

# 10 data protection tips for day-to-day journalism

This quick guide includes tips to help you comply with data protection law and good practice in day-to-day journalism.

## 10 data protection tips for day-to-day journalism



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.
- So, get to know how your organisation protects personal data. Find out what process you need to follow. There may be specific policies or procedures to help you.
- Make sure that you understand your role and responsibilities 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;
- 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.

## 3

### There is an exemption in data protection law to protect journalism

- There is 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:
  - your organisation intends to publish journalistic content;
  - you reasonably believe it is in the public interest; and
  - reasonably believe that complying with a specific part of data protection law is not possible or would unduly restrict journalism.
- If you use the exemption, then your organisation must be able to show that 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.
- Remember risk is key. The higher the risk, the more important it is that your organisation can show that it made the right decision.

## 4

### You need a specific legal reason to use personal data

- You must generally have a **specific legal reason** for using personal data. There are six of these in data protection law.
- 'Legitimate interest' is often the most appropriate legal reason for you to use for journalism. It is a good place to start when considering which one applies. It allows you to collect personal data if 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 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 in ways people would reasonably expect and which are in the public interest

- You must generally use personal data fairly. This 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 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 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

- 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.
- Your organisation does not need to provide privacy information in certain cases, for example if:
  - it is not possible;
  - It would be disproportionate; or
  - it would seriously prejudice your aim.
- Ask your organisation if you are not sure:
  - if it is ok to collect personal data;
  - how and when to provide privacy information; or
  - whether you should do so in particular circumstances.

## 7

## Carry out reasonable accuracy checks

- How far you go to check accuracy 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 must still carry out reasonable checks.
- Distinguishing between fact and opinion in respect of personal data is an important part of making sure the data you use is accurate.
- 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

- When time is limited, only use the right amount of personal data to write your story. 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 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 discrimination.
- Once you put your story together, consider whether there's any data that you no longer need to keep. There's no specific time limit in the law, but you must not keep personal data longer than you need to. 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

- When people are acting on behalf of your organisation, such as freelancers or photographers, you must have a written contract in place guaranteeing that they will also protect the personal data.
- You may also work with other people who have the same responsibilities for protecting data as your organisation. When this is done jointly, you need to have a transparent 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 need to comply with data protection law if you want to use the data. This is unless the journalism exemption applies (see Tip two).
- 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 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.