Data protection and journalism: a quick guide

Please note: The following information has not been updated since the Data Protection Act 2018 became law. Although there may be some subtle differences between the guidance in this document and guidance reflecting the new law – we still consider the information useful to those in the media.

Data protection basics

- The DPA will apply whenever media organisations collect, use or keep any information about a living person – even if it's not 'private'.
- There are eight main principles of the DPA that organisations should comply with (see box) but these are flexible enough to accommodate many day-to-day journalistic practices.
- The media's journalistic uses of personal information can be exempt, if publication is in the public interest and compliance would be incompatible with journalism (see box).

Who is responsible for compliance?

- The 'data controller' is legally responsible and would be subject to any enforcement action. Generally this will be a media organisation not an individual journalist – but freelance journalists and bloggers are likely to have obligations. However, in practice anyone acting on its behalf (eg employees) will need to comply.
- Individual journalists can commit a criminal offence if they obtain information unlawfully in breach of section 55 (see box on next page).

Obtaining information

- Be open and honest wherever possible. People should know if you are collecting information about them or from them, where it is practical and wouldn't undermine the journalistic activity.
- Only use covert methods if you are confident that this is justified in the public interest.

Summary of the data protection principles

1. Collect and use information about people fairly and lawfully, without **unwarranted** harm or intrusion into their private life
2. Don't use the information for any other incompatible (ie non-journalistic) purposes
3. Ensure the information is adequate, relevant and not excessive for your purpose
4. Ensure the information is accurate and (where necessary) kept up to date
5. Don't keep it for longer than necessary
6. Comply with individuals' rights (eg to access their information, or to object)
7. Keep the information secure
8. Don't send it to anyone outside the EEA without adequate protection

The section 32 exemption for journalism

- Can exempt the media from most provisions, in appropriate cases - but never principle 7 (security) or the section 55 offence.
- The only purpose must be journalism (or art or literature), with a view to publication.
- The data controller must reasonably believe publication is in the public interest, taking into account the general public interest in freedom of expression, any specific public interest in the subject, and potential harm to individuals.
- The data controller must reasonably believe compliance is incompatible with journalism – ie it would be unreasonable or impractical to comply. This must be more than just an inconvenience.
- We expect media organisations to be able to explain why the exemption is required in each case, and how and by whom this was considered at the time. The ICO does not have to agree with the organisation's view – we must be satisfied that they had a reasonable belief.

- Only collect information about someone's health, sex life or criminal behaviour if you are confident it's relevant and the public interest in doing so sufficiently justifies the intrusion into their privacy.

The section 55 offence

- It is a criminal offence to knowingly or recklessly obtain (or disclose) personal data from a data controller without its consent.
- This can cover obtaining information about someone by deception (blagging), hacking, exploiting poor security, or unauthorised leaks.
- There is currently no specific defence for journalists, but there is a public interest defence.
- The ICO will only prosecute if this is in the public interest, taking into account the special importance of freedom of expression and a free and independent media. In particular, we recognise the importance of unauthorised leaks to journalists in the public interest.
- The penalty is currently limited to a fine.

Publication

- Consider what personal information it is fair to publish. Balance how much personal information you need to publish in order properly to report the story against the level of intrusion into the individual's life and the potential harm this may cause.
- The public interest in publication should be considered at an appropriate level. Depending on the nature of the story, you may need senior editorial input into the decision.

Subject access requests

- Individuals can make a written request to find out what information a data controller holds about them, where it was obtained from, and ask for copies of the information.
- The data controller must consider whether information (or some of it) can be provided without undermining its journalistic activities. The journalism exemption can be applied to refuse the request if providing the information would be incompatible with journalism (see box on previous page.
- Information about other people only needs to be supplied if that individual consents or it is reasonable to supply it without that consent.

Accuracy

- Following existing journalistic practices that enable journalists to distinguish clearly between fact, opinion and speculation will enable compliance with the DPA.
- We expect reasonable steps to be taken to check facts and record personal information correctly.
- If the individual disputes the facts, say so. If the published story is later shown to be inaccurate, records should be updated to avoid repetition and online archives should have a correction attached.

Security

- You must keep information about people secure by taking reasonable steps to stop it being lost, stolen or misused.
- You need to be particularly aware of security when you are out of the office with documents, phones, tablets, laptops or memory sticks containing personal information.
- Make sure you are aware of and follow your organisation's security policies and procedures. Information should be locked, password protected or encrypted.

Retaining information

- The DPA doesn't stop you keeping useful personal information as long as it was obtained legitimately.
- There are no set time limits in the DPA about how long people's information can be kept, but you should review the information from time to time to ensure it's still relevant and up to date and delete any you no longer need.

Confidential sources

- The DPA requires you to protect the identity of individual sources.
- You only have to disclose information from or about individual sources if that individual consents or it is reasonable to do so.
- If your source is an organisation and not an individual you would need to rely on the exemption for journalism to withhold its identity when it's not appropriate to disclose it (see box on previous page).