Lockstown Practice

Data Protection Impact Assessment Policy & Template

Document History

Document Reference:	DPIA
Document Purpose:	This Policy provides advice when a DSA or DPC needs to be completed, and its suggested contents.
Date Approved:	11 January 2024
Version Number:	1.1
Status:	FINAL
Next Revision Due:	January 2025
Developed by:	Paul Couldrey – IG Consultant
Policy Sponsor:	Practice Manager
Target Audience:	This policy applies to any person directly employed, contracted, working on behalf of the Practice or volunteering with the Practice.
Associated Documents:	All Information Governance Policies and the Information Governance Toolkit, and Data Security and Protections Toolkit 2023/24

Introduction

A data-sharing agreement between the parties sending and receiving data can form a major part of your compliance with the accountability principle, although it is not mandatory. A data-sharing agreement is a formal contract between two or more data **Controllers** covering what happens to the data at each stage, what data is being shared and how the information will be used. It sets standards and helps all the parties involved in sharing clarify the roles and responsibilities.

Your organisation might use a different title for a data-sharing agreement, for example:

- an information-sharing agreement.
- a data or information sharing protocol or contract; or
- a personal information-sharing agreement.

It is not necessarily important what your organisation calls it, but it is important and good practice to have a data-sharing agreement in place.

Government departments and certain other public bodies (for example, regulators, law enforcement bodies and executive agencies) may enter a memorandum of understanding with each other that includes data-sharing provisions and fulfils the role of a data-sharing agreement.

However, on their own, the following do not constitute a data-sharing agreement:

- a memorandum of understanding (except between government departments and certain other public bodies);
- a list of standards; or
- an addendum to a purchase agreement or to a purchase order or proposal.

What is a data-sharing agreement?

A data-sharing agreement is an agreement between two or more data **Controllers** (organisations decide how to use the data shared) covering what happens to the data at each stage, what data is being shared and how the information will be used. It sets standards and helps all the parties involved in sharing clarify the roles and responsibilities.

What are the benefits of a data-sharing agreement?

A data sharing agreement:

- helps all the parties be clear about their roles;
- sets out the purpose of the data sharing;
- covers what happens to the data at each stage; and
- sets standards.

It should help you to justify your data sharing and demonstrate that you have been mindful of, and have documented, the relevant compliance issues. A data-sharing agreement provides a framework to help you meet the requirements of the data protection principles.

There is no set format for a data-sharing agreement; it can take a variety of forms, depending on the scale and complexity of the data sharing. Since a data-sharing agreement is a set of common rules that binds all the organisations involved, you should draft it in clear, concise language that is easy to understand.

Drafting and adhering to a data-sharing agreement should help you to comply with the law, but it does not provide immunity from breaching the law or from the consequences of doing so. However, the ICO will consider the existence of any relevant data-sharing agreement when assessing any complaint, we receive about your data sharing.

What is a data-processing Contract?

A data processing contract is very similar to a data sharing agreement, but this is an agreement issued by a Controller to a Data **Processor**, (an organisation that does contracted work on your behalf and cannot decide for itself how to process the data)

If your organisation is subject to the UKGDPR, you must have a written data processing agreement in place with all your data processors.

When is a contract needed and why is it important?

Whenever a controller uses a processor to process personal data on their behalf, a written contract needs to be in place between the parties.

Similarly, if a processor uses another organisation (ie a sub-processor) to help it process personal data for a controller, it needs to have a written contract in place with that sub-processor.

Contracts between controllers and processors ensure they both understand their obligations, responsibilities, and liabilities. Contracts also help them comply with the UKGDPR and assist controllers in demonstrating to individuals and regulators their compliance as required by the accountability principle.

What needs to be included in the contract?

Contracts must set out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the controller's obligations and rights.

Contracts must also include specific terms or clauses regarding:

- processing only on the controller's documented instructions;
- the duty of confidence;
- appropriate security measures;
- using sub-processors;
- data subjects' rights;
- assisting the controller;
- end-of-contract provisions; and
- audits and inspections.

What responsibilities and liabilities do controllers have when using a processor?

Controllers must only use processors that can give sufficient guarantees they will implement appropriate technical and organisational measures to ensure their processing will meet UKGDPR requirements and protect data subjects' rights.

Controllers are primarily responsible for overall compliance with the UKGDPR, and for demonstrating that compliance. If this isn't achieved, they may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

What responsibilities and liabilities do processors have in their own right?

In addition to its contractual obligations to the controller, a processor has some direct responsibilities under the UK GDPR. If a processor fails to meet its obligations or acts outside or against the controller's instructions, it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

A processor may not engage a sub-processor's services without the controller's prior specific or general written authorisation. If authorisation is given, the processor must put in place a contract with the sub-processor. The terms of the contract that relate to Article 28(3) must offer an equivalent level of protection for personal data as those in the contract between the controller and processor. Processors remain liable to the controller for the compliance of any sub-processors they engage.

What should you include in a data-sharing or processing agreement?

Within the agreement, you should address a range of questions so that nothing is missed; below are a few to consider:

- **The purpose of the data sharing**

In the agreement, you will need to explain why the information is being shared, the benefits, and how it will help you achieve the objectives.

- **Other organisations are involved**

You must identify all the organisations or legal entities involved with the data sharing, and you must provide the contact details for each of those Controllers or Processers

- **Information is being shared with another controller**

If your organisation has joined with another organisation to have joint data controllers, you must set out their responsibilities in writing as it is a legal obligation. A data flow map can be a very easy way to achieve this.

- **What data is going to be shared?**

You will need to specify the types of, and categories of data you will be sharing; this will need to be detailed, for example, standard or special category, the types of individuals, such as employees, students, website visitors, etc.

- **The lawful basis for sharing**

You and all the organisations involved will need to document a lawful basis for processing and sharing personal data. The organisations will each need to consider this, as the lawful basis may differ from one organisation to another.

- **Special category data**

This includes any information related to the individual's race, religion, political opinions, health information, sexual orientation, genetic information, and criminal offence data.

- **Data subject rights**

In your data sharing or data processing agreements, you should ensure that your processing activities respect the rights of individuals and ensure that they can activate their rights. This includes them having the right to access the data, objecting to the processing, and having a mechanism for requesting that their data be rectified or removed.

- **International transfers**

When you are dealing with transfers to insecure third countries, such as the US, you need to embed certain terms called standard contractual clauses (SCC) which in essence embed the key elements of the GDPR into an enforceable contract. At the time of writing the EU have issued new **SCC templates,** however, the UK is still waiting for the ICO to authorise wording for non-EU-UK agreements – see consultation document.

- **The small print**

Agreements will vary and you need to ensure caveats are included to do with ownership of information, retention, who is responsible for reporting breaches, managing subject access requests, and compensation claims.

In the agreement, you must make it clear that all controllers and processors remain responsible for compliance, whilst ultimately the controller is always liable, you should ensure that the agreement states that the processor is liable if the breach was their fault.

- **Appendix or Annex**

It will be constructive for your agreement to summarise the key legislation and other legal provisions, e.g., relevant sections of the Data Protection Act 2018.

If Processors are required to gain consent on your behalf, then providing a model form or template wording for seeking the individual's consent would be useful. As stated previously, data flow maps or diagrams are very useful in showing how data will flow and roles and responsibilities.

When should I review my data-sharing agreement or data-processing contract?

Reviewing your data sharing or data processing agreements should be done regularly, especially if there is a change throughout the agreement. Also, if there is a complaint or a potential security breach, you should immediately review the arrangement and update the agreement to reflect any changes.