening in a public place. NOTE: is it possible for the ICO to add something here or in 5.20 as to how ICO would regard public figures, politicians, celebrities etc who are photographed or filmed carrying out their public functions or duties in public?

5.20 You **should** act proportionately, taking into account the public interest in using the personal data and the harm it could cause. You **should** consider whether the public interest can be sufficiently served without disclosing the specific personal data shown in the photograph or film.

Covert surveillance, subterfuge and similar intrusive methods

NOTE: This topic is also covered in existing industry codes and it may be helpful to refer to this here.

5.21 These types of techniques include the use of private detectives, covert recording, disguise, and long-lens photography. Such methods are more likely to be used for investigative journalism.

5.22 You **should** consider whether it is proportionate to use these kinds of methods to serve the public interest, or whether there is a less intrusive way of doing it.

5.23 If you are using covert and intrusive methods, you are likely to need to use the journalism exemption (see below). This is because such techniques are unlikely to be in line with the data protection principles to use personal data fairly and transparently, although they may still be justified in the context of journalism.

5.24 You **should** carefully consider the strength of the public interest in publication and take into account harm to the person concerned. Given the

risk of harm, it is more likely to be appropriate to record your decision and the factors you considered. There is generally a greater risk of harm if you are using special category data, such as details about an individual's sex life or criminal offence data.

6. Use personal data transparently

At a glance

- You **must** use personal data transparently. NOTE: The term 'must' is inappropriate in respect of conditions that only apply if the journalism exemption does not. If the same language is used as when the provision is mandatory for everyone it will cause confusion.
- You **must** tell people about your use of their personal data. This information is known as privacy information. NOTE: The code should make clear that the provision of privacy information is not an individual obligation on journalists and that media organisations can provide privacy information in the form of a privacy notice on their website
- When you collect personal data from the person it is about, you **must** provide them with privacy information at the time you collect it.
- When you collect personal data from a source other than the person it is about, you **must** provide that person with privacy information within a reasonable period and no later than one month. NOTE: It is not realistic to apply this to journalism (see note on 6.4 below)
- You **must** make people aware of privacy information and it must be easy to understand and access, especially if you use personal data about children or vulnerable people.
- When you collect personal data from a source other than the person it is about, you do not need to provide information if an exception applies, including that it would be impossible, involve disproportionate effort or cause serious prejudice to your journalistic aims.
- You **should** consider whether you need to do a DPIA if you collect personal data from a source other than the person it is about without providing them with privacy information.
- **When the criteria applies, the journalism exemption can remove the usual requirements to:**
  - **use personal data transparently; and**
  - **provide privacy information to the person the personal data is about when you collect it.**

In more detail

What does “use personal data transparently” mean?

6.1 You **must** use personal data transparently to help people understand data protection and exercise control over their personal data. NOTE: This journalism exemption is likely to apply to many of the provisions of this section and using the mandatory 'must' and not referring to the section in this chapter except in the introduction gives a misleading impression about the journalists' duty to comply with these provisions.

6.2 In particular, you **must** generally provide information to people about your use of their personal data. This is called privacy information.

6.3 When you collect personal data from the person it is about, you **must** provide privacy information at the time you collect it unless they already have it.

6.4 When you obtain personal data from a source other than the person it is about, even if it is a publicly accessible source, you **must** provide that person with privacy information within a reasonable period. NOTE: It is not realistic that this provision is applied to journalists since providing details that a source may have provided to them about a third party to that third party is likely to compromise their reporting and the source. It is misleading to set out the provision in this way without referring to the relevance and applicability of the journalism exemption. It should not be later than one month. If you are contacting the person the data is about, or plan to disclose or publish the data, you **must** provide privacy information when you make contact or disclose the data at the latest.

6.5 When you obtain personal data from a source other than the person it is about, you do **not** need to provide privacy information if:

- the person already has the information;
- providing the information would be impossible;
- providing the information would involve a disproportionate effort;
- providing the information would make it impossible or seriously impair your ability to achieve your objectives;
- 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.

How do we process personal data transparently?

6.6 You **must** provide privacy information at the time you collect personal data or within a reasonable period, as explained above. This means acting fairly in the circumstances and giving people a meaningful opportunity to consider privacy information, where possible.

6.7 The privacy information you provide **must** be concise and easy to understand, especially when you are using children's data or data about vulnerable people. There are a variety of different techniques. For example, you **could** consider using graphics and videos.

6.8 You **must** actively provide privacy information. If you have a website, you **should** include a privacy notice and you **should** also consider whether you need to provide privacy information in other ways to make sure it is easily accessible.

7. Use accurate personal data

At a glance

- You **must** use personal data that is accurate and, where necessary, keep it up-to-date. [NOTE: The term 'must' is inappropriate in respect of conditions that only apply if the journalism exemption does not. If the same language is used as when the provision is mandatory for everyone it will cause confusion.]
- You **must** take reasonable steps to check that personal data is accurate.
- You **should**:
  - make sure that the source of the personal data and their status is clear, where possible;
  - consider any challenges to the accuracy of the data; and
  - consider whether you need to update it. NOTE: The circumstances in which media organisations are expected by the ICO to reexamine previously published material should be set out in this section.
- As a general rule, the greater the risk of harm to people, the more thorough your accuracy checks need to be.
- If normal accuracy checks are not possible, you **should** make sure your staff know how to manage the risk of harm.
- You **should** consider how accurate the sources of personal data are. NOTE: Please see more detailed comments on the substances of these bullets below.
- You **should** clearly distinguish between fact and opinion when reporting personal data.
- You **should** clarify the nature or context of personal data where necessary.
- You **must** help people to exercise their data protection rights if they challenge the accuracy of personal data.
- **When the criteria applies, the journalism exemption can remove the usual requirement to use accurate personal data.** However, accuracy is generally a fundamental journalistic value so you are unlikely to use it for this reason often.

In more detail

- What does "use accurate personal data" mean?
- How do we make sure that we use accurate personal data?

What does use accurate personal data mean?

7.1 You **must** use personal data that is accurate and, where necessary, keep it up-to-date. You **must** also take reasonable steps to make sure that personal data is accurate. NOTE: There has to be some acknowledgment in this section that data, which is historic and no longer up to date, can still be accurate in respect of journalism if for the relevant period of the investigation it was accurate. ie during the relevant period X had an offshore account but no longer has one.

The ICO should also specify where it considers it 'necessary' to keep personal data up to date. There is a lot of material published by media organisations and left available in their archives. The ICO should be clearer on the obligations that they are imposing on media organisations in this respect

7.2 The DPA 2018 says that "inaccurate" means "incorrect or misleading as to any matter of fact".

How do we make sure that personal data is accurate?

NOTE: It would be helpful if the code referred to the accuracy provisions of existing editorial codes, that are likely to be useful for journalists.

The code should also refer to the fact that the ICO's role is not to interfere with editorial decision making.

Reasonable accuracy checks

7.3 Even in lower profile stories, you **must** take reasonable steps to check that personal data is accurate. Simple accuracy checklists **could** help you to do this when working at pace.

7.4 You ~~**sh**~~ **could**:

- make sure that the source of the personal data and their status is clear where possible;
- consider any challenges to the accuracy of information; and
- consider whether you need to update the data.

7.5 To help you decide what accuracy checks are reasonable, you **should** consider the circumstances, including the urgency of the particular story and the risk of harm. As a general rule, the greater the risk of harm to someone, the more thorough your accuracy checks should be.

7.6 There may be circumstances when you decide that it is in the urgent public interest to publish personal data without carrying out normal accuracy checks. This may be the case when broadcasting live, for example. You **must** be able to show that you put in place appropriate measures to manage the

risks (see Take steps to protect personal data). You **could** consider the following factors:

- who has authority to make the decision;
- what checks might be possible;
- whether you could delay publication;
- the nature of the public interest at stake; and
- the risk of the information spreading quickly online.

~~7.7 If you go ahead with publication or broadcast in the above circumstances, you **should** be as clear as possible that you are reporting on unconfirmed facts and any potential inaccuracies.~~ NOTE: Delete as strays into editorial-decision making regarding what should be published.

Sources of information

7.8 You **should** consider how accurate the sources of personal data are. A clear process for checking facts and sources **could** help you to do this. ~~For example, you **could** consider whether you are dealing with:~~

- ~~a primary source (who you hear from directly);~~
- ~~a generally reliable source such as a news agency; or~~
- ~~a secondary source (typically a second-hand report by someone else).~~

~~7.9 Primary sources may be more reliable generally. For example, you may feel confident in the eye-witness account of a colleague working within your organisation or in an interview broadcast by another news outlet. However, you **must** still carry out reasonable checks (eg if you have several different accounts from eye-witnesses).~~

~~7.10 Secondary sources may be less reliable than a primary source. This may be a tip-off, comments on social media or something reported to have happened by another news outlet. You **should** take particular care when using online material, especially social media or other user-generated content.~~

NOTE: Delete as straying into editorial discretion and making generalisations that may not be of practical use

7.11 You **should** consider what steps it is reasonable to take to check and corroborate what a source has told you or put the data into its appropriate context (see below).

~~7.12 If possible, you **should** be clear about the source of the personal data you use to help the public judge their status and credibility. When you need to protect a source, you may still be able to provide some general information (eg about their status). You should not say anything inaccurate about a source's status.~~ NOTE: Delete as strays into editorial-decision making regarding what should be published.

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

Facts, opinions and context

~~7.14 You **should** clearly distinguish between fact and opinion when reporting personal data. Some programmes may involve a blend of factual and fictional elements about people, so you should make the extent of the facts clear.~~

NOTE: Delete as straying into editorial discretion and matters already covered by editorial codes. Would suggest it could be replaced with: It is always helpful to clearly distinguish between fact and opinion when reporting personal data.

7.15 You **could** consider how the words would strike the ordinary reasonable reader, taking into account their context and the subject matter when determining whether the personal data is a fact or an opinion. Opinions are subjective by their nature and not necessarily inaccurate simply because someone disagrees or it is later proven to be incorrect.

~~7.16 While deciding what editorial position to take when reporting the news, it is important to make sure you continue to present personal data 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, you **should** check that headlines are supported by the text.~~ NOTE: Delete as straying into editorial discretion and matters already covered by editorial codes.

7.17 If personal data is deliberately inaccurate and this is obvious from the context, such as satirical or parody articles, this is unlikely to breach the accuracy principle.

Complaints and corrections

7.18 You **must** help people to exercise their individual rights under data protection law (see Individual rights). You **should** be clear with people about how they get in touch with you if they believe you have published or broadcast inaccurate personal data about them, and how you will consider the issue (see Complaints, enforcement and investigations).

7.19 Recording inaccuracies and monitoring any recurring themes **could** help you to review your processes and make improvements where needed.

Updating personal data

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

updating your contacts book if someone tells you they have new contact details.

8. Use personal data for a specific purpose

At a glance

- You **must** use personal data for a specific purpose that is legitimate, clear and in line with your original purpose. NOTE: The term 'must' is inappropriate in respect of conditions that only apply if the journalism exemption does not. If the same language is used as when the provision is mandatory for everyone it will cause confusion.
- To comply with this principle, you **must** also use personal data fairly, lawfully and transparently and be accountable for how you use it.
- You can use data for another purpose, if it is in line with your original purpose.
- Keeping a news archive is part ~~of the end-to-end process~~ of journalism so there is no change in purpose.
- If you are using data for a purpose that is very different, unexpected or which would have an unjustified impact, this is not likely to be in line with this data protection principle. However, you **could** consider whether you could get consent to use the data for that purpose.
- **When the criteria applies, the journalism exemption can remove the usual requirement to use personal data for a specific purpose.**

In more detail

What does using personal data for a specific purposes mean?

8.1 You **must** use personal data for a specific purpose that is legitimate, clear and in line with your original purpose, or which is "compatible".

NOTE ON 8.1, 8.2 and 8.3: Code needs to be clearer that these obligations are subject to the exemption applying

8.2 This data protection principle is closely linked to other principles. To comply with it, you **must** also:

- be clear about why you are using the data (see Use personal data transparently);
- be able to demonstrate the steps you take to protect data, in particular by recording why you are using personal data (see Take steps to protect personal data); and

- use personal data fairly, lawfully and transparently, if you plan to use it for a new purpose (see Use personal data lawfully, Use personal data fairly, and Use personal data transparently).

How do we make sure that we use personal data for a specific purpose?

8.3 You **must** use personal data fairly, lawfully and transparently. If you do this, you are also likely to comply with the principle to use data for a specific purpose.

8.4 If you comply with your other obligations to be transparent and accountable, you are unlikely to need to do anything more to specify your purposes for using personal data. In particular:

- you **must** provide privacy information to people unless an exception applies; and
- if you have 250 or more employees, you **must** keep records about how you use personal data in line with legal requirements.

8.5 You **must** review how you use personal data and your privacy information to check that your purposes have not changed over time. Sometimes this can happen gradually, known as function creep. NOTE: There is no practical guidance here about how this should be done and with what frequency.

Using personal data for another purpose

8.6 You can use personal data for a new purpose, if it is in line with your original purpose.

8.7 Keeping personal data for a news archive or for defending journalism, whether in the courts or regulatory investigations, is still using personal data for journalism ~~because this is part of the end-to-end process~~.

8.8 Factors you **should** take into account when considering if you may use personal data for a new purpose include:

- any link between the original purpose and the new purpose;
- how you collected the information and the reasonable expectations of the people concerned;
- the nature of the personal data and any harm to people;
- how you have kept the data safe and how you will continue to keep it safe.

8.9 If you are using data for a purpose that is very different, unexpected, or which would have an unjustified impact on people, this is not likely to be in

line with this data protection principle. However, you **could** consider whether the person will consent to the new use (see Use personal lawfully).

9. Use no more personal data than you need

At a glance

- You **must** have enough personal data to do what you need to do and it **must** be relevant and not excessive. NOTE: Again since these provisions may be limited by the operation of the journalism exemption the ICO should not use the word 'must' or in each case qualify it in order to distinguish this obligation, which may be exempt, from those which cannot disapplied.
- Before you collect any personal data, you **should** think about why you need it.
- You **should** think about any factors people bring to your attention when exercising their rights that may suggest you are not using the right amount of personal data.
- You **must** use accurate personal data for journalism, which also involves considering how much data you need.
- You **should** keep in mind what you are trying to achieve and aim to collect the data you need to do that efficiently.
- You **must** use personal data that is relevant to your story or your wider journalistic purpose. Using irrelevant personal data, particularly sensitive types of data, can cause significant harm to people (eg discrimination).
- You **must** use personal data in limited ways (ie not use excessive data).
- You **should** think about whether you need to collect personal data and whether you also need to use it in other ways.
- You **must** review any data you keep from time to time to make sure you do not keep it for longer than you need to.
- **When the criteria applies, the journalism exemption can remove the usual requirement to use no more personal data than you need.**

In more detail

What does use no more data than you need mean?

9.1 You **must** have enough personal data to do what you need to do, and it **must** be relevant and not excessive. This is known as the data minimisation principle.

9.2 You **must** use personal data that is:

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

NOTE: Need to make it clearer that these requirements are subject to an exemption applying

How do we make sure that we use no more data than we need?

9.3 Before you collect any personal data, you **should** think about why you need it. This will help you to decide whether you will have enough data that is relevant to your story and not more than you actually need. NOTE: The code should make it clear that the ICO recognises that data-led investigations can involve large quantities of data and that it may not be clear for some time which data is going to be used in publications.

9.4 You **should** consider any factors people using their data protection rights bring to your attention about how much data you hold.

9.5 You **must** also review the data you hold from time to time (see Keep personal data only for as long as you need to).

Adequate data

9.6 You **must** use enough personal data to do what you need to do, or data that is adequate for your purpose.

9.7 You **must** use accurate personal data, which also involves considering how much data you need (see Use accurate personal data).

9.8 You **should** keep in mind what you are trying to achieve and aim to collect the data that you need to do that efficiently. For example, you **could** plan what questions you need to ask someone in an interview.

Relevant data

9.9 You **must** use personal data that is relevant. Even if personal data is not obviously relevant to a specific story, it can still be relevant to your wider journalistic purpose, but you **should** be able to justify this (see Keep personal data only for as long as you need it).

9.10 Using irrelevant personal data may cause significant harm to people. When using special category or criminal offence data in particular, you **must** only use the data that is relevant (see Use personal data lawfully).

Limited data

9.11 You **must** use personal data in limited ways that are not excessive. For example, you **could** consider the ways you are using personal data throughout the process of developing a story. Although you might have needed to collect a lot of data for background research, you are likely to be more selective about what data to publish.

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

At a glance

- You **must** keep personal data only for as long as you need it. NOTE: The term 'must' is inappropriate in respect of conditions that only apply if the journalism exemption does not. If the same language is used as when the provision is mandatory for everyone it will cause confusion.
- There are no specific time limits, so you **should** consider why you are using the data, amongst other factors, to help you decide how long to keep it.
- You **must** act lawfully and fairly when you use the data, so you **should** consider any legal risks and any risk of harm to a person associated with keeping or destroying it.
- Where possible and appropriate, you **must** record how long you expect to hold different types of data.
- You **could** have a retention policy or schedule to help you record standard retention periods, that you could incorporate into your existing processes.
- You **should** review the personal data you hold at appropriate intervals and erase or anonymise any data you no longer need.
- Research and background details, such as contacts, are vital to journalism so it may often be justifiable to keep this data for long periods of time or indefinitely.
- **When the criteria applies, the journalism exemption can remove the usual requirements to:**
  - **keep personal data only for as long as you need it in line with the data protection principle; and**
  - **inform the person concerned when you can demonstrate that the data does not identify them or no longer identifies them (ie it is anonymised and outside the scope of the UK GDPR).**

In more detail

- What does keep personal data only as long as you need to mean?
- How do we avoid keeping personal data for longer than we need to?

What does keep personal data only as long as you need to mean?

10.1 You **must** keep personal data only as long as you need to. There are no specific time limits so you **should** consider why you are using the data to help you to decide how long it is reasonable for you to keep it.

How do we avoid keeping personal data for longer than we need to?

10.2 How long it is appropriate to keep data for varies depending on the circumstances, however you **must** be able to justify how long you keep it.

10.3 You are in the best position to judge how long to keep personal data to achieve your journalistic purpose. Factors you **could** consider include:

- how likely you are to use the data in the future, taking account of the public interest;
- whether you may need to keep information to defend possible future legal claims;
- any legal or regulatory requirements (eg limitation periods for claims); and
- relevant industry standards or guidelines.

10.4 You **must** also consider the risk of harm to a person if you keep personal data. You **must** only keep personal data if it would be fair and lawful to do so.

10.5 You **must** record how long you expect to hold different types of personal data where possible and review this at appropriate intervals (see Take steps to protect personal data). You **could** use a retention policy or schedule to help you. NOTE: It would have been helpful if the ICO had included practical guidance here acknowledging that personal data may remain relevant in connection with journalistic investigations for many years and given this to be the case it is not always easy or relevant to attempt to record how long you are going to keep it.

10.6 Removing all traces of electronic data is not always possible so you **should** make sure that you put the data beyond use. If it is appropriate to delete data from a live system, you **should** also delete it from any back-up system.

What is the difference between anonymisation and pseudonymisation?

Anonymising personal data means that it is no longer in a form which allows people to be identified – either from that data or by combining it with other data. This means that the data is then outside the scope of the UK GDPR.

Pseudonymisation refers to techniques that replace, remove or transform information that identifies people and keeps that information separate. This is not the same as anonymisation. Data that has been pseudonymised is still personal data covered by data protection law.

Research and background materials

10.7 Research and background details, such as contact details, are vital to journalism, so it may often be justifiable to keep this information for long periods of time or indefinitely. You are the best judge about what you may need in the future based on your experience.

10.8 However, you **should** still review any data you decide to keep to make sure you still need it. For example, you may no longer need out-of-date contact details.

11. Be clear about roles and responsibilities

At a glance

- If you are dealing with personal data and any third parties, you **should** decide whether they are a controller, joint controller or processor under the UK GDPR. This affects legal responsibilities.
- To decide this, you **should** consider who decides why and how the data is used, known in the UK GDPR as a controller.
- If you ask a third party to help you with a story and they are permitted to act only on your instructions, they are a processor.
- You **must** have a written contract with processors and they must give you sufficient guarantees that they can comply with data protection law.
- If you are acting as a joint controller with a third party this means that you both determine the means and purposes of the using the data. You **must** have a transparent arrangement in place setting out your respective responsibilities.
- When sharing personal data, you **must** keep certain records to comply with the UK GDPR's requirements and carry out a DPIA if there is likely to be a high risk. You **could** also use a data sharing agreement.
- You **must** comply with data protection law if you receive personal data from a third party that you want to use. Relevant checks include confirming the source, how and when the data was collected, and checking its accuracy.
- The specific rules about making international transfers do not apply to online publication.
- **When the criteria applies, the journalism exemption can remove the usual requirements to comply with the general principles for restricted transfers of personal data to countries outside the UK or to international organisations.**

In more detail

What are the possible roles and responsibilities of different parties?

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

What is the difference between controllers, joint controllers and processors?

The key question is who determines why and how the personal data is used?

Controllers is a term used in the UK GDPR to describe the main decision-makers exercising control over the why and how personal data is used.

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

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

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

Decide whether a third party is a controller or a processor

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

11.3 For example, private investigators, freelance photographers and journalists are likely, in many cases, to be controllers in their own right. This is because they are likely to have a significant degree of independence to decide for themselves what is the most effective way of doing something, albeit they may still generally act in line with your instructions.

11.4 If acting as a joint controller, you **must** have means of arrangement ~~an agreement~~ with the other party or parties that sets out your respective responsibilities, particularly about transparency and individual rights. You **must** make this information available to people. NOTE: It should be made clear that this is subject to the exemption, the requirement to disclose such an agreement to a data subject could effectively destroy an investigation.

11.5 If you ask a third party to help you with a story and they are permitted to act **only** on your instructions, they are a processor, even if they make some technical decisions about how to use the data. NOTE: Please give practical examples of both joint controllers and processors in the journalism context in these paragraphs, as is done for controllers in 11.3

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

Data sharing with third parties

11.7 When sharing personal data between controllers, you **must** comply with the data protection principles. In particular, you **must** share personal data lawfully, fairly and transparently (see Use personal data lawfully, Use personal data fairly and Use personal data transparently). NOTE: These requirements should be stated as subject to the journalism exemption

11.8 You **should** consider our Data sharing code of practice to help you comply with the law and good practice when sharing personal data. This sets out that you **must** keep certain records about the sharing (see Take steps to protect personal data) and you **must** carry out a DPIA if needed (see Take steps to protect personal data).

11.9 You **could** also have a data sharing agreement with other parties to make sure the details are clear, especially if you are sharing data regularly, routinely or it is planned in advance.

Receiving personal data from third parties

11.10 You **must** comply with data protection law if you receive any personal data from another controller that you want to use, such as a freelance journalist or photographer. For example, you **must** make sure you use the data fairly, lawfully, transparently and carry out reasonable accuracy checks (see Use accurate personal data). NOTE: These requirements should be stated as subject to the journalism exemption

International transfers

11.11 The specific rules about making international data transfers do not apply to online publication, even if this makes information available outside the European Economic Union.

12. Help people to use their rights

At a glance

- People have specific data protection rights which they can exercise on request. You **must** help people to use these rights and respond within specific time limits. [NOTE: The term 'must' is inappropriate in respect of conditions that only apply if the journalism exemption does not. If the same language is used as when the provision is mandatory for everyone it will cause confusion.]
- You **can** refuse to comply with individual requests in certain circumstances, including if the request is manifestly unfounded or excessive.
- People can ask for copies of their data. You **should** make reasonable efforts to find relevant information and provide what you can to them.
- 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 such information.
- People can also object to your use of their data, ask you to restrict it or erase it in certain circumstances. If you have disclosed the data to others, you **must** tell them if the data is restricted or erased unless this is impossible or involves disproportionate effort.
- The right to erasure does not apply if using the data is necessary to protect the right to freedom of expression and information.
- If data is inaccurate, you **must** correct or complete it. NOTE: The ICO should make it clear when this applies. There is a public interest in maintaining archives that accurately record what was published at the time and not what happened later. It is also the case that data becomes inaccurate very quickly as it becomes out of date. this appears to impose an unlimited obligation to media organisations to correct these archives even though at the time of first publication the information that they contained may have been accurate. You **should** also consider whether you need to add a note to make sure your records are not misleading.
- There is a strong, general public interest in the preservation of news archives (including any user generated comment attached to any
- archived news reports), which contribute significantly to the public's access to information about past events and contemporary history. This is generally a strong factor in favour of not erasing personal data from or amending personal data within news archives.
- **When the criteria applies, the journalism exemption can remove the usual requirements to:**

- **confirm to the person whether you are using their data, provide access to their data as well as other information;**
- **inform the person when their data is transferred to a country outside the UK or an international organisation;**
- **provide the person with a copy of their personal data;**
- **comply with the right to have data completed or corrected, erased, or restricted and the right to object to use of personal data; and**
- **comply with the right to data portability.**

In more detail

What are individual rights?

12.1 Under data protection law, people have specific rights about 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
- rights related to automated decision-making, including profiling.

NOTE: It would be a missed opportunity not to refer to the ways in which the DPA can also be useful as a tool by journalists to obtain information.

12.2 We have focused below on the rights most likely to be relevant to journalism. See Use personal data transparently for information about the right to be informed.

How do we comply with individual rights?

Responding to requests

12.3 People can make requests in writing or verbally to use their rights. There are no specific requirements about how they should do this.

12.4 Generally, you **must** comply with a request without undue delay within one month of receiving it. However, you can extend the time to respond by a

further two months, if the request is complex or you have received a number of requests from the person to exercise their data protection rights.

12.5 You **should** have appropriate resources in place to enable you to handle requests and you **should** train staff about what to do if they receive one (See Take steps to protect personal data).

Refusals

12.6 You can refuse to respond to a request if an exemption applies, such as the journalism exemption. You may be exempt from providing an explanation for your response to the requester.

12.7 You can also refuse to comply with a request if it is manifestly unfounded or manifestly excessive. These provisions can help if you receive vexatious or harassing requests.

12.8 You **must** be able to justify any decision you take to refuse someone's request. The key point to consider is whether, objectively, the request would clearly have a disproportionate or unjustifiable impact. NOTE: Neither this code nor the surrounding notes provide examples of when this might apply. It is clearly relevant in cases such as where supplying the information to the person requesting it could tip that person off to the existence of an investigation. It might also apply where the disclosure of information would disclose the identity, whether directly or indirectly of the identity of a confidential source. This must be obvious because the wording used in the law is "manifestly". Factors you **could** consider include:

- whether the request has any serious purpose or value;
- what is the requester's motive;
- whether the request would impose an unreasonable burden on your resources; and
- if it involves any harassment of your staff.

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

12.10 If you refuse to comply with a request you **must** tell the requester:

- why you are refusing the request;
- 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

12.11 People have the right to ask you to:

- confirm that you are using their personal data;
- give them a copy of their personal data; and

- provide other supplementary information (often this will already be in a privacy notice which you may have on your website, so you can simply link to it).

12.12 You **should** make reasonable efforts to find relevant information and provide what you can to the requester. You can ask for clarification if you need to.

12.13 You **must not** give someone personal data about another person in response to an access request unless:

- the other person has consented (see Use personal data lawfully); or
- it is reasonable to disclose it without their consent.

12.14 ~~It is very unlikely that you would be~~ You will not be required to disclose information about confidential sources in response to a subject access request from another person. ~~In most cases,~~ A confidential source ~~is unlikely to~~ would not consent to the disclosure of their personal data to a third party. They also ~~are also likely to~~ have a strong expectation of confidentiality, which is reflected in the strong legal protection for journalistic sources. For example, sources are protected under the Contempt of Court Act 1981.

Right to restriction

12.15 People have the right to ask you to restrict the use of their personal data in certain circumstances:

- you have processed their personal data unlawfully and they have requested restriction rather than erasure (see Use personal data lawfully);
- they contest the accuracy of their personal data and you are verifying it (see Use accurate personal data);
- they object to your use of their data and you are considering whether your legitimate reasons override theirs (see Right to object); or
- you no longer need the data but the person concerned needs you to keep it for a legal claim.

12.16 You **must** be able to restrict personal data, if required. You **could** achieve this in different ways, for example:

- temporarily move the data to another system;
- make the data unavailable to users; or
- temporarily remove published data from a website.

12.17 Unless it is impossible or involves disproportionate effort, you must tell each recipient of the data that you have restricted it. If the person concerned wants to know who these recipients are, you **must** tell them.

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

Right to rectification (correcting or completing data)

12.19 People have a right to ask you to correct their personal data if it is inaccurate, or to complete it if it is incomplete. This is known as the right to rectification.

12.20 If you receive a request for rectification, you **should** take reasonable steps to check that the data is accurate. Factors you **should** consider include:

- what the requester tells you – they should be able to prove, on the balance of probabilities, that the information is inaccurate;
- any steps you have already taken to verify the accuracy of the personal data (see Use accurate personal data); and
- the risk of harm to the person.

12.21 If appropriate, you **could** restrict your use of the personal data while you check its accuracy even if the person has not specifically requested this.

12.22 If you are satisfied that the data is accurate, you **could** put a note on your internal system recording that the person challenges its accuracy, explaining why.

12.23 If necessary, you **must** correct or complete the data. Even if you took all reasonable steps to make sure the data was accurate at the time, if information later comes to light that suggests it may be inaccurate, you **should** reconsider and take steps to rectify it.

12.24 Opinions are subjective by their nature and not necessarily inaccurate simply because someone disagrees or it is later proven to be incorrect. However, if it becomes clear than an opinion was based on inaccurate data, you **should** correct it.

12.25 If an inaccuracy is only minor, such as a typographical error, it is usually reasonable to simply edit an online article to correct it. However, you **should** consider whether it is appropriate and proportionate to add a note to make sure that your records are not misleading. This may take a variety of forms, for example, an advisory line at the top of an online article, or a printed correction in a newspaper. Most typographical errors do not involve data protection issues.

12.26 Unless it is impossible or involves disproportionate effort, you **must** tell each recipient that you have rectified the data. If the person concerned wants to know who these recipients are, you **must** tell them.

12.27 If you have published the personal data in multiple locations, such as in print and online, you **should** consider what steps it is reasonable for you to take in each context. For example, on social media platforms, you **could**

encourage people who have shared the inaccurate information to help to circulate the correction.

Right to object

12.28 People have the right to object to the use of their personal data if you are relying on the legitimate interests lawful reason for using it (see Use personal data lawfully).

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

12.30 If someone objects, you **should** consider the reason carefully. However, you may be able to carry on using the data if your legitimate interests in using it are stronger than the person's in the circumstances.

12.31 If you have no reason to refuse the objection, you **must** stop using 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.

Right to erasure

12.32 People have the right to have their personal data erased without undue delay if:

- you do not need to keep the personal data for the purpose you originally collected or used it for;
- you are relying on the consent lawful reason, consent is withdrawn and there are no other legal reasons for using the data;
- a person objects to your use of the data (see Right to object) and there are no overriding legitimate reasons for using it;
- you have used personal data unlawfully (See Use personal data lawfully);
- you collected the data to offer online services to a child; or
- you need to erase the data to comply with a legal obligation.

12.33 You **must** give particular weight to any request for erasure if you are using data based on consent given by a child, especially for online services.

12.34 When personal data is made public, you **must** take reasonable steps to inform other parties with legal responsibility for using the personal data about the request. You **must** tell them that the person concerned has asked them to erase any links to the data or any copies or replication of it.

12.35 Unless it proves impossible or involves disproportionate effort, you **must** tell each recipient of the personal data that you have erased it. If the person concerned wants to know who these recipients are, you **must** tell them.

Protection for freedom of expression and information

12.36 Crucially, the right to erasure does **not** apply if using the data is necessary to exercise the right to freedom of expression and information. In practice, this is likely to be similar to balancing public interest considerations proportionately (see Apply the journalism exemption).

12.37 To help you determine whether you need to use the data to exercise the right to freedom of expression, you **should** take into account the factors used by the European Court of Human Rights when balancing these rights.

12.38 These factors are a guide and some may have more or less relevance, depending on the circumstances, including:

- how much the information contributes to a debate of public interest;
- how well known the person concerned is and the subject of the article;
- the prior conduct of the person (eg have they actively invited media attention?);
- how you obtained and verified the information;
- the content, form and impact of the publication; and
- whether the interference with the person's right to privacy is proportionate and justified in light of the above factors.

12.39 An offender may reasonably expect privacy as a result of the passage of time. You **should** take into account the strong public interest in the rehabilitation of offenders (See Use personal data lawfully).

12.40 You **should** take into account that information published online generally poses a higher risk to privacy because of the potential to reach a larger audience than print. This is particularly so when information is amplified by search engines.

News archives

12.41 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 strong factor in favour of not erasing personal data from or amending personal data within news archives.

12.42 Protecting the integrity of records is vitally important, so any steps considered necessary are unlikely to include erasing or deleting the actual record. For example, you may be required to anonymise a digital archive record so it does not appear in a search using someone's name, leaving the original record as it is and still accessible by less prominent means.

Information Commissioner's Office

Draft data protection and journalism code of practice

Reference notes

ico.
Information Commissioner's Office

Contents

These reference notes support the Data protection and journalism code of practice but they are not part of the statutory code itself. They contain:

Case law examples - These examples will help you understand how the courts have considered and applied relevant aspects of privacy law.

Although you should consider each law and case on its own merits, there are some similarities and general points that you may find helpful when you think about how to apply data protection law.

Key legal provisions - This lists the relevant sections of the UK General Data Protection Regulation (UK GDPR) and Data Protection Act (DPA 2018) relating to each part of the code.

Further reading – This lists more detailed ICO guidance and some external links for wider context which you can refer to, if you need more information.

About this code

Key legal provisions

- DPA 2018 section 124 - duty to prepare a journalism code of practice
- DPA 2018 section 125 – approval of codes
- DPA 2018 section 126 – publication and review of codes
- DPA 2018 section 127 - legal effect of the code
- DPA 2018 section 178 - review of processing of personal data for the purposes of journalism

NOTE: Suggest website links added to all sections of the DPA for easy access to the provisions referred to in these notes.

Further reading

Guide to the UK GDPR: key definitions provides more information about who the UK GDPR applies to, what personal data is and responsibilities.

The Equality and Human Rights Commission website has further information about human rights generally.

The European Court of Human Rights (EctHR) has also published detailed guidance on Article 10 and Article 8 of the European Convention of Human Rights.

Complaints, enforcement and investigations

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 NOTE: The code should set these out in full for journalists
- 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

Further reading

Data protection and journalism: how to complain about media organisations has more information about how to make complaints about media organisations, including details about court action.

ICO Regulatory action policy and statutory guidance on our regulatory action (currently in draft form following a public consultation).

ICO prosecution policy statement

1. Apply the journalism exemption

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, paragraph 26 – special purposes exemption for journalistic, academic, artistic or literary purposes
- DPA 2018 schedule 2, part 5, paragraph 26(5) – requirement for controller to take into account those listed industry codes relevant to the publication ~~specific industry codes~~
- DPA 2018 schedule 2 Part 5 paragraph 26(9) – provisions of the UK GDPR that can be disapplied by the special purposes exemption.

The exemption for journalism can remove the usual requirements to comply with the following parts of the UK GDPR listed in Schedule 2 Part 5 paragraph 26(9) of the DPA 2018:

- Article 5(1)(a) to (e) – the UK GDPR's principles, apart from the security principle and accountability principles
- Article 6 – requirement to satisfy a lawful basis for processing
- Article 7 – conditions for consent NOTE: These rules should be set out in full in this guide

- Article 8(1) and (2) – conditions for children's consent NOTE: These rules should be set out in full in this guide
- Article 9 – rules relating to special category data NOTE: These rules should be set out in full in this guide
- Article 10 – rules relating to criminal offence data NOTE: These rules should be set out in full in this guide
- Article 11(2) – specific rules regarding informing people when their personal data has been anonymised
- Article 13(1) to (3) – requirement to provide privacy information to people when you have collected data directly from the data subject
- Article 14(1) to (4) – requirement to provide privacy information to people 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

Case law examples

NOTE: GNM suggests that the notes explain that there is relatively little data protection case law / that the ICO considers the principles developed in a number of privacy/defamation cases may be of assistance as to how data protection law is interpreted.

Case example 1 – definition of journalism NOTE: Please cross refer each case example to the relevant paragraphs of the code. For instance, this case example is relevant to paragraphs 1.8-1.12 of the code, 'when are we using personal data for journalism?'

UK Supreme Court

Sugar (Deceased) v BBC and another [2012] UKSC 4

The court considered the meaning of journalism to decide whether the BBC was required to respond to a request under the Freedom of Information Act 2000. The wording for the derogation derives from data protection law.

The judge considered that journalism, art and literature is likely to include all types of "output" by the BBC to inform, educate or entertain the public. He added that because of the overlap between journalism, art and literature, there was unlikely to be value in a debate about whether journalism encompassed more than news and current affairs. (38)

However, the judge cautioned against tangential links when defining information held for the purposes of journalism: "…I would not be sympathetic to the notion that information about, for instance, advertising revenue, property ownership or outgoings, financial debt, and the like would normally be 'held for purposes…of journalism'"(84).

Another judge agreed that there should be a "sufficiently direct link" to journalism. (106)

Case example 2 – definition of journalism

High Court

NT1 & NT2 v Google LLC and ICO [2018] EWHC 799 (QB)

The judge in this case considered the meaning of journalism under the previous version of data protection law, which used similar wording.

He found that the operation of Google's search engine was for purposes other than journalism. He said:

"The concept [of journalism] extends beyond the activities of media undertakings and encompasses other activities, the object of which is the disclosure to the public of information, opinions and ideas…"

However, he also explained that "the concept is not so elastic that it can be stretched to embrace every activity that has to do with conveying information or opinions. To label all such activity as 'journalism' would be to elide the concept of journalism with that of communication. The two are plainly not the same…"(98).

Case example 3 – definition of journalism

European Court of Justice

Satamedia (Case C-73/07)

The European Court of Justice (ECJ) said the following about journalism:

"In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary, first, to interpret notions relating to that freedom, such as journalism, broadly" (56).

The court described journalism as an activity involving "the disclosure to the public of information, opinions or ideas" (61).

It added that, "…account must be taken of the evolution and proliferation of methods of communication and dissemination of information" (60).

Case example 4 – definition of journalism

European Court of Justice

Buivids (C-345/17)

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

The ECJ said that:

- Mr Buivids could not rely on the exemption in data protection law for personal and household use because he had published a video on You Tube without any restrictions;
- Mr Buivids could still be engaged in journalism, even though he is not a professional;
- although journalism is a broad concept, it did not extend to all information published on the internet; and
- in determining whether Mr Buivids is using 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.

Case example 5 – meaning of "with a view to publication"

High Court

Campbell v MGN Limited [2002] EWCA Civ 1373

In this case, the court considered the meaning of "with a view to publication" in the older version of data protection law.

The court said:

"…it would seem totally illogical to exempt the data controller from the obligation, prior to publication, to comply with provisions which he reasonably believes are incompatible with journalism, but to leave him exposed to a claim for compensation…the moment that the data have been published.

For these reasons we have reached the conclusion that, giving the provisions of the sub-sections their natural meaning…they apply both before and after publication". (120-121)

Case example 6 – meaning of "reasonable belief"

High Court

NT1 & NT2 v Google LLC and ICO [2018] EWHC 799 (QB)

The judge considered the meaning of "reasonable belief" under an older version of data protection law.

The judge said:

"Each of s.32(1)(b) and (c) has a subjective and an objective element: the data controller must establish that it held a belief that publication would be in the public interest, and that this belief was objectively reasonable; it must establish a subjective belief that compliance with the provision from which it seeks exemption would be incompatible with the special purpose in question, and that this was an objectively reasonable belief. That is the ordinary and natural meaning of the words used (and of the somewhat similar provisions of s.4 of the Defamation Act 2013…" (102)

Case example 7 – scope of editorial discretion

House of Lords

Campbell v MGN [2004] UKHL 22

In this case, the judge made the following comments about the scope of editorial discretion:

"There is no doubt that the presentation of material that it was legitimate to convey to the public in this case without breaching the duty of confidence was a matter for the journalists. The choice of language used to convey information and ideas, and decisions as to whether or not to accompany the printed word by the use of photographs, are pre-eminently editorial matters with which the court will not interfere. The respondents are also entitled to claim that they should be accorded a reasonable margin of appreciation in taking decisions as to what details needed to be included in the article to give it credibility. This is an essential part of the journalistic exercise.

But decisions about the publication of material that is private to the individual raise issues that are not simply about presentation and editing. Any interference with the public interest in disclosure has to be balanced against the interference with the right of the individual to respect for their private life. The decisions that are then taken are open to review by the court". (112-113)

Case example 8 – evidence to demonstrate decision-making

High Court

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 the 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 said, "…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". (131)

Case example 9 – Public interest and whether someone is a "public figure" or has a "role in public life"

European Court of Justice

Google Spain C-131/12

Working party guidance published to support this judgement may help you to decide whether someone is "a public figure" or has "a role in public life".

Role in public life

The guidance acknowledges that it is not possible to establish hard-fast rules about this, but it said:

"…by way of illustrating, politicians, senior public officials, business-people and members of the (regulated) professions can usually be considered to fulfil a role in public life…

A good rule of thumb is to [consider whether publication to the public]…would protect them against improper public or professional conduct".

Public figures

The guidance again acknowledges the difficulties of a set description of this sub-group of people. However, it said:

"In general, it can be said that public figures are individuals who, due to their functions/commitments, have a degree of media exposure.

The Resolution 1165 (1198) of the Parliamentary Assembly of the Council of Europe on the right to privacy provides a possible definition of 'public figures'. It states that, 'public figures are persons holding public office and/or using public resources and, more broadly speaking, all those who play a role in public life, whether in politics, the economy, the arts, the social sphere, sport or in any other domain'.

Case example 10 – public interest and proportionality

House of Lords

Campbell v MGN Ltd [2004] UKHL 22

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 published information revealed significant additional information, including that Miss Campbell was receiving treatment at Narcotics Anonymous, the details of her treatment, and a photograph of her leaving a meeting with others. The court said anyone who knew the locality would know where it was.

The Supreme Court found that there was not a sufficient public interest to justify the publication of this additional information, particularly bearing in mind that it was sensitive health data which could put Miss Campbell's recovery at risk.

~~Case example 11 – meaning of "incompatible with journalism"~~

~~First-Tier Tribunal~~

~~True Vision Productions (TVP) v ICO (EA 2019 0170)~~

~~This case before the First-Tier Tribunal concerned whether the ICO was correct to impose a monetary penalty. 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 on 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…"~~

NOTE: This is an Employment Tribunal decision and should not be used as an example.

Further reading

Guide to data protection: Children

Industry codes contain guidance about the public interest including:

Independent Press Standards Organisation (IPSO) Editors' Code of Practice;

BBC Editorial Guidelines;

Ofcom Broadcasting Code; and

IMPRESS Standards Code.

2. Take steps to protect personal data

Key legal provisions

- UK GDPR article 5, paragraph 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

Further reading

Guide to the UK GDPR: Accountability and governance

ICO Accountability framework

SME web hub – advice for all small organisations

DPIA template

DPIA screening checklist

3. Keep personal data secure

Key legal provisions

- UK GDPR article 5, paragraph 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

Further reading

Guide to the UK GDPR: Security

ICO Accountability framework

Working from home

Bring your own device – what should we consider?

SME web hub – advice for all small organisations

4. Use personal data lawfully

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 NOTE: These should be set out for ease of reference either in the main code or in these additional notes.
-
- DPA 2018 part 2 of schedule 1 – substantial public interest conditions for special category data NOTE: These should also be listed so that these document can stand alone without the necessity for recourse to other documents.

Case law examples

Case example 12 – Criminal investigations by the state ~~allegations under state investigation~~ and reasonable expectation of privacy

UK Supreme Court

Bloomberg LP v ZXC [2022] UKSC 5

This case concerned information based on a confidential letter of request from a UK law enforcement body. The claimant said that Bloomberg had misused his private information.

Although this case was not considered under data protection law, it is nonetheless relevant to the following:

- considering the requirement to use personal data fairly;
- when the legitimate interests lawful reason is used; and
- where relevant, when considering the special purposes exemption.

The court considered whether, in general, a person under criminal investigation has, prior to being charged, a reasonable expectation of privacy about information relating to that investigation. It set out the following:

- The legitimate starting point is that there is a reasonable expectation of privacy in the above circumstances.
- The reason for this is that publication of such information ordinarily causes damage to a person's reputation together with harm to multiple aspects of their private life. The harm and damage can on occasion be "irremediable and profound".
- The legitimate starting point is not a legal rule or legal presumption. It all depends on the facts.
- The claimant still has to prove that the circumstances mean there was a reasonable expectation of privacy.
- From the starting point, the court will consider whether the expectation did not arise at all, or was significantly reduced. If it is significantly reduced, that is factored into the balance of the public interest.

For the public interest, a weighty factor in the balance was the generally strong public interest in observing duties of confidence and the specific public interest in not prejudicing an ongoing criminal investigation.

This outcome is limited to circumstances where there is a state investigation.

Case example 13 – reasonable expectation of privacy and spent convictions

High Court

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 about 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".

Further reading

Guide to the UK GDPR: Lawfulness, fairness and transparency

Guide to the UK GDPR: Lawful basis for processing

Lawful basis interactive tool

Appropriate policy document template

Guide to data protection: Children

Age appropriate design code: a code of practice for online services

HM Courts and Tribunals Service: Reporter's Charter

College of Policing guidance: Authorised professional practice (APP) on Media Relations

5. Use personal data fairly

Key legal provision

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

Case law examples

Case example 14 – reasonable expectation of privacy

High Court

Murray v Big Pictures (UK) [2008] EWCA Civ 446

This case concerned a newspaper's publication of a photograph of Ms Murray's child taken as her family were walking in a public street (Ms Murray is better known as JK Rowling, author of the Harry Potter books).

The judge's comments in this case about misuse of private information have become part of general guidance to help assess whether a reasonable expectation of privacy exists. The judge said:

"…the question whether there is a reasonable expectation of privacy is a broad one, which takes account of all the circumstances of the case. They include the attributes of the claimant, the nature of the activity in which the claimant was engaged, the place at which it was happening, the nature and purpose of the intrusion, the absence of consent and whether it was known or could be inferred, the effect on the claimant and the circumstances in which and the purposes for which the information came into the hands of the publisher." (36)

Case example 15 – reasonable expectation of privacy and public figures

High Court

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 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."

Case example 16 – unwarranted intrusion NOTE: Same principle from the case also referred to in case example 10 - would suggest repetition is avoided.

House of Lords

Naomi Campbell v MGN Ltd. [2004] UKHL 22

Miss Campbell brought an action under the tort of misuse of private information about a newspaper which used a photograph of her in the street outside the place where she was receiving therapy for drug addiction.

It was not in dispute in this case that because Miss Campbell had presented a false image of herself by claiming she did not take drugs, the media were entitled to "set the record straight".

However, although the newspaper could justify publishing the facts that Miss Campbell had taken drugs and that she was seeking treatment, it was not justified in publishing any further information, especially if this might jeopardise the continued success of the treatment.

Further reading

Guide to the UK GDPR: Lawfulness, fairness and transparency

Guide to data protection: Children

6. Use personal data transparently

Key legal provisions

- UK GDPR article 5(1)(a) – the lawfulness, fairness and transparency principle
- UK GDPR articles 13 and 14 – right to be informed

Further reading

Guide to the UK GDPR: Lawfulness, fairness and transparency

Guide to the UK GDPR: Right to be informed

ICO Accountability framework

Guide to data protection: Children

7. Use accurate personal data

Key legal provisions

- Article 5(1)(d) – the accuracy principle
- Article 16 – the right to rectification
- Article 17 – the right to erasure

Case law examples

Case example 17 – Fact and opinion and link with defamation

High Court

Aven and Others v Orbis Business Intelligence Limited [2020] EWHC 1812 (QB)

In this case, which concerned a claim brought under the DPA 2018, the judge used principles from defamation law to consider a dispute about accuracy.

Reflecting on whether a statement is a fact or an opinion, the judge said:

"The DPA contains no guidance on this topic. But this is an issue that arises frequently in defamation cases. The principles are very well established and familiar to this court". He also said "I caution myself that this is not a libel action. But these principles are not technical matters, of relevance only to a niche area of the law. They reflect the experience of generations in analysing speech and striking a fair balance between the right to remedies for false factual statements, and the need to safeguard freedom of opinion".

He summarised the "core points" as follows:

- A key question is how the words would strike the ordinary reasonable reader.
- A comment is a deduction, inference, conclusion, criticism, remark, observation etc.
- Words must be looked at in their context along with the subject matter.

Other important factors may be whether the statement is capable of verification, and whether the words stand by themselves or accompany others.

Further reading

Guide to the UK GDPR – Accuracy

8. Use personal data for a specific purpose

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

Further reading

Guide to the UK GDPR – Purpose limitation

9. Use no more data than you need

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

Further reading

Guide to UK GDPR: Data minimisation

Guide to UK GDPR: Accuracy

Guide to UK GDPR: Fairness, lawfulness and transparency

Guide to UK GDPR: Storage limitation

Guide to UK GDPR: Right to rectification

Guide to UK GDPR: Right to erasure

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

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

Further reading

Guide to UK GDPR: Storage limitation

Guide to UK GDPR: Right to erasure

Guide to UK GDPR: Documentation

11. Be clear about roles and responsibilities

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

Further reading

Guide to UK GDPR: Key definitions – controllers and processors

Guide to UK GDPR: Accountability and governance

Data sharing information hub

Guide to UK GDPR: International transfers after the UK exit from the EU Implementation Period

International data transfer agreement and guidance

12. Help people to use their rights

Key legal provisions

- UK GDPR article 12 – requirements about providing information to people
- 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
- Contempt of Court Act 1981 Section 10 Sources of information

Case law examples

Case example 18 – Right of access and protection of journalistic sources

European Court of Human Rights

Goodwin v United Kingdom (1996) 22 EHRR 123

The European Court of Human Rights said in this case:

"Protection of journalistic sources is one of the basic conditions for press freedom…Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected.

Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect of an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest". (39)

Case example 19 – right to erasure (or right to be forgotten) and distinction between search engines and publishers of websites ~~third party publication of data~~

European Court of Justice

Google Spain C-131/12

This ECJ considered a person seeking to exercise their privacy rights about a search engine.

Although this case was about a search engine, it is important because it distinguished between use of personal data by the search engine and use of personal data carried out by publishers of ~~third-party~~ websites.

Working party guidance has further information about this judgment and the flexible criteria the court set out to help search engines decide whether "de-listing" of search results is appropriate.

Case example 20 – right to erasure (or right to be forgotten) and strong public interest in news archives

European Court of Human Rights

ML and WW v Germany [2018] ECHR 554

This case concerned someone who sought to exercise their "right to be forgotten" under human rights law about their murder conviction.

The ECtHR decided that it was not proportionate to require anonymisation of media reports.

The court recognised the strong public interest in the media and news archives. It also recognised the potential chilling effect of right to be forgotten requests.

Factors affecting this outcome included:

- There was considerable interest in the crime at the time. The applicants had also subsequently sought to reopen the case and had not even been granted parole when they commenced legal proceedings.
- The applicants had lodged every possible judicial appeal and had also directly contacted the press.
- The reports were fair and accurate.
- The dissemination of the reports was limited in scope because they were no longer available on the news pages of the websites and subject to restrictions such as paid access or subscription.
- The applicants had not attempted to contact search engine operators to further limit the availability of the information.

Case example 21 – Right to erasure (or right to be forgotten) and anonymisation of digital archive record

European Court of Human Rights

Hurbain v Belgium [2021] ECHR 544

A person was named as the cause of a fatal car accident. The person was convicted, served their sentence, and received a pardon. They subsequently sought to exercise their "right to be forgotten" under human rights law.

Given the facts of this specific case, the ECtHR decided that it was proportionate to ask the newspaper to anonymise only the digital archive record that was freely accessible through an online search, not the original article.

The court recognised the strong value of archives "…for teaching and historical research, as well as for contextualising current events". It also recognised that anonymising archives undermines their integrity. It urged domestic courts to be "particularly vigilant" about people seeking to anonymise or modify electronic archives.

Factors affecting the outcome in this case included:

- The information was of no topical value 20 years after the event and the person concerned had no public profile.
- The public interest in the rehabilitation of offenders.
- The person had not sought media attention.
- Online publication is much more likely to undermine the right to privacy than paper publication.

Further reading

Guide to UK GDPR: Individual rights

Guide to data protection: Children

1. Data protection is an important part of journalism

- Personal information, or data, often forms the heart of the stories you tell as a journalist. Whenever you use personal data, you need to comply with data protection law.

- Personal data is any information relating to an identifiable living person that is, or will be, kept on a digital device like a computer or in an organised way.

- You are already likely to be doing lots of the right things, particularly if you comply with industry codes and guidelines. Core journalistic values and data protection have a lot in common.

Data protection law focuses on seven key principles to:

- take steps to protect personal data;
- keep it secure;
- use it fairly, lawfully and transparently;
- use accurate personal data;
- use it for a specific purpose;
- use no more than you need; and
- only keep it for as long as you need it.

2. The key to getting data protection right is managing risk

- The more risk of harm there is, the more important it is that you can show the steps you take to protect people's personal data. [This wording is very abstract and unlikely to be helpful for a journalist]

- So, get to know how your organisation ~~protects~~ uses personal data from a journalistic perspective. Find out what processes your organisation has and how they relate to your use of personal data ~~need to follow~~. There may be specific policies or procedures to help you.

- Make sure that you understand your role and responsibilities as a journalist and ask if you need training or support.

- Follow the latest security advice, especially when working remotely or using portable devices. Report security breaches to your organisation.

Remember to take extra care if:

- there is a risk of discrimination, financial loss, damage to reputation, loss of confidence or ~~a risk of~~ physical harm arising from

your use of personal data;

- you are using sensitive types of personal data, particularly special category data revealing someone's race, political or religious beliefs, genetic data, health or sex life, or criminal offence data;

- you are using children's personal data, or data about other people who may be vulnerable. They may be less able to understand risk; or

- you are using ~~online material, especially~~ social media or other user-generated content. Inaccurate data can spread very quickly online and may even be deliberate disinformation. [NOTE: A lot of online material is reliable - for example, the websites of reputable news websites, the government, the ICO etc]

3. There is an exemption in data protection law to protect journalism

- In many cases, journalists will be complying with data protection law when routinely using personal data they consider necessary for their day to day journalism as they will be able to rely on the lawful basis of legitimate interests (see section 4 below)

- There is however also an exemption for journalism that can remove many, but not all, parts of data protection law. For example, you always need to show how you are complying and keeping personal data secure. The exemption applies if you:

  o ~~your organisation~~ intend~~s~~ to publish journalistic content;

  o~~ you~~ reasonably believe it is in the public interest; and

  o reasonably believe that complying with a ~~specific~~ part of data protection law would be impractical ~~is not possible or would unduly restrict journalism~~.

- If you use the exemption, then you~~r organisation~~ must be able ~~need~~ to show it applies. So, make sure you understand any process for using it, including who has authority to make the decision and if you need to keep a record. [NOTE: Not all journalism happens within an organisation.]

- Remember risk is key. The higher the risk, the more important it is that your organisation can show that it made the right decision. [This is very abstract and unlikely to be helpful for a journalist]

4. You need a specific lawful ~~legal~~ reason to use personal data

- Unless you are relying on the exemption, You must generally have a specific lawful ~~legal~~ reason for using personal data. There are six of these in data protection law.

- 'Legitimate interest' is often the most appropriate lawful ~~legal~~ reason for you to use personal data for journalism. There is a legitimate interest in journalism because of the special public interest in freedom of expression and information. It is a good place to start when considering which one applies. It allows you to use ~~collect~~ personal data if you are pursuing a legitimate interest ~~there is a public interest in collecting the data~~ which is stronger than the harm to a person.

- Consent is also a well-known but often misunderstood legal reason. It is only relevant if you are giving someone genuine choice and control, including the right to withdraw consent at any point.

- You generally need stronger legal reasons for using sensitive types of personal data, known as special category and criminal offence data (see above). These are set out in data protection law as specific conditions.

5. Use personal data fairly ~~in ways people would reasonably expect and which are in the public interest~~

- Applies unless you are relying on the exemption

- You must generally use personal data fairly. This generally means using it in ways people would reasonably expect and which do not cause unjustifiable harm.

- Various factors may be relevant, including whether:
  - information is already publicly available;

- the person concerned has a public profile – although you always need to consider all the circumstances;and
- the risk of harm to the person.

- People may reasonably expect privacy in a public place, so even if an activity takes place in public, make sure you still consider the risk of harm.

- Ultimately, be guided by what's in the public interest. ~~What is in the public interest~~ This involves considering the strength of factors for and against publication and deciding how to best serve the public interest in a balanced way.

6. Be clear and open with people about how you use their personal data when you can

- Applies unless you are relying on the exemption

- Your organisation must generally tell people about their use of personal data by providing specific privacy information.

- Privacy information must be easy to access and understand, especially for children. Organisations often provide it in a privacy notice on their website, but you still need to make people aware of it. [Is this relevant to journalism?]

- Your organisation does not need to provide privacy information in certain cases, for example if:
  o it is not possible;
  o It would be disproportionate; or
  o it would seriously prejudice your aim.

- Ask your organisation if you are not sure:
  o if it is ok to collect personal data;
  o how and when to provide privacy information; or
  o whether you should do so in particular circumstances.

7. Carry out reasonable accuracy checks

- How far you go to check the accuracy of personal data is likely to vary ~~varies~~ depending on different factors, including the type of source you use and the risk of harm to a person. The greater the risk of harm, the more careful you need to be.

- Even if your story seems routine and you are on a tight deadline, you generally must still carry out reasonable checks. [NOTE: Generally added given the final bullet acknowledging accuracy checks may not always be possible, for example during a live broadcast]

- ~~Distinguishing between fact and opinion in respect of personal data is an important part of making sure the data you use is accurate.~~ [NOTE: This strays into editorial discretion and should be omitted]

- If your normal accuracy checks are not possible, make sure you understand how your organisation expects you to manage the risk of using potentially inaccurate data.

8. Use the right amount of personal data and only keep what you need

- Applies unless you are relying on the exemption

- ~~When time is limited, only~~ Use the right amount of personal data to write your story~~.~~, making sure it is relevant and not excessive. This helps you to ~~be more efficient and~~ comply with data protection law.

- But sometimes not having enough data is the issue – ~~remember you need to make~~ you should be sure you have enough data for an accurate story.

- Using irrelevant data, particularly sensitive types of personal data (see above) such as details of someone's religion or ethnicity, may increase the risk of harm to them ~~discrimination~~.

- ~~Once you put your story together, consider whether there's any data that you no longer need to keep.~~ Only keep personal data for as long as you need it. There's no specific time limit in the law, but ~~you must not keep personal data longer than you need to~~. ~~Y~~your organisation may have its own rules about this.

9. Data protection law provides a safe legal framework for you to share data with others

- Applies unless you are relying on the exemption

- When people are acting on behalf of your organisation and they are permitted to act **only** on your instructions, ~~such as freelancers or photographers~~, you must have a written contract in place guaranteeing that they will also protect the personal data. [NOTE: Freelancers/photographers are likely to be controllers rather than processors (see 11.3 of the second draft Code)]

- You may also work with ~~other~~ people who have a significant degree of independence, such as freelancers or photographers ~~the same responsibilities for protecting data as your organisation~~. When acting ~~this is done~~ jointly, you should ~~need to~~ have a transparent arrangement ~~agreement~~ in place between everyone explaining who does what.

- If other people share personal data with you, for example sources for a story, you still generally need to comply with data protection law if you want to use the data. ~~This is unless the journalism exemption applies (see Tip two).~~ [Strange to have this reference to the JE given that the exemption may apply to many of the other obligations set out above]

- There are specific rules about international transfers.

10. Help people to exercise their data protection rights

- People have specific rights under data protection law, including the right to ask for access to their data and to ask you to amend, erase or correct it. You must help people to use their rights and know what to do if you get a request.

- In some circumstances you can refuse a request. For example, if an exemption applies, such as the journalistic exemption, or if the request is manifestly unfounded or excessive.

- There is strong legal protection for confidential sources, so it is very unlikely you would ever have to disclose ~~someone could access~~ this

type of data.

- The right to erasure does not apply if using the data is necessary for freedom of expression and information. For example, the strong public interest in news archives and the vital contribution archives make to public knowledge is generally a strong factor in favour of not erasing data.

  Need more help? Contact us or read the data protection and journalism code of practice.