Information Commissioner's Office

Data protection and journalism code of practice

Reference notes

ico.
Information Commissioner's Office

Contents

How do these reference notes help us?

These reference notes support the Data protection and journalism code of practice (the code), but they are not part of the statutory code itself. They cover each section of the code and use the same numbering as the code to make cross-referencing easier. They contain, where relevant:

Further details about the legislation

These notes set out legislative wording more fully, as appropriate. However, they are not exhaustive and do not set out all the legislative requirements. They refer to key provisions if you need further detail about what the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) say.

Further good practice and reading

These notes include some examples of good practice to help you consider some different ways to comply. There are likely to be various other ways you could also comply. The notes also refer to some further information from our UK GDPR guidance and resources intended to help you understand and comply with the code without necessarily having to refer to our wider guidance. However, this is not exhaustive. Further reading is below if you need more detail.

Case law examples

These notes include some case law examples to help you understand how the courts have considered data protection and privacy issues in areas relevant to the code. Although not all personal information is private, privacy is an important part of data protection law.

Where considered relevant and helpful, the case law examples cover:

- data protection law, including the previous data protection regime;
- misuse of private information actions; and
- human rights law.

You should consider each privacy law and case outcome separately on its own merits, but you may nonetheless find these examples help you to understand and apply the code.

1. About this code

1.1 Statutory code of practice

The DPA says that we must prepare a code of practice to help people comply with data protection law and good practice when using personal information for journalism.

If someone complains about how you have used their personal information, the ICO, courts and tribunals must take this code into account once it is in force, where relevant.

Courts and tribunals will generally follow the guidance in statutory codes of practice and give weight to it unless there is a good reason not to do so.

If you do not do what this code says you should do, you will need to be able to persuade us or the courts that you have nevertheless complied with the law.

Data protection law

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

Data protection law applies to organisations using personal information that operate within the UK. It also applies to organisations outside the UK that offer goods or services to people in the UK.

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

1.2 Code's application

The code is mainly for media organisations and journalists using personal information for journalism. 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 senior management 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 information for journalism, including journalists.

We also recognise that journalism is not limited to media organisations or the journalists they employ. The code also applies more broadly to other groups and

people, including campaign groups or members of the public using personal information for journalism.

Using personal information

Personal information does not need to be private. Anything about a person can be personal information – even information that is public knowledge or about someone's professional life (eg a job title).

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

Information is not personal information 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 information.

In the code, we refer to personal information, which means the same as "personal data" in data protection legislation. We also refer to "using" personal information in the code. This means the same as "processing" it in the legislation. Using personal information means anything that you do with it, including collecting, recording, storing, publishing, sharing or deleting it.

1.3 Code's relationship with industry codes

Media standards are covered by other industry codes including:

- Editors' Code of Practice;
- IMPRESS Standards Code;
- BBC Editorial Guidelines; and
- Ofcom Broadcasting Code.

This code is generally well-aligned with industry codes and is designed to complement industry guidance. Core journalistic values and data protection have a lot in common so complying with industry codes will help you to comply with data protection law. Where relevant to data protection, we will take industry codes of practice into account and work with industry bodies as appropriate.

1.4 Data protection principles

Data protection law, and this code, focuses on seven key principles to:

- take responsibility for complying with the principles and be able to demonstrate how you comply;

- keep personal information secure;
- use personal information lawfully, fairly and transparently;
- use accurate personal information;
- use personal information for a specific purpose;
- use only the personal information that you need; and
- keep information only for as long as you need it.

1.7 Review

We must review how personal information is used for journalism under the DPA 2018. The first review period began on 25 May 2018 and ran for four years. We must begin a review within six months from the end of the first review period and submit a report to the Secretary of State within 18 months from when the review was started. Subsequent review periods are five years long.

These periodic reviews will inform the code in due course and help us to evaluate how it is working in practice. We will also keep the code under general review and update it where necessary in line with changes to law, guidance or other relevant developments.

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

Further reading

Personal information: what is it? provides more information about who the UK GDPR applies to, what personal information is and responsibilities.

2. Demonstrate how you comply

2.1 The journalism exemption

Even if you apply the journalism exemption to one of the data protection principles, this only means that you are not required to comply with the principle in the circumstances of the particular case. You **must** still be able to demonstrate in general how you comply with the principle.

When you use the journalism exemption, you **must** be able to demonstrate that you comply with the relevant criteria (see Apply the journalism exemption).

2.3 Wider context

Examples of the wider context include:

- the size of your organisation;
- its overall structure;
- the resources available to you; and
- your ways of working.

Harm

The harm to people's rights and freedoms can vary in degree and type. In line with damages, as described in Article 82 of the UK GDPR, harms can include:

- Physical harm (physical injury or other harms to physical health);
- Material harm (harms that are more easily monetised such as financial harm) or
- Non-material harm (less tangible harms, such as emotional or mental distress).

This means that harm can arise from actual damage or more intangible harms, including any significant economic or social disadvantage. Of course, harms may fall into more than one of these categories.

There may also be a harmful impact on wider society. For example, loss of public trust in journalism and the vital public interest role it serves in a democratic society.

2.4 Integrating data protection

Integrating data protection into your normal, day-to-day practices is sometimes called taking a "data protection by design and by default" approach.

This includes:

- implementing the data protection principles effectively;
- protecting individual rights; and
- using only the personal information that you need.

2.5 Proportionate data protection policies

It is more likely to be proportionate to have data protection policies in environments where there is significant delegation from the top and where decisions are often made at pace, such as news environments.

What your policies cover and their level of detail will vary depending on what you think is proportionate.

For example, a policy (either standalone or part of another policy) could help people understand how to use the journalism exemption, which might include:

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

2.6 Data Protection Officer

Under the UK GDPR, you **must** appoint a DPO if:

- you are a public authority or body (except for courts acting in their judicial capacity);
- your core activities require large scale, regular and systematic monitoring of people (for example, online behaviour tracking); or
- your core activities consist of large scale use of special category or criminal offence data.

This applies to most large organisations. If you are not sure, you can use our interactive tool below to help you decide.

2.7 Limited exemption for smaller organisations

Smaller organisations with fewer than 250 employees only need to record when they use personal information 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.

2.8 Data Protection Impact Assessments (DPIA)

You **must** always do a DPIA when you use personal information in ways specified by the UK GDPR which are deemed to be high risk. These are:

- Systematic and extensive use of personal information using automated means with significant effects (eg profiling).
- Large scale use of special category or criminal offence data.
- Systematic monitoring of a publicly accessible area on a large scale.

You **must** also do a DPIA if the way you want to use personal information is on the list we have produced under Article 35(3) of the UK GDPR. There are also European guidelines with some criteria to help you identify other uses of personal information that are likely to result in a high risk (see further reading below)

As well as doing a DPIA when there is likely to be a high risk, you **could** also do a DPIA for any other major project involving personal information.

If you are not sure whether to do a DPIA, you can use our screening test in the Further reading below.

2.11 Assessing risk

Assessing the risk involves considering how likely it is that using personal information will cause harm and how severe any harm could be.

2.12 Significant risks

Examples of other significant risks include:

- stopping people from accessing their rights or controlling their personal information;
- using sensitive types of personal information known as special category data or criminal offence data;
- physical harm;
- using personal information of people who are more at risk of harm, especially children; or
- using a large amount of personal information affecting a large number of people.

2.14 Approach to implementing data protection measures

Governance is often the name given to the framework of measures organisations use to comply with data protection and hold people to account appropriately.

There are lots of different ways of doing this but you could consider adapting our Accountability framework (see below). This indicates the main building blocks of an effective governance system or privacy management programme.

Smaller organisations are more likely to benefit from a smaller scale approach, using our dedicated resources below.

2.16 Training and awareness raising

Data protection training includes induction and refresher training, tailored appropriately to someone's role.

For example, ways to raise awareness of data protection include:

- creating quick-reference guides;
- running internal campaigns; or
- drawing attention to important information through your usual internal communication channels.

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

UK GDPR guidance and resources: Accountability and governance

ICO Accountability Framework

SME web hub – advice for all small organisations

Do I need a DPO? Interactive tool

Examples of processing 'likely to result in a high risk'

DPIA template

DPIA screening checklist

3. Keep personal information secure

3.13 Travelling with personal information

If you are travelling with personal information, fundamental security advice includes:

- 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 you are not using it.

Common security issues when travelling

Common security issues when travelling with personal information include:

- discussing confidential information;
- allowing people to overlook a screen; and
- writing down or telling someone your password.

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

UK GDPR guidance and resources: 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 information lawfully

4.1 Six lawful bases

The six lawful bases available are:

- legitimate interests;
- consent;
- contract;
- legal obligation;
- vital interests; and
- public task.

4.13 Journalism relating to unlawful acts and dishonesty condition

This condition applies if special category data is **disclosed** for journalism by the person with legal responsibility for complying with data protection law **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.

A person with legal responsibility for personal information can disclose it to you for journalism if they:

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

4.14 Appropriate policy document

An appropriate policy document is a short document outlining:

- the schedule 1 condition (or conditions) you are relying on;
- your procedures for complying with each of the data protection principles;
- your retention and deletion policies; and
- an indication of the retention period for the specified personal information.

Key legal provisions

- UK GDPR article 5(1)(a) – the lawfulness, fairness and transparency principle
- UK GDPR article 6 – lawfulness of processing

- UK GDPR article 9 – processing of special category data
- UK GDPR article 10 – processing of criminal offence data
- UK GDPR articles 13 and 14 – right to be informed
- UK GDPR article 17(1)(d) – right to erasure when personal data has been processed unlawfully
- DPA 2018 Schedule 1, paragraphs 1-37 – conditions for processing criminal offence data
- DPA 2018 part 2 of schedule 1 – substantial public interest conditions for special category data

Further reading

UK GDPR guidance and resources: Lawfulness, fairness and transparency

UK GDPR guidance and resources: A guide to lawful basis

Lawful basis interactive tool

Appropriate policy document template

UK GDPR guidance and resources: Children's information

UK GDPR guidance and resources: Introduction to the Children's code

HM Courts and Tribunals Service: Reporter's Charter

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

5. Use personal information fairly

5.6 Factors to help consider reasonable expectations of privacy

If you are not sure whether someone has a reasonable expectation of privacy, general factors considered by the court in misuse of private information actions may help you. The court typically considers:

- 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 information;
- the absence of consent and whether it was known or could be inferred;
- the impact on the person; and
- how and why you obtained the information.

These factors are not exhaustive, and their significance varies from case to case, but they are regularly applied by courts as guidance.

Information already in the public domain

To consider the impact of any information that is already in the public domain, you may find it helpful to consider:

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

When you are considering whether the information may be private, the extent to which it is in the public domain is generally an important factor. However, information does not necessarily lose its private character because the person concerned (or another person) has already disclosed, or intends to disclose, personal information about the same or similar parts of their life.

5.14 Naming a suspect in police investigations

The College of Policing guidance says the following about identifying suspects in a police investigation:

> "Suspects should not be identified to the media (by disclosing names or other identifying information) prior to the point of charge, except where justified by clear circumstances, such as a threat to life, the prevention or detection of crime, or a matter of public interest and confidence".

Allegations of criminal activity

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).

5.16 Children

The Convention on the Rights of the Child, which was ratified by the UK in 1991, is a treaty designed to promote the protection of children worldwide.

Article 3 says:

"In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration".

Case law examples

Case example 1 – Data Protection Act 1998 (DPA 1998) - reasonable expectation of privacy (paragraph 5.6 of the code).

Court of Appeal

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 2 – DPA 1998 - Spent convictions (paragraph 5.13 of the code).

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".

Case example 3 – Misuse of private information - Criminal allegations under investigation by the state, reasonable expectation of privacy, and professionals and business people (paragraph 5.14 and 5.22 of the code).

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 information fairly;
- when the legitimate interests lawful basis is used; and
- where relevant, when considering the journalism exemption.

The court considered whether, in general, a person under criminal investigation by the state 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.

The court was clear that this case is:

"…confined to the impact of information derived from an investigation of a person by an organ of the state rather than the distinct and separate situation that might arise if Bloomberg wished to publish information as to the results of its own investigations." (78)

Case example 4 – Data Protection Directive 95/46/EC - whether someone is a "public figure" or has a "role in public life" (paragraph 5.23 of the code)

European Court of Justice (ECJ)

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 5 – Misuse of private information and DPA 1998 - Public figures and reasonable expectation of privacy (paragraph 5.23)

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 across 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 6 – Misuse of private information – arrest in a public place (paragraph 5.27)

High Court

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

This case concerned the arrest of a suspect in the investigation into the terrorist attack at the Manchester Arena in 2017. In line with standard practice, the police did not name the suspect, but he was named by a newspaper.

The newspaper largely relied on the argument that someone who was arrested in "a high-profile police operation in the middle of a small town would stand little

expectation of privacy given the speed at which a story like this would spread around local residents." (89)

The court referred to the action against Bloomberg by ZXC (see case 3 above). It referred to the general principle that a person under criminal investigation by the state has, prior to being charged, a reasonable expectation of privacy about information relating to that investigation. It said that the court had made clear in different decisions that:

"…there may be exceptions to the general rule, which stands 'not as an invariable or unqualified right to privacy during an investigation but as a legitimate starting point'…Factors that might defeat the legitimate expectation were identified in ZXC." (86) The court gave examples, including:

- the public nature of the activity under consideration (eg rioting); and
- a decision by the police for operational reasons to reveal a suspect's name.

The court also said that "…it may accordingly be too much for a person arrested at his home to expect his neighbours to stay silent, and not to gossip amongst themselves…and yet entirely reasonable for that same person to expect that a media publisher will refrain from reporting his identify as a suspect online, in permanent form, to tens of millions of strangers." (93)

Key legal provision

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

Further reading

UK GDPR guidance and resources: Lawfulness, fairness and transparency

UK GDPR guidance and resources: Children's information

6. Use personal information transparently

6.1 Privacy information

Privacy information includes:

- why you are using the personal information;
- your lawful basis for using the information;
- who you will share it with;
- how long you will keep it for;
- details about people's rights.

You can read a full checklist of the privacy information you **must** provide in our UK GDPR guide and resources below.

6.3 Exceptions to providing privacy information

When you obtain personal information 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 information; or
- you are subject to an obligation of professional secrecy regulated by law that covers the personal information.

6.13 Ways to provide privacy information

There are different ways to provide privacy information, including for example:

- a layered approach;
- dashboards;
- just-in-time notices;
- icons; and
- mobile and smart device functionalities.

6.14 Privacy notices for children

In the case of children, it is even more important to present the information clearly and in an age-appropriate way. For example, graphics, cartoons and videos to appeal to children.

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

UK GDPR guidance and resources: Lawfulness, fairness and transparency

UK GDPR guidance and resources: Right to be informed

ICO Accountability framework

UK GDPR guidance and resources: Children's information

7. Use accurate personal information

7.4 Monitoring complaints and recurring themes

Recording inaccuracies and monitoring any recurring themes may help you to review your processes and make improvements, where needed.

7.10 Reasonable accuracy checks under time pressure

There may be circumstances when you decide that it is in the urgent public interest to publish personal information without carrying out normal accuracy checks.

If you are not able to carry out your usual accuracy checks because there is an urgent public interest, relevant factors for you to consider may include:

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

Simple accuracy checklists may help you to check personal information is accurate when you are working at pace.

Case law examples

Case example 7 – DPA 1998 - Fact and opinion (paragraph 7.7 of the code)

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.

Key legal provisions

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

Further reading

UK GDPR guidance and resources: Accuracy

8. Use personal information for a specified 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

UK GDPR guidance and resources: Purpose limitation

9. Use only the personal information 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

UK GDPR guidance and resources: Data minimisation

UK GDPR guidance and resources: Accuracy

UK GDPR guidance and resources: Fairness, lawfulness and transparency

UK GDPR guidance and resources: Storage limitation

UK GDPR guidance and resources: Right to rectification

UK GDPR guidance and resources: Right to erasure

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

10.3 Recording how long to keep personal information

A retention policy or schedule may help you to record how long you expect to keep different types of personal information. If you have 250 or more employees, you **must** record your use of personal information including, where possible, how long you expect to keep it.

10.4 Deciding how long to keep personal information

To help you judge how long to keep personal information, it may be helpful to consider the following factors:

- how likely you are to use the information 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.

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

UK GDPR guidance and resources: Storage limitation

UK GDPR guidance and resources: Right to erasure UK GDPR guidance and resources: Documentation

11. Be clear about roles and responsibilities

11.9 Sharing personal information

A data sharing agreement with other parties may help you to make sure the details are clear, especially if you are sharing personal information regularly, routinely or it is planned in advance.

Data sharing agreements:

- set out the purposes of sharing personal information;
- cover what happens to the personal information at each stage;
- set standards; and
- help all parties to be clear about their 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

UK GDPR guidance and resources: Who does the UK GDPR apply to?

UK GDPR guidance and resources: Accountability and governance

Data sharing information hub

UK GDPR guidance and resources: A guide to international transfers

International data transfer agreement and guidance

12. Help people to use their rights

12.1 Individual rights

People have the following rights relating to their personal information:

- 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.

12.2 Extending the time to respond

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.

12.6 Protection of a journalist's confidential sources

There is strong legal protection for a journalist's sources beyond data protection law. For example, sources are protected under the Contempt of Court Act 1981.

12.7 Right to restriction in certain circumstances

People have a right to restriction in the following circumstances:

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

12.13 Right to object in certain circumstances

People can object to the use of their personal information in the following circumstances:

- the information is being used for direct marketing;
- you are relying on the public task or legitimate interests lawful basis; or
- you are using information for scientific or historical research or statistic purposes.

12:15 Refusing the right to object

You can consider a refusal if you are relying on the public task or legitimate interests lawful basis. This is more limited if you are using information for scientific or historical research or statistic purposes.

12.16 Right to erasure in certain circumstances

People have the right to have their personal information erased in the following circumstances:

- you do not need to keep the personal information 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 information;
- a person objects to your use of the information and there are no overriding legitimate reasons for using it;
- you have used personal information unlawfully;
- you collected the information to offer online services to a child; or
- you need to erase the information to comply with a legal obligation.

12.17 Right to erasure

To help you determine whether you need to use the personal information to exercise the right to freedom of expression, you may find the factors used by the European Court of Human Rights (EctHR) helpful.

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.

12.23 Right to correct or complete personal information

If someone challenges the accuracy of an opinion, you may find it helpful to keep an internal record by adding a note of the challenge and the reasons for it.

12.26 Refusing manifestly unreasonable or excessive requests

To help you decide whether to refuse a request because it is manifestly unreasonable or excessive, you may find it helpful to consider:

- 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.

Case law examples

Case example 8 – Right of access and protection of journalistic sources (paragraph 12.6 of the code)

EctHR

Goodwin v United Kingdom (1996) 22 EHRR 123

The ECtHR 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 9 – DPA 1998 - Fact and opinion (paragraph 12.23 of the code)

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.

Case example 10 – Data Protection Directive 95/46/EC - right to erasure (or right to be forgotten) and distinction between search engines and publication of data by other websites (paragraph 12.24 of the code)

European Court of Justice (ECJ)

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 information by the search engine and use of personal information carried out by publishers of other 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 11 – European Convention on human rights (ECHR) - right to erasure (or right to be forgotten) and strong public interest in news archives (paragraph 12.24 of the code)

ECtHR

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 12 – ECHR - Right to erasure (or right to be forgotten) and anonymisation of digital archive record (paragraph 12.24 of the code)

ECtHR

Hurbain v Belgium [2021] ECHR 544

A person was named as causing 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.

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

Further reading

UK GDPR guidance and resources: A guide to individual rights

UK GDPR guidance and resources: Children's information

13. Apply the journalism exemption

13.3 Parts of data protection law that you no longer have to comply with when the journalism exemption applies

The journalism exemption 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 and accountability principles.
- Article 6 – requirement to satisfy a lawful basis for processing
- Article 7 – conditions for consent.
- Article 8(1) and (2) – conditions for children's consent.
- Article 9 – rules relating to special category data.
- Article 10 – rules relating to criminal offence data.
- Article 11(2) – specific rules regarding informing 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.

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

- The principle to be able to demonstrate that you comply.
- The security principle.
- The right to opt-out of direct marketing.

- Rights about automated processing.
- The right to compensation for material or non-material damage.
- Registering with the ICO.

13.6 Specific industry codes

Specific industry codes listed in the DPA 2018 are as follows:

- Editors' Code of Practice;
- BBC Editorial Guidelines; and
- Ofcom Broadcasting Code.

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

13.9 Using personal information for a journalistic purpose

If you are not sure whether you are using personal information for a journalistic purpose, you may find it helpful to consider:

- the purpose of the publication, including any reasons for publishing the information (eg informing the public);
- how closely the activity aligns with the media's traditional functions (eg 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.

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

For third party content or online "user-generated content", you may find it helpful to consider whether you have applied any editorial judgement to the third party content. For example, to decide whether to include a reader's response. The more editorial control you exerted, the more likely it is that you are using personal information for the purposes of journalism.

13.15 Reasonable belief

To make a decision that is objectively reasonable, factors you may find it helpful to consider include:

- whether you have enough relevant and reliable information to make a reasonable decision; and
- what weight to give to the information you decide to take into account to help you to make a balanced, proportionate decision.

In considering whether your belief is reasonable, it is not our role or a judge's 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.

You do not have to prove that publication is in the public interest or that complying with a specific part of data protection law would be incompatible with journalism. Nor do you need to arrive at the same conclusion as us or a judge. Different views may both be reasonable.

13.16 Editorial discretion

See case examples 19 and 20 below.

13.17 Demonstrating you have a reasonable belief

There are different ways to demonstrate a reasonable belief. You may find it helpful to:

- 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
- keep a record of your decision. The level of risk involved will help you consider what may be appropriate and proportionate. You might do this at a later stage, if more appropriate.

What is relevant is your belief as the person with legal responsibility for personal information. However, you might decide to delegate responsibility for decisions to individual journalists, taking into account the level of risk. A policy may help you to be clear about who has the authority to make decisions.

13:19 General public interest

General examples include, but are not limited to:

- 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.

There may be a public interest in the general subject matter of the information. Examples include, but are not limited to:

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

The above are only illustrative examples of general public interest factors. This is not an exhaustive list. It does not mean there is not a public interest in other journalism, including for example lifestyle, entertainment or showbusiness news.

13.20 The right to freedom of expression and information

The right to freedom of expression and information is protected by Article 10 of the ECHR. This is incorporated into UK law by the Human Rights Act 1998 (HRA). All public authorities, including the courts, have a duty to act compatibly with people's rights under the ECHR. Article 10 says:

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impact information and ideas without interference by public authority and regardless of frontiers. This right shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democracy society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary".

13.22 Equal status of human rights

None of the rights protected by the HRA take precedence over others as a matter of principle. This is consistent with Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe, para 10 which says:

"The Assembly reaffirms the importance of everyone's right to privacy, and of the right to freedom of expression, as fundamental to a democratic society. These rights are neither absolute nor in any hierarchical order, since they are of

equal value".

The right to privacy

The right to respect for private and family life is protected by Article 8 of the ECHR. This is incorporated into UK law by the HRA. All public authorities, including the courts, have a duty to act compatibly with people's rights under the ECHR. Article 8 says:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

13:23 Data protection

Protection for personal data derives specifically from the EU Charter of Fundamental Rights. Although the UK is no longer a member of the EU, data protection is incorporated into UK law through the UK GDPR and DPA 2018.

Case law examples

Case example 13 – Freedom of Information Act 2000 (FOIA) - definition of journalism (paragraph 13.9 of the code)

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 FOIA.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)

The judge generally endorsed earlier analysis by a tribunal that journalism encompassed a range of activities including "…the collecting, writing and verifying of material for publication…the editing of the material, including its selection and arrangement, the provision of context for it and the determination of when and how it should be broadcast…the maintenance and enhancement of standards of the output by reviews of its quality, in terms in particular of accuracy, balance and completeness, and the supervision and training and journalists." (39)

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 14 – DPA 1998 - definition of journalism (paragraph 13.9 of the code)

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 15 – Data Protection Directive 95/46 - definition of journalism (paragraph 13.9 of the code)

ECJ

Satamedia (Case C-73/07)

The 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 16 – Data Protection Directive 95/46/EC - definition of journalism (paragraph 13.9 of the code)

ECJ

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 17 – DPA 1998 - meaning of "acting with a view to publication" (paragraph 13.13 of the code)

Court of Appeal

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 18 – DPA 1998 - meaning of "reasonable belief" (paragraph 13.15 of the code)

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 19 – DPA 1998, Misuse of Private information - editorial discretion (paragraph 13.16 of the code)

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 20 – Misuse of private information – editorial discretion and evidence to demonstrate decision-making (paragraph 13.16 and 13.17 of the code)

High Court

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

The court referred to the concept of editorial discretion in this case. It said, "Properly understood, the authorities on the topic of editorial latitude are concerned with factors [such as] the importance of the free speech rights at stake, and – in particular – the appropriate way to give practical effect to those rights. That is why the Strasbourg authorities refer to 'tone' and to the 'methods of objective and balanced reporting', the 'techniques of reporting' and the 'form in which' information and ideas are conveyed'…the Court stated that Article 10 leaves it for journalists 'to determine what details it is necessary to reproduce to ensure credibility'."

The court said that it would determine the outcome of the case objectively, whilst giving weight to editorial discretion as appropriate. It said "The degree of latitude or weight giving to editorial decision-making depends on the circumstances", including:

- the subject-matter;
- the nature of the information at stake;
- the context in which the defendant wishes to use it, and
- the extent to which the individual defendant can be seen to have relevant knowledge and expertise.

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 21 – DPA 1998. Misuse of private information - public interest and proportionality (paragraph 13.18 of the code)

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. This included 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 House of Lords found that there was not a sufficient public interest to justify publishing this additional information, particularly bearing in mind that it was sensitive health data which could put Miss Campbell's recovery at risk.

Case example 22 – ECHR - Importance of the right to freedom of expression and information, and the role of the press (paragraph 13.20 of the code)

Sunday Times v UK (No.2) 26 November 1991

The ECtHR court said:

"Freedom of expression constitutes one of the essential foundations of a democratic society…it is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive as a matter of indifference, but also to those that offend, shock or disturb. Freedom of expression, as enshrined in Article 10, is subject to a number of exceptions which, however, must be

narrowly interpreted and the necessity for any restrictions convincingly established.

These principles are of particular importance as far as the press is concerned. Whilst it must not overstep the bounds set…it is nevertheless incumbent on it to impart information and ideas on matters of public interest. Not only does the press have the task of imparting such information and ideas: the public has a right to receive them. Where it otherwise, the press would be unable to play its vital role of public watchdog." (50)

Case example 23 – DPA 1998 and Misuse of Private information - Importance of right to privacy (paragraph 13.22 of the code)

House of Lords

Campbell v MGN [2004] UKHL 22

The court said:

"The case involves the familiar competition between freedom of expression and respect for an individual's privacy. Both are vitally important rights. Neither has precedence over the other. The importance of freedom of expression has been stressed often and eloquently, the importance of privacy less so. But it too, lies at the heart of liberty in a modern state. A proper degree of privacy is essentially for the well-being and development of an individual. And restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state…"

Case example 24 – ECHR and HRA 1998 – balancing Article 8 and Article 10 rights (paragraph 13.22 of the code)

House of Lords

In re S (A Child) [2004] UKHL 47

At paragraph 17, Lord Steyn said the following about Article 8 and Article 10 of ECHR:

"First, neither article has as such precedence over the other. Secondly, where the values under the two articles are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary. Thirdly, the justifications for interfering with or restricting each right must be taken into account. Finally, the proportionality test must be applied to each. For convenience, I will call this the ultimate balancing test."

Case example 25 – DPA 1998 - meaning of "incompatible with a journalistic purpose"(paragraph 13.26 of the code)

First-Tier Tribunal

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

This case concerned whether we were 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 a journalistic purpose in this case.

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 journalism exemption because compliance with the data protection principle was not incompatible with the journalistic purpose. .

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…"

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 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.

Further reading

UK GDPR guidance and resources: Children's information

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.

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

The EctHR has also published detailed guidance on Article 10 and Article 8 of the ECHR

14. 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
- 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

What to expect from the ICO when making a data protection complaint contains information about our data protection complaints process.

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