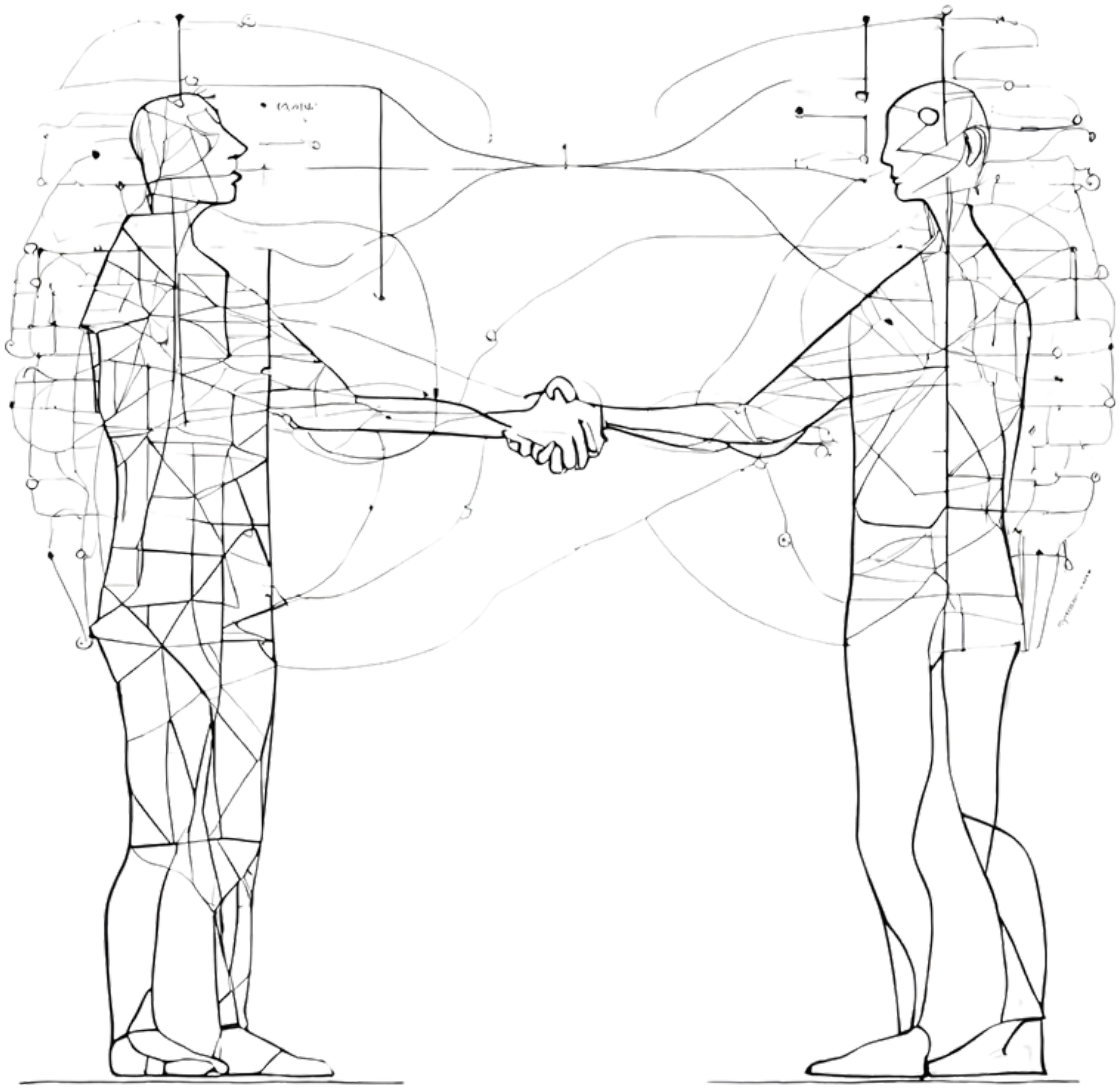
THE OFFICE OF THE
Data Protection
Authority

# GUIDANCE: Data sharing



**2024 issue**

# Data Sharing: a simple guide

This guidance is for anyone who works with information about people and wants to share that information with others when appropriate and in a way that complies with *The Data Protection (Bailiwick of Guernsey) Law, 2017* ('The Law'). This guidance applies to you in your role as a 'controller' or 'processor' of personal data under the Law.

## What is data sharing?

Data sharing is the practice of giving or making personal data available to other controllers.

It is used to make it simpler for other controllers to use the personal data and to collaborate effectively. Appropriately managed and shared personal data allows controllers to work with the most recently available information, avoids duplication and supports better outcomes.

The Law protects the rights of individuals in relation to their personal data and provides for the free movement of personal data.

Some **key things to remember** about data sharing:

1. The Law facilitates data sharing when you approach it in a **fair and proportionate** way.
2. The Law is an **enabler** for fair and proportionate data sharing, rather than a blocker. It provides a framework to help you make decisions about sharing data appropriately.
3. This guidance helps you to balance the **benefits and risks** and implement data sharing.
4. Data sharing has **benefits** for society as a whole when done properly.
5. Sometimes it can be **more** harmful not to share data.
6. When considering sharing data:
    - you must **comply** with the Law;
    - we recommend that you **assess the risks** using a Data Protection Impact Assessment (DPIA); and
    - it is good practice to have a **data sharing agreement** in place.

Remember that the Law only applies where the sharing involves **personal data** – i.e. information relating to identified or identifiable living individuals.

## Understanding your role – Controller/Processor

- A controller is any entity[1] that is **responsible for the decisions made** about **why** and **how** it uses personal data.

[1] this entity would normally be an organisation, but it could be a specific human being (e.g. sole traders, landlords, elected officials etc).

- A processor is any entity[2] that is **given the task** of processing personal data by a **controller**. Processors **do not** determine the nature or the means of the processing, they just do what the controller tells them to do. If you are part of such an arrangement you need to have in place a written, legally binding Controller/Processor agreement.

## What types of data sharing are there?

Data sharing falls into three broad categories:

1. The sharing of personal data with a third party to be used for **joint purposes (joint controller).**

2. The passing of personal data to a third party for it to use for **its own purposes (controller)**.

3. Engaging a third party to handle, store or otherwise use certain personal data **on your behalf (processor)**.

On occasion, the sharing of personal data is obligatory under law, but usually it is at your assessment or discretion whether to share personal data.

## General points to bear in mind in advance of sharing personal data.

**Before** sharing personal data, make sure that:

- there is a **valid reason** for the sharing to take place (e.g. to meet a contractual obligation or some other legal basis);
- if you are relying on consent as the legal basis for sharing personal data, you have **obtained specific, informed and freely given consent** from the individual(s) concerned;
- the **category**(s) of personal data to be shared are clearly defined;
- the **roles and responsibilities** of the controller(s) and processor(s) are clearly defined;
- consideration has been given as to how to share the **minimum** amount of personal data necessary to achieve the purpose;
- the sharing is done as **securely** as appropriate for the data involved (e.g. by tracked/signed-for post or courier delivery, encrypted file transfer or password-controlled access rights);
- the sharing is for the minimum **time** necessary, and it is clear what happens to the data at the end of the data sharing agreement;
- the sharing has been **documented**; and, very importantly; where appropriate, the **individuals have been made aware** that their data is being shared.

[2] this entity would normally be an organisation, but it could be a specific human being (e.g. sole traders, landlords, elected officials etc). Examples of processors are **outsourced provisions** such as IT providers, cleaners, paper shredding companies and payroll.

In your data sharing agreement, you should have policies and procedures that allow data subjects to exercise their individual rights easily.

You can share data in an emergency, where it is necessary and proportionate. Examples of an emergency situation are where there is a risk of serious harm to human life, or the immediate need to protect national security.

## Data sharing principles

When sharing personal data, you must follow the seven key principles in data protection legislation:

**1. Lawfulness, Fairness & Transparency.**
You must have a **valid legal reason** for processing personal data. You must obtain it without deceiving the person whose data it is, and you must make it clear exactly how you are going to use their data.

**2. Purpose Limitation.**
You must **only** use personal data for the reason (or reasons) you have told the person you are using it for.

**3. Minimisation.**
You must only ask for the **minimum amount** of personal data necessary from the person.

**4. Accuracy.**
You must ensure that any personal data you hold is **accurate** and where necessary, up-to-date.

**5. Storage Limitation.**
You must not keep personal data for **longer** than you need it for.

**6. Integrity & Confidentiality.**
You must keep personal data **safe** so that it does not get accidentally deleted, changed or seen by someone who is not allowed to see it.

**7. Accountability.**
This is the foundation on which the other six principles rest. You must be able to evidence your accountability by **showing how you take responsibility** for what you do with people's data.

## Sharing data outside of the Bailiwick of Guernsey

Additional safeguards should be considered when sharing personal data outside of the Bailiwick, to ensure that appropriate safeguards are in place. This is known as a 'data transfer'.

It is important to understand that 'data transfers' and 'data sharing' are different things:

- 'Transfers' are related to the **geographical** location of data and how it moves around.

- ‘Sharing’ normally relates to an organisation **giving a third-party** access to data or otherwise providing data to them.
- So bear in mind that if you are sharing someone’s information with a third-party outside the Bailiwick you are **sharing data via a ‘data transfer’**.

If you are planning to send someone’s data outside the Bailiwick, the first thing you need to do is check whether the intended third-party is in an “authorised jurisdiction”. Transfers to authorised jurisdictions can be made without any extra consideration regarding the transfer. Transfers to unauthorised jurisdictions will require an additional and appropriate safeguard, such as Standard Contractual Clauses. For further information about data transfers, please refer to our data transfers page on our website.

**Help and advice**

If after reading the above guidance you need further clarification on your specific circumstances, please visit the Contact Us page of our website for details of our free drop-ins, and our contact information.