ORGANISATIONS

DATA SHARING AND SUBJECT ACCESS **CHECKLIST**

digital **TOOLKIT**

Guidance for Organisations

This document is purely for guidance and does not constitute legal advice or legal analysis. It is intended as a starting point only, and organisations may need to seek independent legal advice when renewing, enhancing or developing their own processes and procedures or for specific legal issues and/or questions.

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

Data Sharing and Subject Access Checklist

Data sharing policy

Does your business have communicated policies, procedures and guidance to all staff that clearly set out when they are allowed to share or disclose data?

Your policies, procedures and guidance should set out how your staff ought to respond to sharing requests. Any sharing of data must comply with the law, be fair, transparent and in line with the rights and expectations of the individuals whose data you are sharing. Your policy should explain how you will achieve compliance with these requirements, e.g. monitor information sharing logs, quality assess samples of instances of sharing.

Your policy should also link in with your Data Protection Impact Assessment ('DPIA') policy or process, as you should carry out a DPIA on any data sharing that poses a high risk to the rights and freedoms of individuals. You should communicate this policy to all staff, e.g. via your intranet.

Accountability

Has your business assigned responsibility to an appropriate member of staff for ensuring effective data sharing?

It is good practice to nominate a senior, experienced person to take overall responsibility for information sharing (including deciding what information can be shared), ensure compliance with the law, and provide advice to staff making decisions about sharing.

Your policy should make it clear who this person is and how to contact them.

You should also provide specialist training to this individual to allow them to fulfil their role.

Staff training

Does your business provide adequate training on an ongoing basis for staff that regularly make decisions about whether to share personal data with third parties?

It is essential to provide appropriate training to staff who are likely to make significant decisions about personal data sharing or have access to shared data. The nature of the training will depend on their role within the sharing process. You can incorporate this into any training you already give on data protection, security, or legal obligations of staff.

You should also maintain staff awareness through materials such as posters, office wide emails, intranet updates or data sharing content in newsletters.

Data sharing records

Decision log

Does your business maintain a log of all your decisions to share personal data and you review this regularly?

Your business should be able to justify the reasons why you decided to share specific personal data. Sharing should be lawful and comply with any statutory restrictions. In addition you must be able to establish your appropriate lawful basis for the sharing (processing) set out in data protection legislation.

Data sharing agreements

Does your business have a data sharing agreement (DSA) *with any party you routinely share personal data with or transfer large quantities of data to? Do you review these agreements regularly?*

In some instances you may need to agree and formalise the way you share personal data. This may be due to the number of requests you receive from a particular organisation or because you have introduced a new process that means you need to share large quantities of data.

Prior to introducing a DSA, you should complete and record a Data Protection Impact Assessment (DPIA). This helps you to demonstrate that your business has legal authority to share the information and that the sharing complies with relevant data protection legislation.

Your DSA should address all risks relevant to the type of sharing you are undertaking.
As a minimum, it should address:

- The purpose or purposes of the sharing;
- The potential recipients or types of recipient and the circumstances in which they will have access;
- The data you will share (this should be kept to the minimum necessary for your purposes);
- Data quality – accuracy, relevance, usability etc;
- Data security - this covers responsibilities relating to technical, physical and operational security;
- Retention of shared data;
- Individuals' rights – procedures for dealing with access requests, queries and complaints;
- Review of effectiveness/termination of the sharing agreement;
- Sanctions for failure to comply with the agreement or breaches by individual staff.

You should review these arrangements regularly. You should check whether you still need the data to fulfil the purposes you are sharing it for and whether the DSA still reflects current data sharing arrangements.

Privacy information

How does your business inform individuals about the sharing of their personal data?

You must process personal data fairly and lawfully. In order for processing to be considered fair, you need to explain to individuals how you will use their personal data, who you will share it with and why. You should include this information in your privacy notice. It should clearly explain the reasons why you are using the data including any disclosures or arrangements for sharing.

Security measures

Does your business have appropriate security measures in place to protect data that is in transit, received by your business or transferred to another business?

Your business must have appropriate technical and organisational measures in place to protect the personal data that you share.

It is therefore important that you set out, and ensure compliance with, agreed levels of security when you share personal data.

In addition, when transferring data between organisations you should take appropriate measures to ensure its security while in transit. This may include the use of encryption on email, secure file transfer protocol (SFTP) or Virtual Private Network (VPN) for electronic files. Equally you should have equivalent security around paper documents in transit. Controls might include using a reliable courier or other secure postage, locked containers or tamper evident packaging.

Process for personal data requests

Does your business have a documented process for dealing with requests for personal data that all your staff are aware of and you have effectively implemented?

You should assign responsibility for responding to requests for personal data to one or more individuals.

You should have a documented process for dealing with requests for personal data efficiently and in accordance with data protection legislation.

Management should approve this process and you should make it readily available to staff.

The process should also include details about how to:

- Seek verification of the requestors identity;
- Calculate any administrative fees (if applicable);
- Find and retrieve the information requested;
- Comply with the timescales for response;
- Log the request and manage each stage of the response process;
- Apply exemptions if applicable;
- Redact information if applicable;
- Quality check responses.

You must provide information in response to a request free of charge. However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. You may also charge a reasonable fee to comply with requests for further copies of the same information. You must base the fee on the administrative cost of providing the information.

You may find it useful to produce a checklist to summarise and track each stage of the process.

You should retain copies of your responses for audit purposes.

Accountability and training

Has your business appropriately trained all personnel who have responsibility for processing requests for personal data? Have you made them aware of how to identify and channel requests to the appropriate team or person?

You should train all staff on their responsibilities to identify, process and escalate requests. You should provide training at the time of their appointment (or shortly thereafter) and relevant updates at regular intervals thereafter to maintain their awareness. Awareness materials might include 'on the job' training, posters, office wide emails, intranet updates and newsletters.

Staff with specific responsibilities such as processing, logging or overseeing responses to requests for personal data should receive appropriate training in order to allow them to carry out their role effectively.

Compliance monitoring

Does your business monitor and review all requests relating to the sharing of personal data and, where necessary, implement additional measures to improve compliance with data protection legislation?

You should periodically review your documented process and, where appropriate, update it to ensure it remains adequate and relevant.

You should have mechanisms to regularly monitor and report on agreed performance measures, and apply any recommendations or lessons learned in a timely fashion.

Your business should consider maintaining records that show measures and reporting, e.g. management information/KPI, meeting minutes, emails, etc.

You could introduce periodic compliance checks and audits to demonstrate any reviews of your process.