ICO statutory review on how personal data is processed for the purposes of journalism

This note represents a collective response, coordinated via the [redacted], from a number of UK based media organisations to the ICO's statutory review on how personal data is processed for the purposes of journalism. It seeks to assist the ICO to understand how personal data is processed for the purposes of journalism in the media industry, both print, online and broadcast, in the modern era. This note focuses on the use of personal data for the purposes of journalism by UK media organisations - it does not deal with how media organisations implement compliance with the UKGDPR/Data Protection Act 2018 in the commercial sectors of their business - for example how they process consumer and employee data. The way that the media sector processes personal data for the purposes of journalism varies across the media sector. There is no "one size fits all" approach. It is not intended as definitive and does not represent the actions of any one media organisation.

Executive summary

Modern day news reporting is dynamic and wide-ranging in nature. The imperative for news organisations is to provide accurate information to the public in a timely manner. The nature of modern journalism requires quick decisions to be made in response to developing situations so that news can be reported accurately, quickly and efficiently.

At the heart of any processing by UK media organisations of personal data for the purposes of public interest journalism is the special purposes exemption. The relevance and practical effect of the special purpose exemptions - principally but not solely the journalism exemption (the archive exemption is also relevant) - should not be underestimated. A number of principles, for example legal basis or purpose limitation, will not apply if journalists can rely on the special purposes exemption in respect to those principles.

In addition to the use of data associated directly with the publication of their journalism output, media organisations like any other commercial organisation, collect and process personal data about for instance subscribers, readers, registered users of their websites and apps, those attending its events, its employees, contributors and contractors, its commercial suppliers and information that it is provided by third parties. However, this response focuses on the use of personal data for the purposes of journalism - it does not address how media organisations comply with their data privacy obligations in the commercial sectors of their business.

Some larger media organisations have Data Protection Officers who monitor their organisation's overall compliance with the UKGDPR, advise on their data privacy obligations (accountability obligations), conduct audits, provide training, respond to data incidents and breaches,, and respond to data subject rights requests. However, there are also individuals and organisations who rely on the special purposes exemption who are not required to appoint a DPO.

There are serious concerns about the way in which the UKGDPR/Data Protection Act can be used against publishers and the media more widely in a manner that restricts and impinges upon freedom of expression. The existing journalism exemption can be cumbersome and impractical for the day to

day workings of a busy newsroom. There are arguments that the exemption should be replaced with a more workable exemption.

Introduction

It is noted that this is a statutory review under Section 178 of the Data Protection Act 2018 and that according to the ICO's website, the aim of the review is to understand how personal data is being processed for the purposes of journalism, which will help the ICO understand how the media industry has been using and complying with personal information since the new data protection laws came into effect in May 2018.

Data protection law specifically protects journalism and the special public interest in freedom of expression and information, reflecting its importance to society. In particular, the broad special purposes exemption under the DPA 2018 can dis-apply many of the usual requirements of data protection law.

As the ICO has itself recognised, journalism plays a vital role in the free flow of communications in a democracy. It increases knowledge, informs debate and helps citizens to participate more fully in society. It also helps to hold the powerful to account. In addition, individuals have rights to free expression and to being informed in order to participate in a democratic society[1]. This is reflected in data protection law which acknowledges that rights and freedoms must be balanced: "*the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.*" (GDPR, Recital 4)

Data protection law specifically protects journalism and the special public interest in freedom of expression and information, reflecting its importance to society. In particular, the broad special purposes exemption under the DPA 2018 dis-applies certain requirements of data protection law.

News reporting is dynamic and wide-ranging in nature. The imperative for news organisations is to provide accurate information to the public in a timely manner. Reporting can be highly reactive to developing news events. It is now a 24-hour operation, across multiple time zones, in a range of territories with different legal regimes and often with tangible personal risks to journalists. It can involve large multinational organisations or single freelancers. An essential aspect of Article 10 of the European Convention on Human Rights is the requirement that due deference should be given to editorial decisions made by journalists over their choice of which issues to cover, what news gathering techniques to employ, and the verbal and pictorial content of what they finally decide to publish. As noted by Jo Glanville in her 2018 essay in The London Review of Books[2] on the (then new) Data Protection Act 2018 and the journalism exemption:

[1] Article 10 ECHR: Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.
[2] https://www.lrb.co.uk/the-paper/v40/n13/jo-glanville/the-journalistic-exemption

" Personal information and human stories are the raw material of journalism. … the new laws are not intended to impede the business of legitimate daily journalism. The Data Protection Act recognises the 'special importance of the public interest in the freedom of expression and information', and allows exemptions for journalistic, literary, artistic and academic expression where data is processed with a view to publication, where there is a reasonable belief that publication is in the public interest and that compliance would be 'incompatible with the special purposes'. At the same time, the Act makes no distinction between personal and private data, between information that many of us might reveal in the course of our daily lives and the most intimate details that we might only share with our partner or doctor. In its guidelines for journalists (due to be replaced by a statutory code), the ICO states that 'anything about a person can be personal data, even if it is innocuous or widely known.' That might include a person's job, education, the town they live in and the organisations they belong to."

News plays a fundamental role in a democratic society informing, investigating issues and analysing events. Media organisations across the board, large and small, report on individuals in the public eye: politicians, business people, sporting personalities, entertainers and celebrities, as well as telling the stories of private people who come to public prominence because of an event they were caught up in. These stories will almost inevitably be accompanied in some form or other by pictorial images. All such stories will involve personal data and some of them, if discussing issues concerning an individual's health, political and/or religious views, race and sexuality and sometimes their criminal conduct or record, will involve special category data. All such information is a vital part of media organisations' work and output. At its heart, organisations will be processing - ultimately by publishing, but also by obtaining, recording and storing - private personal data about a whole range of individuals. Some may be happy about the way their personal data is used and published, others may be less so; some may have specifically consented to their data being used; others will not have consented, as generally media organisations rely on either the legitimate interests or the special purposes exemption with regard to their legal basis for processing. The special purposes exemption for the purposes of journalism is key where public interest journalism is concerned.

As part of their reporting and newsgathering processes, media organisations and individual journalists retain and store considerable amounts of personal data - they have photo libraries, they have archives of published stories; their journalists will keep contact books and store information, with the consideration that it may be useful in the future for a story. Newspapers' archives of their previously published material, now online and often free to access, or accessible on the payment of a relatively small fee, are well recognised as serving an important democratic function. This vast archive provides a valuable public historical source of information for people searching on the internet: it also by its very nature contains a lot of personal data. This is recognised in data protection laws by the special purpose exemption for the purpose of archiving in the public interest, which is important for media organisations. Not all information obtained about individuals will be published immediately, depending on the outcome of an investigation, data may be retained but not published. All of this involves considerable processing of personal data. Media organisations of course understand and appreciate our obligation to keep this data secure and to review their retention of it from time to time.

In addition to the use of data associated directly with the publication of their journalism output, media organisations like any other commercial organisation, collect and process personal data about subscribers, readers, registered users of website, those attending its events, its employees, contributors and contractors, its commercial suppliers and information that it is provided by third parties. However, as noted above, this response focuses on the use of personal data for the purposes of journalism - it does not deal with how media organisations implement compliance in the commercial sectors of their business - for example how they process reader, marketing and advertising data.

The special purposes exemption

The special purposes exemption exists so that journalists can 'disapply' the usual requirements of data protection law if they consider that it would disproportionately restrict their activity - for example, the requirement to provide privacy information to the subject of a story or comply with a deletion request may seriously undermine journalistic activities.

However, in many cases, journalists will be complying with data protection law when using personal data for journalism as they will be relying on their legitimate interests as commercial news, current affairs and information publishers as the basis for much of their routine day to day publishing of personal data.

While the special purposes exemption is relied upon by media organisations for publishing personal data which has a more than minimal privacy impact in a public interest context, media organisations routinely rely on the broader legitimate interests as the basis for their processing. Media organisations do not need to rely on the journalism exemption for and do not proceed on the basis that every story that features personal data needs to be published in accordance with the journalism exemption.

The legitimacy of this approach is borne out by the latest iteration of the ICO's draft Data protection and journalism code of practice[3]**:**

> **4.8 You can rely on [legitimate interests] 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.**

In *Ambrosiadou v Coward [2011] EWCA Civ 409* Lord Neuberger MR said at [30]:

---

3 https://ico.org.uk/media/about-the-ico/consultations/4021635/ico-draft-data-protection-and-journalism-code-of-practice-second-consultation-21092022.pdf

'Just because information relates to a person's family and private life, it will not automatically be protected by the courts: for instance, the information may be of slight significance, generally expressed, or anodyne in nature. While respect for family and private life is of fundamental importance, it seems to me that the courts should, in the absence of special facts, generally expect people to adopt a reasonably robust and realistic approach to living in the 21st century.'

Under both the 1998 Act (s.32(1) Data Protection Act 1998) and the 2018 legislation (specifically Schedule 2, Part 5 para.26) special provision has been made for journalism to enable it to continue to produce publications in the public interest through the journalism exemption. If the special purposes exemption applies, the processing for the purposes of journalism can be exempt from the lawfulness, fairness and transparency principles. The importance of this exemption is highlighted in the GDPR when it states that EU member states shall provide for 'exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

The availability of the special purpose exemption for journalism is important to protect journalists who publish personal data which will sometimes include special category data and information they believe to be in the public interest. Media organisations across the spectrum from news organisations to consumer publications to celebrity magazines, will seek to rely on the special purpose exemption for journalism in the public interest which has a higher risk of impact on people's personal data, in all areas of their publication process, from the initial gathering of information, through to publication and post-publication processing. While there may be from time to time consents obtained for the publication of personal information, for example when an interview is conducted on the record for a magazine feature, that is not the usual basis relied upon where journalism is concerned.

In most stories, the legitimate interests basis and the various elements of the special purpose exemption are generally applied as part and parcel of the normal editorial thought process. So far as the latter is concerned, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest. The person ultimately exercising the decision to publish - the journalist or editor - will, where appropriate, reasonably believe that publication would be in the public interest, and that the application of the other listed GDPR principles would be incompatible with its journalistic purpose. They will be able to demonstrate this if called upon - whether through a pre-existing audit trail, diary entries or personal testimony.

The second condition of the special purpose exemption: that publication of the specific personal data would be in the public interest is a normal part of the pre-publication process. Since this is a normal part of the publication process and the selection of content, regularly recording or documenting such matters for every single public interest story that is published or produced that uses personal data, would impose an enormous and onerous burden; indeed such a requirement would, in the words of the exemption itself, be 'incompatible' with the journalistic purpose since it would slow down, if not

completely stop, the process of publication (which would of itself be contrary to the public interest) and at the same time require the production and filing of a large amount of information connected with personal data which would have to be kept securely. The same public interest considerations may span a number of stories which may be related to each other by subject matter or may be contemporaneous with each other. It would clearly be unduly burdensome to require busy news desks to record the same arguments over and over again in respect of each such story.

A considerable amount of journalism will not involve personal data at all - it may be about businesses, or national or geographic or historic events for example. However, where a story involves personal data the use of which is more than minimal, the special purposes exemption is routinely relied on where a lawful lawful basis for processing may not be available, but each case is dealt with on a fact-specific basis. Some editorial decisions may warrant and time may reasonably permit the contemporaneous documentation in writing of the decision making process leading to publication, but there is no common practice around this within the industry and the reality is that the majority of day-to-day editorial decision-making, is not subject to documented processes. Indeed as already stated, there is a general thought process around these issues as part of any pre-publication decision on whether to publish certain information in a story or not. Further, a considerable amount of reporting of course does not warrant any documentation because personal data is not published or no significant privacy issue is engaged. Editorial codes such as those published by Ofcom or IPSO or Impress, as well as internal editorial codes, often set out definitions of what might amount to the "public interest", and also require editors to be able to demonstrate they considered it. Such codes are well known to journalists and may indeed be part of their contracts of employment. Further, the common law (for example in privacy and defamation cases) increasingly requires a "show your workings approach". What is key in any publishing decision is having the belief: obviously it is helpful to be able to show that by reference to contemporaneous evidence but that is not always going to be practicable or possible.

This approach is recognised in the 2014 Data Protection and Journalism Guide for the Media issued by the ICO:
https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf
which specifically states that

> *We will expect organisations to be able to show that there was an appropriate decision-making process in place to consider the public interest of a story. We accept that the level and availability of audit trails of decision making will vary from case to case, but there should be an overarching decision making process in place that can support decision making related to data protection issues. What is appropriate is likely to depend on the case – in many day-to-day stories it may well be appropriate for the journalist to use his or her own judgement, but more high-profile, intrusive or damaging stories are likely to require more editorial involvement and a more formal consideration of the public interest. Organisational policies should be used to explain when greater editorial involvement is required.*

There are a number of concerns about the way in which the UKGDPR/Data Protection Act is being deployed against publishers and the media. Publishers feel they are being required to demonstrate that they "complied" with the special purposes exemption, which is thus deployed not as an exemption, but rather as a means of attack. As indicated above, demonstration of compliance can be achieved by a number of ways. Contemporaneous documentation in most daily news rooms is not an option. Discussions often take place that are face to face and unrecorded with notes or contemporaneous correspondence or which might be legally privileged or restricted for some other reason such as source protection. In such cases record keeping is an additional and onerous obligation. Publishers believe that the current exemption is unwieldy, impractical and onerous. News and information publishing should be properly protected. There should in essence be a much more clear cut special purposes exemption available for the media, along the lines of the exemptions used in Australia [s 7B(4) of the Privacy Act,], or Canada [Personal Information Protection and Electronic Documents Act 2000 SC 2000, c 5 (Canada) ss 4(2)(c), 7(1)(c)] and Sweden [Section 7 of Sweden's statute implementing the GDPR], which would exempt processing solely by reference to the identity of the controller as a news publisher – perhaps by reference to the definition that was included in the draft Online Safety Bill.

The special purposes exemption in the DPA 2018 (insofar as it applies to the media) should be amended so as to provide a general exemption from relevant provisions of the GDPR, which would apply to all processing by the press and not require case-by-case balancing. Article 85 GDPR provides that there can be exemptions or derogations from Chapters II, III, IV, V, VI, VII and IX. A provision should be introduced, which exempts processing solely by reference to the identity of the controller as a news publisher – perhaps by reference to the definition in the draft Online Safety Bill.

This change could be introduced by an amendment to the DPA as below:

> **In schedule 2, paragraph 26, add:**
>
> **(1A) The listed provisions do not apply to the processing of personal data for the purposes of journalism [by a Recognised News Publisher as defined in [clause 40] of the Online Safety [Act 2022 (when enacted)].**

Data Subject Access Requests [DSAR]

Most media organisations receive DSARs from individuals and organisations acting on behalf of individuals who are subjects of their journalism. Organisations have processes for handling and responding to Subject Access Requests. Depending upon the circumstances and the type of data which is being sought, organisations deal with DSARs either through their specialised data protection teams, or through their Editorial Legal departments, or through a combination of both. In the publishing/journalism context, most organisations have processes in place to respond to requests to delete or edit their editorial content - for example requests to have names or personal information removed from published material. Such requests have been becoming increasingly common following on from the so-called *Google Spain* case. Specialist data protection teams within organisations will usually oversee a similar process in respect of data requests relating to commercial information held by their organisations.

Responding to a DSAR can often be time-consuming and expensive and engage a lot of internal resources. The financial costs associated with a DSAR request can vary, but are generally not related so much to the administration costs but to obtaining legal and other advice about the search that is needed, assessing the results of such searches and the level of information that should be released, once the information has been retrieved. DSARs are being used as a means to intimidate, chill, limit and prevent journalism. Responding to a DSAR in a journalistic context can be very time consuming, it can raise difficult issues around sources and reveal pre-publication work to the subject of a potential story.

Even though there is a journalism exemption for DSARs in the Data Protection Act 2018, the current state of the law requires searches to be made, and each document has to be reviewed as to whether the journalism exemption applies. Most of the time, the journalism exemption will mean that little if anything beyond what has been published and is already in the public domain, will need to be disclosed.

Many DSARs are undertaken as a way to create administrative and legal burdens for media organisations, and to force early disclosure at no cost with the goal of sapping the time and resources of journalists, data protection and editorial legal advisers.

Training

Media organisations recognise the significance that processing personal data plays in modern day journalism. A key aspect of this recognition is ensuring that regular data protection training is generally provided. Most organisations will provide wider training on data protection issues to all employees, freelancers and contract staff. Some, but by no means all, organisations make such training compulsory for all staff. Others will also provide focused bespoke data protection training to relevant editorial teams and /or ensure that regular training updates are provided and resources are accessible on internal intranet systems. Training can be provided via a variety of formats, including face to face, remotely using on-line and e-learning courses.

Training for reporters and editorial staff will include topics such as what is personal data, what is processing, as well as explaining how the special purposes exemption works. Journalists and editorial teams are also trained on special category data and criminal offence data.

In addition to focused training for editorial staff on how data protection impacts on the day to day work of journalists, organisations will additionally have wider policies and training for all staff which will also apply to their journalists and editorial staff, including but not limited to keeping data safe, including what to do in the event of a data breach / loss of laptop / mobile phone; data and cyber security etc.

Governance

Many governance and accountability requirements are dependent on the operation of the various data principles (for example, lawful basis), which may not apply if a journalist can apply the special purposes exemption in respect to those principles. This means in practice where journalism is

concerned, that there are a different set of considerations to those that will apply more generally to an organisation's data protection governance. Some larger media organisations have Data Protection Officers who monitor their organisation's overall compliance with the UKGDPR, advise on their data privacy obligations (accountability obligations), conduct audits, provide training, respond to data incidents and breaches,, and respond to data subject rights requests. Internal processes and systems are in place to manage personal data breaches, for example organisations will have security incident management policies and policies around data breach to determine whether an incident meets the threshold for reporting to the ICO and / or whether data subjects need to be notified. Incidents, risk assessments and associated information and communications are logged. Most organisations have a team of dedicated data privacy specialists to advise on specific issues which impact and can involve all those working within the organisation, such as data breaches, training, SARs, data policies and procedures throughout an organisation. DPOs will have ultimate responsibility for monitoring compliance with data protection laws and policies and raising awareness of data protection issues. However, because journalism can involve very sensitive and complex legal and ethical considerations, such as around source protection, more often than not internal editorial lawyers and editorial data specialists will usually be involved in the editorial aspects of responding to DSARs and deletion requests. **As explained above, most organisations provide regular training to journalists and editors which will routinely include data protection which reinforce the organisation's compliance.**

Once material is published on a news organisation's website, it is considered to be part of the historical archive. Organisations having processes and policies around updating, correcting, clarifying or removing and/or noting articles where appropriate when accuracy or other complaints are received and it is accepted that published material is inaccurate or personal or private information was inappropriately published. In most instances these are matters governed by internal or external editorial codes.

Records of processing activity (ROPA)

A RoPA is maintained subject to the special purposes exemption.

Privacy statements

All organisations have privacy policies covering the use of reader and other data for commercial purposes. Such policies are not however focused specifically on the use of personal data for journalism, as that is in most instances going to be covered by the legitimate interests basis or special purposes exemption.

Privacy statements / notices are usually publicly available documents accessed via company websites, usually by clicking a "privacy policy" or similar link found at the bottom of the home page of organisations websites. Such statements will include the information required under Article 13 UKGDPR.

The following are just some examples of privacy statements as available on the websites of some media organisations (other examples can be drawn from a range of websites):
https://www.theguardian.com/info/privacy

ITV News Privacy Notice
ITN Privacy Policy
Channel 4 News Privacy Policy
https://help.ft.com/legal-privacy/privacy-policy/
https://www.bbc.co.uk/usingthebbc/privacy/

Data Protection Impact Assessments [DPIA]

As far as their publishing activities are concerned, media organisations will carry out DPIAs (or have processes which embrace or serve a similar purpose) on a case by case basis where the processing of personal data for the purposes of journalism is considered to be high risk - for example where children and young persons data might be involved. (The use of processes other than dedicated DPIAs will often be warranted because editors have to make a broad assessment of the editorial justification for working with and publishing information and cannot think of these processes just in data protection terms). Most organisations will not however have a generic DPIA covering their day to day processing of personal data for the purposes of their journalism. Some organisations may record details of specific editorial controls, checks and balances for certain article or programme types in broader DPIAs. For example, a DPIA, or an equivalent process, could be conducted for a specific "investigative journalism" project that might record an analysis of how the data will be kept securely, whether it is considered to be in the public interest to publish it, and what the risks of publishing such data may be. Such an assessment would normally be signed off by senior editorial management. Some will utilise documented processes where covert or undercover journalistic activities are to be undertaken.

Security

Information security is a priority for the media industry, as retaining the trust of readerships / audiences and sources is essential to business brand viability. The industry is aware that a serious data breach from whatever source (deliberate or accidental) could have serious business consequences in terms of fines and reputational damage, or personal consequences to individuals involved. [Evidence the MoD data breach of Afghan interpreter information.] Security and data protection teams lead in terms of policies and processes. The range of security measures will vary but will include technical controls such as firewalls, encryption, anti-virus software, cyber awareness training, secure passwords, two factor authentication, back-ups, updates and VPNs - and organisational controls such as data protection training, policies, procedures, picture IDs, role-based access, physical security including locked doors, CCTV and security guards. Controls will be applied depending on risk e.g the type / sensitivity / amount of data and the circumstances in which it's being processed e.g. whether in the office, at home, on the move or in the field.

Sharing data

There are often many participants in the production and delivery of journalism. These can include staff employed by the media organisations, freelancers and casuals. Not all will be based in the UK.

Sharing of data between freelancers, sources, but also media companies is an important part of processing for the purposes of journalism and in the public interest. Media organisations working with outside third parties might deploy a memorandum of understanding or have an agreed set of protocols as to how data could be used and shared, making clear the appropriate level of security.

The sharing described above is an important part of processing for the purposes of journalism, but is separate from sharing with processors or other vendors, which will be subject to contracts including Article 28 clauses (if applicable).

Conclusion

Despite the broad nature of the exemption, the sector appreciates that it's not relieved of all obligations under data protection legislation. Journalists and editors are trained professionals who understand their responsibilities and how these must be balanced against the right to freedom of expression – for the benefit of audiences, readers and society as a whole.

Media organisations take appropriate measures and expend substantial time and resources in ensuring personal information is processed in line with the data protection principles, ensuring data is used in ways that are, for example, fair, lawful and transparent, accurate, secure and accountable.

Simplifying and clarifying the exemption would make it easier for media organisations to adopt individual flexible risk-based approaches to protecting people's data; and balance this with the right of freedom of expression which will vary considerably depending on a range of circumstances and factors.

There should be a reduced focus on prescriptive controls to be implemented at the cost of other areas that may be more relevant and carry a higher risk for the organisation and for data subjects e.g. relying too heavily on a requirement for individual risk assessments, the completion of which could prevent broadcast or publication.

Too rigid oversight of the journalistic process would be detrimental to democratic freedom of speech. It's not the job of supervisory authorities to dictate or determine when and how the exemption is engaged, or to hinder freedom of speech through cumbersome bureaucracy.

The nature of journalism is dynamic and changing, almost daily. Guidance and oversight needs to be sufficiently light touch and flexible to adapt to future ways of reporting, to methods of media delivery not yet imagined.

12 October 2022