Data Sharing in the Public Sector

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Sharing in the Public Sector

Introduction

Individuals whose personal data are collected, stored, shared, or otherwise 'processed' ('data subjects') are entitled to expect that public sector bodies will only handle and share their personal data lawfully, fairly, and in a transparent manner. Their data should only be processed where it is relevant, essential, and necessary to provide them with public services or to carry out another public function. The Data Protection Commission (DPC) fully supports the aim of developing more efficient and customer-centric public services in this regard, in line with the requirements of the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED), and the Data Protection Act 2018.

Importantly, this must take into account that data subjects need to be informed as to how their personal information are used and for what purpose, who has access to it, and how the sharing of that information will impact them. Therefore, whilst data sharing can bring benefits in terms of efficient delivery of public services, it must be done in a way that respects the rights of individuals to have their personal data treated with care and not accessed or used without good reason.

As such, the DPC recommends that all data sharing arrangements in the public sector should generally:

- Have a basis in primary legislation;
- Have a clear justification for each data sharing activity;
- Make clear to individuals that their data may be shared and for what purpose;
- Be proportionate in terms of their application and the objective(s) to be achieved;
- Share the minimum amount of data to achieve the stated public service objective;
- Have strict access and security controls; and
- Ensure secure disposal of shared data.

The DPC welcomed the decision of the Court of Justice of the European Union (CJEU) in the case of Bara & Others (C-201/2014), noting the strong trend emanating from the CJEU in interpreting data protection law (in that case the precursor to the GDPR, the Data Protection Directive) so as to re-enforce the protection of the rights of individuals in the context of the public sector use of personal data.

The Bara judgment, which focused upon a public sector data sharing arrangement, re-iterated the importance of informing data subjects about the processing of their personal data (which includes sharing that personal data) as it affects the exercise by the data subjects of their rights, such as the right of access to their personal data, their right to rectify their personal data being processed, and their right to object to the processing of their personal data.

It is important to restate from the outset that all processing of personal data under the GDPR must comply with the principles of data protection (as set out in Article 5 and throughout the GDPR), must have a 'legal basis' under Article 6 GDPR (to legitimise and justify the processing), and must comply with the requirements under Articles 12-14 (to provide data subjects with information about that processing). Further, in cases where sensitive, 'special categories' of personal data are processed, public sector bodies need to comply with the requirements of Article 9 GDPR, in addition to these other requirements.

Likewise, the processing of personal data by public sector bodies for law enforcement purposes and falling within the scope of the LED must comply with the similar obligations and requirements which are set out in Part 5 of the Data Protection Act.[1]

The DPC also notes the recent passage of the Data Sharing and Governance Act 2019, the stated purpose of which is to provide a generalised legal basis for the sharing of data between public bodies, as well as to set out further appropriate safeguards under which such sharing should take place. [2] Whilst public sector bodies should also be aware of the rules and requirements set out in that Act, these are in addition to the general principles required under data protection law, which are dealt with in this guidance note. In undertaking a review of all current and future data sharing arrangements, public sector bodies should ensure that the following best practice guidelines are considered and applied as appropriate.

Lawfullness and Legal Basis

The very first principle relating to the processing of data which is set out in Article 5 GDPR is that any processing should be done in a manner which is lawful, fair, and transparent.

To ensure that data sharing is lawful, public bodies should only share personal data where it complies with the above in addition to the other principles set out in Article 5 – purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability – as well as the requirement to have a legal basis for the processing of personal data under Article 6.

The public policy objective being pursued by a particular data sharing arrangement, as well as the legal basis for the processing in question, should be explicit and transparent. An assessment should be made as to whether the likely benefits of the sharing are balanced with the individual's data protection and privacy rights. It should also be ensured that the sharing is for specified, explicit, and legitimate purposes and the personal data will not be further processed in a manner that is incompatible with those original purposes. The personal data shared should also be adequate, relevant, and limited to what is necessary to achieve the purpose(s).

When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both) it is imperative to identify the purpose that it is meant to achieve. In doing so, public sector bodies should consider the potential benefits and risks, either to individuals or society, of sharing the data. An assessment as to the likely results of not sharing the data should also be conducted.

As held by the CJEU in the case of Digital Rights Ireland (C-293/2012), any legislative measure enacted to provide a legal basis for the processing of personal data must meet a proportionality test, be an appropriate step towards meeting the legitimate objectives pursued by the legislation at issue, and not exceed the limits of what is appropriate and necessary in order to achieve those objectives.[3]

Public bodies should consider the following non-exhaustive checklist from the outset when assessing a data sharing arrangement (either as a provider, a recipient, or both):

[1] See sections 69 to 104 of the Data Protection Act 2018.
[2] Per the Department of Public Expenditure and Reform website, at https://www.per.gov.ie/en/datasharing/
[3] Note also Article 52 of the Charter of Fundamental Human Rights whereby any limitation on those rights must be provided by a legislative measure, and subject to the principle of proportionality, limitations may only be made if they are necessary and genuinely meet the objectives of a general interest or the need to protect the rights and interest of others.

- **Identify what the arrangement is meant to achieve.** All data sharing arrangements should have a clearly understood set of objectives which are documented and recorded.
- **Identify whether the objective could be achieved without sharing the data or by anonymising it.** The default position should be to analyse whether personal data needs to be shared in the first instance in order to achieve the goal(s).
- **Identify the minimum information required to achieve that purpose**. All data sharing arrangements should share only the minimum required personal information to achieve the body's objectives.
- **Identify any risks which the data sharing may pose.** When considering whether to implement and place a data sharing agreement on a legislative footing consideration should be given of the fact that such sharing could increase the reluctance of individuals to provide accurate personal data to public sector bodies. It should also take account of any disproportionate negative impact on particular sections of society.
- **Identify when and how often the data should be shared**. It is good practice to document this and set out whether the sharing arrangement will be ongoing or periodic or whether it will occur in response to a particular set of events.
- **Consider whether a Data Protection impact Assessment (DPIA) is required**. DPIAs can be used to identify and mitigate against any data protection related risks arising from a new project, which may affect a public body or the individuals it engages with.[4]

Legal Basis

As mentioned above, for the sharing of personal data between public bodies, there must be a legal basis, as required by Article 6 GDPR. Although there are a number of potential legal bases under Article 6 GDPR, in most cases[5] for data sharing in the public sector the appropriate legal basis is likely to be found in Article 6(1)(e) – "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*". Article 6(3) GDPR goes on to explain that the basis for any such processing must be laid down in EU or Irish law, and that the law should meet an objective of public interest and be proportionate to the aim pursued.

The DPC recommends (where appropriate) that the conditions of the data sharing arrangement are outlined clearly and in adequate detail either in primary legislation or alternatively, in secondary legislation (provided a primary legislative basis exists) thereby leaving no room for confusion or doubt as to the nature of the arrangement and providing legal certainty.[6] The legislation (or a regulatory measure based on a legislative measure) should clearly identify the public sector bodies involved, the information that will be shared and the purpose(s) for sharing the information. Public sector bodies should also ensure that adequate, appropriate and relevant safeguards are put in

[4] See the DPC's guidance on DPIAs for further details, at https://www.dataprotection.ie/en/guidance-landing/data-processing-operations-require-data-protection-impact-assessment

[5] Regarding other legal bases, for example, Article 6(1) GDPR specifically states that public authorities cannot rely on the legal basis of 'legitimate interests' in performance of their tasks as public sector bodies; similarly, if a public authority were to seek to rely on the legal basis of 'consent' they would have to ensure that the consent was 'freely given' which can be difficult to establish where there is a significant imbalance of power between the data subject and the controller.

[6] The DPC recognises that, whilst data sharing arrangements need to have a basis in primary legislation, public sector bodies may, at a later juncture and in advance of any data sharing, outline the details of the arrangement by prescribing same in secondary legislation such as a statutory instrument or via a regulatory measure such as a Memorandum of Understanding which is laid before the Houses of the Oireachtas.

place to protect the data rights of the individual. Prior consultation with the DPC, as per Article 36(4) GDPR, will also be a requirement during the preparation of such a proposal.

Alternatively, in certain cases of public sector data sharing, personal data may be shared between public bodies for the purposes of law enforcement. Where processing of personal data is undertaken for such purposes, it is likely to be covered by the LED, rather than the GDPR. The LED is transposed into Irish Law through Part 5 (i.e. sections 69-104) of the Data Protection Act 2018. The equivalent of a legal basis under the LED is that the processing must be for necessary for the performance of a function of a 'competent authority' (defined by section 69) for the purposes of 'the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against, and the prevention of, threats to public security', or 'the execution of criminal penalties'.

Transparency

The Law

Personal data must be obtained and processed in a transparent manner. With regard to public bodies' obligations under the principle of transparency, there are specific obligations to provide data subjects with information in Articles 13 and 14 GDPR; where a public body obtains the personal data directly from a data subject, and, where a public body obtains the personal data through some other means, respectively.

In the first case, as per Article 13 GDPR, where personal data are gathered directly from the data subject, a data controller must provide (unless they already have the information) the following information at the time of obtaining the personal data:

- Identity and contact details of the of the data controller;
- The contact details for the Data Protection Officer (DPO) (if applicable);
- Purpose of and legal basis for the data sharing;
- Any other recipient(s) of the personal data;
- Details of any intended transfers to a third country (non-EU member state) or international organisation and details of adequacy decisions and safeguards;
- The retention period (how long the data controller holds onto data) or, if that is not possible, the criteria used to determine the retention period;
- The existence of the data subject's various rights;
- Where processing is based on consent, the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before withdrawal;
- The right to lodge a complaint with the DPC;
- Whether the provision of personal data is a statutory requirement or obligation, and the possible consequences of failing to provide the personal data; and
- The existence of any automated decision making processes that will be applied to the personal data, including profiling, and meaningful information about how decisions are made, the significance and the consequences of processing.

In the second case, where the personal data has been obtained by the public body otherwise than directly from the data subject, Article 14 GDPR also provides that a data controller must provide in

addition to the above information the following information, within a reasonable period (at least within one month):

- The categories of personal data concerned; and
- The source from which the personal data were obtained, and whether they came from a publically accessible source.

There is thus a clear obligation to inform data subjects how their personal data are or will be processed, and processing will not be considered fair, lawful, and transparent unless the data subject is given specific information about the identity of the controller, who the information will be disclosed to, and the purposes for which the data are to be processed.

The rationale behind these transparency requirements is that if the processing is to be fair the data subject must be placed in a position to learn of the existence of the processing operation, have access to that information, and consequently be able to exercise their rights as a data subject with regard to the processing of their personal data.

The DPC also recommends that public sector data controllers consider the guidelines on transparency requirements under the GDPR which were produced by the Article 29 Working Party and then endorsed by the European Data Protection Board (the 'EDPB' – the successor to the Article 29 Working Party).[7]

Exceptions and Restrictions

The only general exception to the requirement to provide information under Article 13 GDPR, is where the data subject already has the information. Under Article 14 GDPR, where the personal data has been obtained from a source other than the data subject, public bodies may not be required to furnish certain information where the data subject already has the information, but also in cases where provision of the information would be impossible, involve disproportionate effort, or seriously impair the objectives of the data processing, or where the processing is required by law or the personal data must remain confidential subject to a professional or statutory obligation of secrecy.

Article 23 GDPR also mandates that specific Member State or Union Law (by specific legislative measures) may restrict the scope of rights and obligations provided for in Articles 12 – 22 and Article 34 (and Article 5 insofar as those principles correspond to the rights afforded in the aforesaid Articles). Article 23, by setting out an exhaustive list of requirements which must be met to lawfully impose a restriction, confirms that any measure used to restrict the rights of a data subject must be of limited scope and applied in a strictly necessary, proportionate and specific manner.

The Data Protection Act 2018 contains certain provisions dealing with the restrictions of rights of data subjects, including sections 59, 60 and 61 in particular, which give further effect to the provisions of Article 23 of the GDPR. The relevant provisions of both the GDPR and the Data Protection Act 2018 should be read together. Section 60 specifically deals with restrictions on obligations of controllers and rights of data subjects for important objectives of general public interest.[8]

---

[7] 'Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)', at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

[8] See the DPC's guidance on restrictions of rights on the basis of Article 23 GDPR, at https://www.dataprotection.ie/en/individuals/know-your-rights/restriction-individual-rights-certain-circumstances-article-23-gdpr

However, it is now settled European case-law that any exemptions should be applied on a very narrow basis in order to protect and uphold the fundamental data protection rights of the individual.[9] Any exemption impacting the data protection rights of individuals can only be relied upon where such an exemption is necessary and proportionate. Therefore, if a public body avails of an exception from the requirements to provide data subjects with certain information, they should be able to demonstrate that it is a necessary and proportionate measure, for example, where the release of this information would jeopardise the achievement of the data sharing objective.

The question for a public sector body to determine is whether they are satisfied that the explicit details of a data sharing arrangement, which are in the main outlined as part a wider legislative measure expressed in legalistic language, meet the transparency requirements and adequately inform data subjects under the GDPR and the Data Protection Act.

The DPC recommends that the default position should be that full details of all data sharing arrangements should be explained and outlined to the individuals concerned in plain language, by the public sector bodies involved.

How to Communicate

The DPC recognises that it is for each public sector body to determine how to inform an individual; however, public bodies should ensure that information is easily accessible, and thus data subjects should not have to seek it out – there should be clear links, signposts, and or pop-ups to lead them to the required information.

In some cases it may be acceptable to have an information notice available so people can access it if they want to – though this would need to be clearly signposted and easily accessible – especially when the data sharing is something people are likely to expect and be aware of already. However, in other situations this approach may not be acceptable and a notice, for example, may need to be actively and directly communicated (for example sending a letter, distributing an email, etc.) to each individual data subject, as failure to do so could result in unfairness to individuals.

Article 12 GDPR requires that information provided to data subjects be concise, transparent, intelligible, and easily accessible; clear and plain language must be used, particularly when providing information to children; it must be in writing or by other means, including where appropriate by electronic means; where requested, it may be provided orally. Data controllers must also endeavour to present information in an efficient and succinct manner which avoids information fatigue.

In determining the method of communication which is best suited the following non-exhaustive checklist should be considered:

- Is the public sector body sharing sensitive or 'special category' personal data?[10]
- Might the data sharing be unexpected or objectionable to individuals?
- Is the individual likely to suffer any detriment as a result of the data sharing arrangement?

[9] See for example the ECtHR cases of *Delcourt* (17 January 1970), and *Klass v Germany* (1978) highlighting that any limitations imposed on a fundamental right must be viewed restrictively and also note for example the ECJ joined cases of C- 293/12 & C-594/12 (*Digital Rights Ireland*)

[10] See Article 9 GDPR for the definition of and rules around 'special categories' of personal data, including: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data processed to uniquely identify a person; data concerning health; and data concerning a person's sex life or sexual orientation.

- Will the data sharing have a significant effect on the individual?
- Is the data sharing widespread or involving entities which individuals might not expect?
- Is the sharing being carried out for a range of different purposes?

If any of these questions are answered “Yes” it would strongly suggest that a public sector body may need to consider actively communicating the detail of the data sharing arrangement to each individual.

Who communicates?

It is important to ensure that the public sector bodies involved in data sharing work together to ensure that the individuals concerned know who has, or will have, their data and what it is being used for, or will be used for.

The primary responsibility for communicating to the individual should fall to the public sector body that collected the data initially. Furthermore, any data sharing arrangement should be reflected in a data sharing agreement which should set out appropriate common rules (including the communication responsibilities) between the bodies. The public sector body receiving the personal data also has an obligation to inform the individual.

Data Minimisation

As mentioned above, as part of any public sector data sharing arrangement, only the minimum amount of personal data necessary to achieve an objective should be shared, in line with the principle of ‘data minimisation’ as set out in Article 5 GDPR. The personal data should be ‘adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’. In many cases all that may be required is a "yes" or "no" in regard to whether an individual is, for example, a holder of a permit or a license.

Public bodies should also consider adopting internal policies and implementing measures which meet, in particular, the principles of data protection by design and data protection by default. Such measures could consist, for example, of minimising the processing, including storage, of personal data or pseudonymising or anonymising personal data as soon as possible.

Data Access and Security

Enhanced access controls and security requirements should apply to personal data shared and received as part of an approved data sharing arrangement, in line with public bodies’ obligations under the principle of data security, or ‘integrity and confidentiality’. Access to such data should be limited to a very small number of officials, and public sector bodies should employ a ‘need to know’ basis, thereby ensuring that other organisations should only have access to the data if they need it, and that only relevant staff within those organisations should have access to the data. Arrangements in this respect should also address any necessary restrictions on onward sharing of personal data with third parties.

Security measures should rule out any possibility of data leakage (bearing in mind the increased emphasis on the State's responsibility to prevent personal data breaches and the reputational damage that would result from failure to protect shared personal data). It is important that public

sector bodies ensure that the personal data will be protected at all stages of the arrangement, i.e. during the transmission, receipt of the data, and while the data remains with either party. Furthermore, it is important that the recipient organisation understands the nature and sensitivity of the data being shared and that common rules for its security are established.

From 25 May 2018, the also GDPR introduced a requirement for organisations to report personal data breaches to the relevant supervisory authority, where the breach presents a risk to the affected individuals. Organisations must do this within 72 hours of becoming aware of the breach. Where a breach is likely to result in a high risk to the affected individuals, organisations must also inform those individuals without undue delay. Similar obligations were introduced in the context of the LED in sections 85 and 86 of the Data Protection Act 2018.[11]

Data Retention

Personal data provided as part of an approved data sharing arrangement should be securely destroyed when no longer required. The DPC recommends that public bodies should specify the conditions and the period for which the data may be retained and that such conditions are necessary and proportionate in relation to the purpose to be achieved.

In line with the principle of 'storage limitation', as set out in Article 5 GDPR, personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; although they may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) GDPR, subject to implementation of appropriate technical and organisational measures.

As mentioned above, public bodies should also ensure that they inform data subjects of any relevant retention period(s) or, if that is not possible, the criteria used to determine the retention period for their personal data.

Governance

Any decision to share personal data between public must not be taken lightly. This is especially the case when bulk data are shared. Such decisions should only be taken following due consideration at senior management level.

Public sector bodies involved in a data sharing arrangement will have their own responsibilities and liabilities in respect of the personal data they process. It is important that those entities involved in a data sharing arrangement set out a common set of operational rules to be adopted in a data sharing agreement which is then reviewed on a regular basis to ensure that the data sharing initiative is meeting its objectives, that safeguards continue to match any risks posed, that records are accurate and up to date, that adherence to a consistent retention policy for all records is kept, and that the appropriate security measures remain in place.

A clear description of the roles and responsibilities of public sector bodies in any data sharing arrangement should be made available to the data subject, in particular to assist them in exercising their data protection rights.

[11] Further guidance on breach notifications can be found on the DPC's website, at https://dataprotection.ie/en/organisations/know-your-obligations/breach-notification

Similarly, in certain public sector data sharing arrangements, one entity may be acting as a 'data processor' for the data controller. The GDPR has obligations for both data controllers and data processors. One such obligation is the obligation on controllers and processors to enter into a legally binding contract governing the processing of personal data when a processor is engaged to process personal data on the instruction of a controller.[12]

Under the GDPR, certain data controllers are required to appoint a designated Data Protection Officer (DPO),[13] including all controllers who are public authorities or public bodies. Controllers are also required to publish the details of their DPO and provide these details to the DPC.[14] Public bodies should consider their obligations regarding the appointment of a DPO and the involvement of the DPO in the development of any data sharing arrangements.

And finally...

If a public sector body informs people about their data sharing arrangement and consequently receives a significant number of negative comments or concerns it should review the arrangement and data sharing in question.

In particular, the body should carry out an analysis of the issues raised and decide whether the sharing can go ahead or continue. Alternatively, it may need to reduce the amount of data it shares or share it with fewer organisations.

In large scale data sharing operations, it is good practice to set up focus groups to explore individuals' concerns and to develop more publicly acceptable ways of dealing with the issues that the data sharing was intended to address.

[12] For more detail on such contracts, see the DPC's 'Practical Guide to Data Controller to Data Processor Contracts under GDPR', at https://www.dataprotection.ie/en/organisations/know-your-obligations/controller-and-processor-relationships

[13] See the DPC's 'Guidance on appropriate qualifications for a Data Protection Officer', at https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-officrs/guidance-appropriate-qualifications

[14] For more detail on the requirements regarding DPOs, see the Article 29 Working Party 'Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)', (endorsed by the EDPB), at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048