Justifying oral history sound recordings under GDPR – a worked example

Jonathan Fryer, Data Protection Officer, British Library

Data Protection is made up of a series of layered decisions and considerations. It is sometimes helpful to work through these explicitly, particularly where the proposed data processing is novel, complex, or contentious.

Activity and Purpose

The first question we must answer is 'What does the proposed activity consist of, and what is its purpose?'

For this example, the proposed activity is to record an oral history interview with an individual (who we will call the 'Data Subject'), to store it in perpetuity, and to make it available to the public (either immediately or in the future) for historical research.

Broadly speaking the purpose of this set of activities could be described as 'archiving in the public interest' – for example we want to store personal data and other material of historical significance in the long term, and make it available for the edification of the public.

Legal Basis

The second question we must ask is 'What allows us to process personal data in this way?'. This is the most important question, as the answer will determine which Data Subject rights and which exemptions or obligations apply to the processing.

GDPR (and the Data Protection Act 2018 that underpins it in the UK) states that processing personal data is only lawful if you meet one (and only one) of six conditions:

- The Data Subject has given their consent to the processing
- It is necessary for the a performance of a contract with the Data Subject (or to enter into such a contract)
- The Data Controller (e.g. the person carrying out the activity) is under a legal obligation to do so
- It is necessary to protect the vital interests of the Data Subject or another natural person
- It is necessary for a task carried out in the public interest, or in the exercise of official authority

- It is necessary for the legitimate interests of the Data Controller or any other third party, and these are not outweighed by the rights of the Data Subject.

For this example, we are unlikely to have a legal obligation to perform the proposed activity, and it is very unlikely that the Data Subject will die or be injured if we do not interview them (vital interests). We need to consider our other options however.

We could ask the Data Subject for their consent, which under GDPR must be fully informed, freely given, and made via some form of positive indication of the Data Subject's wishes. We could do this easily by asking them to fill in a form, and they are presumably willing to give their consent else they would not be taking part in the project. As part of that form we will need to tell them exactly how their data will be processed, stored, and used (including whether any third parties will work on it or store it on our behalf), in order to meet the 'fully informed' criteria. There are two problems however, the first of which is that consent may be withdrawn at any time and without reason by the Data Subject. Given that our intent in this example is to create a permanent record in perpetuity, this makes consent a less than optimal choice for our legal basis. We could still use it, but we would run the risk that for the rest of the Data Subject's lifespan they could at any time require us to delete the recording. Additionally, the legal basis selected needs to cover all of the Data Subjects involved e.g. not just the interviewee, but anyone identifiable that the interviewee talks about. Gaining consent from all such persons is likely to be prohibitively difficult to achieve.

Aside: Children in the UK are assumed to be able to give consent to the use of their personal data from the age of 13 (12 in Scotland). In the event of any clash between consent given by a parent on their behalf and the child's consent, the child's consent (or withdrawal thereof) will take precedence.

We could enter into a licence or contractual arrangement with the Data Subject. This may be appropriate for some commercial projects where the participants are paid for their contribution. In order to meet the criteria the Data Subject must still be fully informed of what they are signing over, and some form of consideration must be paid to them in order to qualify the donation of their personal data to us as a contract.

Public bodies (including national libraries museums and galleries, universities, local libraries, and some charities or commercial organisations providing similar services to government) may rely on their 'public task' to carry out data processing. To do so the proposed processing (in our example, the recording and dissemination of oral history) must fall within the remit of their founding charter, act of parliament, or similar commissioning document. For example, the British Library Act requires the British Library to create a comprehensive

collection of research material for the nation – the recording of oral history is therefore definitely part of this public task for the British Library.

Everyone else (including amateur or volunteer archives without an explicit public task founded in law) may rely on legitimate interests, as long as this can be justified. This is a balancing exercise, where the benefit to the Data Controller (and to anyone else including the public at large) must be weighed against any intrusion into the rights of the Data Subject. Presumably, for the sake of our example, the Data Subject is willing to talk to us, so the interview itself is unlikely to be unfairly intrusive, but we do need to consider the rights of anyone that they talk about as well, and any problem with this is most likely to arise from the act of making the oral history available – this is not an insurmountable barrier however, and we will explore their rights later in the process.

For this example then, our best choices are therefore likely to be 'performance of a public task', if that option is available to us by virtue of our status, or 'legitimate interests' if it is not.

Aside: If you cannot find a legal basis that fits your processing then one of two cases applies. Either your proposed processing is downright illegal and may not take place, or else you have too many activities bundled together and this is confusing the choice. It is permissible to break down your proposed activity into steps, and then to justify each step with a separate legal basis. In our example, we could possibly justify the initial act of recording the interview under consent, and then rely on public task or legitimate interests for the storage and dissemination of the recording. The drawback to this approach is that it is much more complex. You have to make the legal basis of every step clear to the Data Subject which is a) potentially a significant administrative overhead, and b) potentially confusing to the participant. If this confusion is sufficient to hinder their understanding in any material way then their consent is not 'fully informed' and therefore invalidated, and it is also unfair, which will undermine your legitimate interests as the Data Subject's rights have not been properly protected. As such this approach is not recommended unless absolutely necessary.

Special Category Data

Unfortunately we are not yet done with the question of legal basis. GDPR forbids the processing of special category data (for example personal data that discloses racial or ethnic origin, political opinion, religious beliefs, trade union membership, sexual orientation, health data, or similarly sensitive subjects) UNLESS this too is justified with a separate legal basis chosen from a different list of options. Given that the most interesting oral history is likely to cover some or many of these subjects, we need to make another decision.

Fortunately, Section 4(a) of Schedule 1 of the Data Protection Act 2018 provides that data processing 'necessary for archiving purposes… in the public interest' is one of these

conditions. As we have already established that this is the purpose of our activity, we need not look at the rest of the list.

The Data Protection Principles

Once we have our legal basis, we also need to consider that all processing of personal data must comply with the Principles set out in Article 5 of the GDPR, and we must be able to demonstrate this compliance with documentary evidence if asked by the ICO. I will address these Principles in reverse order, as this addresses the simplest requirements first.

f) The personal data we are processing must be protected against unauthorised or unlawful processing and against accidental loss destruction or damage, using appropriate technical or organisational measures. In practice, for the sake of our example, this means that the recording (and any administrative personal data collected in parallel) needs to be adequately protected using normal archival best practice, standard IT security measures, and appropriate training and organisational policies.

e) Personal data must be kept no longer than is necessary for the stated purpose. In of our example, the purpose is to keep the recording forever so we do not need to worry about its disposal.

d) Personal data must be accurate and kept up to date. For the sake of our example, you may be aware that the facts put forward by your interviewee are incorrect or at least disputable by the person talked about. This Principle does NOT mean that you have to correct this however; it means that the recording and any transcript or summary must be an accurate record of what was said.

c) Personal data processed must be adequate, relevant, and limited to what is necessary for the stated purpose. Oral history by its very nature is likely to be wide ranging, so this Principle does not really concern us except in relation to any supporting administrative data collected. This administrative data will need to be limited to that necessary to support the archiving activity, such as to support the assignment of rights, authority files, and cataloguing data

b) Personal data must be used for specified, explicit, and legitimate purposes, and not further processed in any way incompatible with those purposes. We have already specified our purpose, made them explicit to the Data Subject, and legitimised our processing with a legal basis. The ‘further processing’ requirement is worth noting however. In our example so far we have set out a scenario that is about creating a record specifically for our archive. You may however, in some cases, wish to ingest other material into your archive, for example a recording of a radio interview. There the stated purpose of the interview was not for perpetual archiving and public access, but for a short term engagement which is transmitted

once. Notwithstanding any other obligations, the archiving of this material is not prevented by this Principle however, as the GDPR provides that the purpose of archiving in the public interest is never incompatible with the original purpose.

a) Personal data must be processed lawfully, fairly, and transparently.

Lawfully: We have already established the lawful basis of our activity, so unless there is another law that specifically forbids us from the proposed activity then we have met this requirement.

Fairly: In order to be fair, particularly under legitimate interests but also more generally, we must ensure that adequate safeguards are in place to protect the rights and freedoms of the Data Subject(s) and consider how our processing may affect them. For the sake of our example, this will be normally be covered off by the usual archival practices of sensitivity review and the redaction or embargo of sensitive material until the passage of time makes the material safe for dissemination. In particular, Section 19(2) of the Data Protection Act 2018 states that such safeguards will not be adequate (and therefore not fair) in the context of the purpose of archiving in the public interest if they allow substantial distress or substantial damage to be caused to a Data Subject, or if they allow decisions of legal or similar import to be made about the Data Subject (for example, it would be unfair to review an oral history recording in order to decide whether to offer the Data Subject insurance cover).

Transparently: For the sake of our example we have already fully informed the interviewee of how and why their data will be processed, the legal basis of that processing, and any other necessary details. However, it is unlikely that we have provided such information to other Data Subjects discussed in the interview. Under normal circumstances we would have an obligation to inform them of the existence and details of our processing, but Section 28(2)(a) of Schedule 2 of the Data Protection Act 2018 provides that the requirement to provide such confirmation of processing does not apply to personal data processed for 'archiving purposes in the public interest' to the extent that the requirement would prevent or impair the archiving process. Given how difficult (or impossible) it would be to contact all such persons this requirement would prevent us from carrying out the archiving activity, and therefore it does not apply. Nonetheless, it *would* be possible to place the required information in our privacy policy on our website, and so that is how the transparency obligation to these Data Subjects should be met. For example, in its Privacy Policy the British Library has a short supplementary statement about the use of personal data in its Collections here.

The information that must be provided to the Data Subject at point of collection, or upon request, is:

- The identity of the Data Controller

- The contact details of the Data Controller's Data Protection Officer (if the organisation has one)
- The purpose and legal basis of the processing
- The recipients of the personal data (e.g. who is the data given to? In our example, the recipients are the general public).
- The identity of any Data Processor (e.g. any third party who will process the data on our behalf. In our example, this is most likely to be an IT company supporting storage or transmission of data, such as DropBox or Google)
- Any storage or transfer of the data outside of the European Economic Area (This is normally forbidden, but can be legitimised in several ways such as Binding Corporate Rules, European Model Contract Clauses, or membership of the EU-US Privacy Shield arrangement. In our example, it is only likely to be relevant if our Data Processors are based outside of the EEA).
- How long the data will be stored for
- Which Data Subject rights apply to the processing (see below)
- The ability to withdraw consent at any time (if consent is the legal basis cited)
- The right to lodge a complaint with the ICO
- Whether the provision of personal data is a statutory or contractual requirement, and the consequences of any failure to do so
- The existence of any automated decision making or profiling (not likely to be relevant for our example)

Data Subject Rights

The GDPR grants certain rights to every Data Subject, but how these rights apply in a given situation depends on the purpose and legal basis of the processing. The last thing we therefore need to consider is how the rights apply to our specific scenario.

We have already covered the 'right to be informed' under Transparency above, and the 'right to object to automated decision making' is unlikely to be relevant. However, the other rights might potentially apply to the processing in our example.

A Data Subject has, upon request, the right to receive from a Data Controller a copy of their personal data free of charge (a request made under this right is called a Subject Access Request). However, Section 28(2)(a) of Schedule 2 of the Data Protection Act 2018 provides that this right does not apply to personal data processed for 'archiving purposes in the public interest' to the extent that the requirement would prevent or impair those purposes. In practice, for the purpose of our example, you do not have to search your entire archive in response to a request for 'everything you hold about me'.

A Data Subject has the right to insist that inaccurate personal data be corrected or completed without delay. However, Section 28(2)(b) of Schedule 2 of the Data Protection Act 2018 provides that this right does not apply to personal data processed for 'archiving purposes in the public interest' to the extent that the requirement would prevent or impair those purposes. As we have already said, in practice and for the purpose of our example, you do not have to correct inaccurate statements in an interview that have been accurately recorded. For purposes of fairness, you may however wish to add additional commentary to your catalogue or summary to indicate that certain statements are contested or inaccurate.

A Data Subject has, in certain circumstance, the right to request erasure of their personal data without undue delay (this is the so-called 'right to be forgotten'). For our example, this right simply does not apply to material necessary for the purpose of archiving in the public interest.

A Data Subject has, in certain circumstance, the right to request that a Data Controller should cease processing their data in certain ways, which we do not have the time to explore here. Section 28(2)(c) of Schedule 2 of the Data Protection Act 2018 provides that this right does not apply to personal data processed for 'archiving purposes in the public interest' to the extent that the requirement would prevent or impair those purposes. In practice, for the purpose of our example, the Data Subject cannot use this right to compel you to cease cataloguing or storing their data. For purposes of fairness however, anyone who would have a legitimate case when exercising this right in other circumstances is likely to be able to make a case for substantial damage or substantial distress, and is therefore likely to have a legitimate case to ask you to suppress their personal data from public access.

Where a Data Controller is required to act on any of the above rights, there is an additional obligation to inform the recipients of that personal data so as to require them to carry out similar measures, unless such notification would be impossible or require disproportionate effort. In our example, it is unlikely that we will have taken any action in the response to those rights, given the wide exemptions for archiving in the public interest. Even if we have however, it is likely to be impossible or prohibitively difficult to inform the general public (our recipients) of the actions taken, and in any event Section 28(2)(d) of Schedule 2 of the Data Protection Act 2018 provides that this right does not apply to personal data processed for 'archiving purposes in the public interest' to the extent that the requirement would prevent or impair those purposes.

Where personal data is processed electronically under consent or under contract, the Data Subject is entitled to request that the data supplied to them in response to a Subject Access Request be supplied to them in a structured, machine readable form and has the right to use that data with another Controller. As above, in our example, we are unlikely to be required provide archival records in response to a Subject Access Request. However, if we were for some reason compelled to do so, or chose to do so voluntarily or for fairness

purposes, we would potentially be required to comply with this right. However, Section 28(2)(e) of Schedule 2 of the Data Protection Act 2018 provides that this right does not apply to personal data processed for 'archiving purposes in the public interest' to the extent that the requirement would prevent or impair those purposes.

Finally, where personal data is processed on the basis of public task, official authority, or legitimate interests, a Data Subject has the right to object to the processing of their personal data if they can make a case on grounds relating to their own situation, unless the Data Controller can demonstrate compelling grounds that override the data subjects rights and freedoms. Section 28(2)(f) of Schedule 2 of the Data Protection Act 2018 provides that this right does not apply to personal data processed for 'archiving purposes in the public interest' to the extent that the requirement would prevent or impair those purposes. As we should have already considered any potential damage or distress that might be caused to the Data Subject by our archival processing, as well as other fairness considerations, it is likely that the prevention or impairment caused to the archiving purpose (for example by a request objecting to cataloguing, storage, or public access) will engage the exemption, and even if it does not, the public interest in the archival activity (having already taken into account the Data Subject's legitimate rights and freedoms) are likely to override the Data Subject's specific right to objection.

Taken together GDPR and The Act are well over 500 pages long, and cover many other organisational provisions and scenarios, but this worked example should be sufficient to demonstrate how the key requirements apply and can be worked through (and potentially documented for evidential purposes.)

Jonathan Fryer

Data Protection Officer – The British Library

01 June 2018