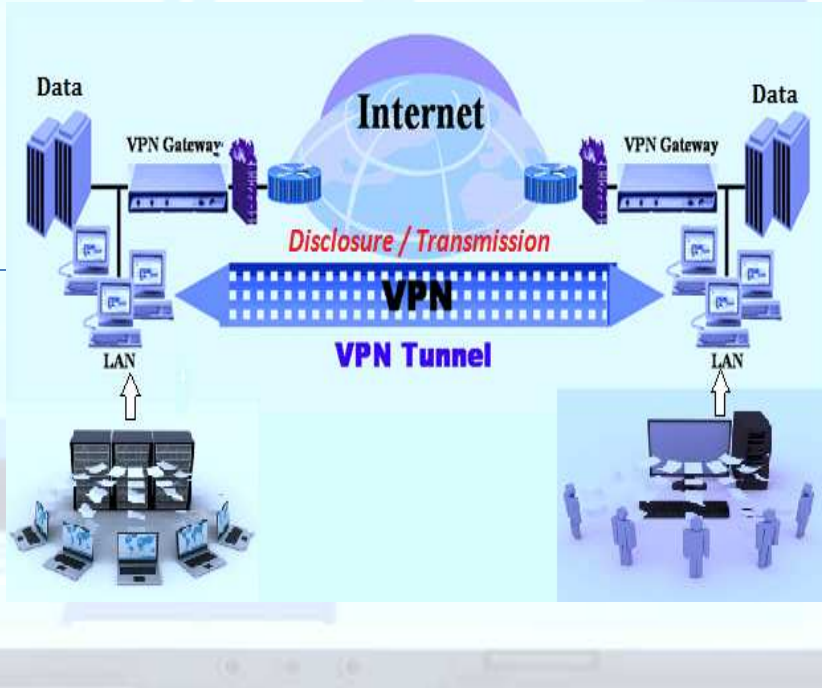
Data Protection Office

PRACTICAL NOTES ON DATA SHARING GOOD PRACTICES FOR THE PUBLIC AND PRIVATE SECTOR



Mrs. Drudeisha Madhub (Barrister-at-Law)
Data Protection Commissioner

Volume 9

Table of Contents

Data Sharing

By 'Data Sharing' is meant the disclosure or transmission of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of the same organisation. Data sharing is definitely a good practice, but it has to be balanced with the protection of individual privacy.

Data sharing normally takes place in a variety of situations:

- several organisations collecting information and disclosing to each other;
- several organisations collecting information and disclosing to a third party/ies;
- one-off disclosures of data in unexpected or emergency situations; or
- different parts of the same organisation disclosing to each other.

Before sharing any personal data you manage, you must consider all the express and implied legal implications. Your power to share information is subject to a number of legal constraints which normally go beyond the requirements of the Data Protection Act (DPA) such as specific statutory prohibitions on sharing found in diverse pieces of legislations, copyright restrictions or a duty of confidentiality that may affect your power to share personal data. A duty of confidentiality may be expressly provided or implied depending on the nature of the information – medical or banking information, for example. You may need to seek your own legal advice on these issues.

Some data sharing do not involve collection of personal data at all, for example where only statistics collected are shared without identifying any living individual. The DPA does not apply to anonymous data. For instance, records may be shared for research or data matching purposes. Technically a unique identifier such as a National Social Security or Identity Card Number is used and an encryption software.

You need to ask yourself these questions before effecting data sharing:-

Is the sharing justified?

- ✓ Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- ✓ Is the sharing proportionate to the issue you are addressing?
- ✓ Could the objective be achieved without sharing personal data?

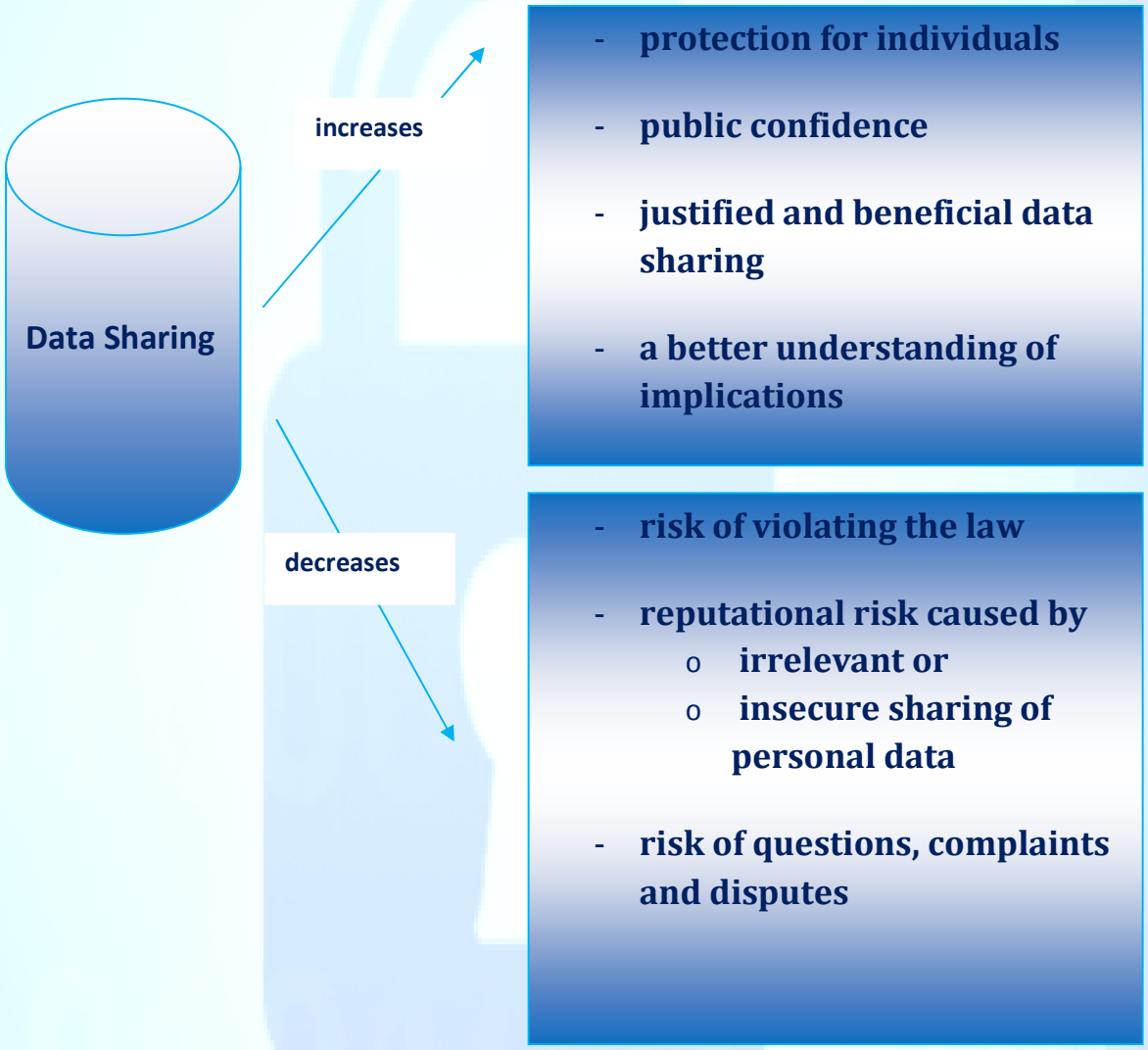
Do you have the legal power to share?

- ✓ The nature of the information you have been asked to share (for example is it confidential?).
- ✓ Any legal obligation to share information (for example a statutory requirement or a court order).

Although the DPA sets out the broad legal requirements to be considered when sharing personal data, it provides no guidance on the practical measures to be taken for compliance.

There is a multitude of benefits that may be acquired by data controllers and processors through data sharing which include:

- minimised risk of violating the law and consequent enforcement action by the DPO or other regulators;
- increased public confidence by ensuring that legally required safeguards are complied with;
- increased protection for individuals when their data is shared;
- increased justified and beneficial data sharing;
- reduced reputational risk caused by the irrelevant or insecure sharing of personal data;
- a better understanding of when, or whether, it is acceptable to share information without people's knowledge or express consent or in the face of an objection; and
- reduced risk of questions, complaints and disputes about the manner in which personal data is shared.


Data Sharing
increases
- protection for individuals
- public confidence
- justified and beneficial data sharing
- a better understanding of implications
decreases
- risk of violating the law
- reputational risk caused by
o irrelevant or
o insecure sharing of personal data
- risk of questions, complaints and disputes

The public sector

Most public sector organisations such as para-statals, other than government departments headed by a Minister, derive their powers entirely from an Act of Parliament which sets them up or from other such legislations regulating their activities. Your starting point in deciding whether any data sharing initiative may proceed should be to identify the legislation that is relevant to your organisation. Even if it does not cater for data sharing explicitly, and usually it will not do so, it is the founding stone which can guide you.

The relevant legislation normally defines the organisation's functions in terms of its objects, and the powers which the organisation may exercise in order to achieve those purposes. So it is necessary to identify where the data sharing in question would fit, if at all, within the range of activities that the organisation should carry out. Broadly speaking, there are three ways in which it may do so:

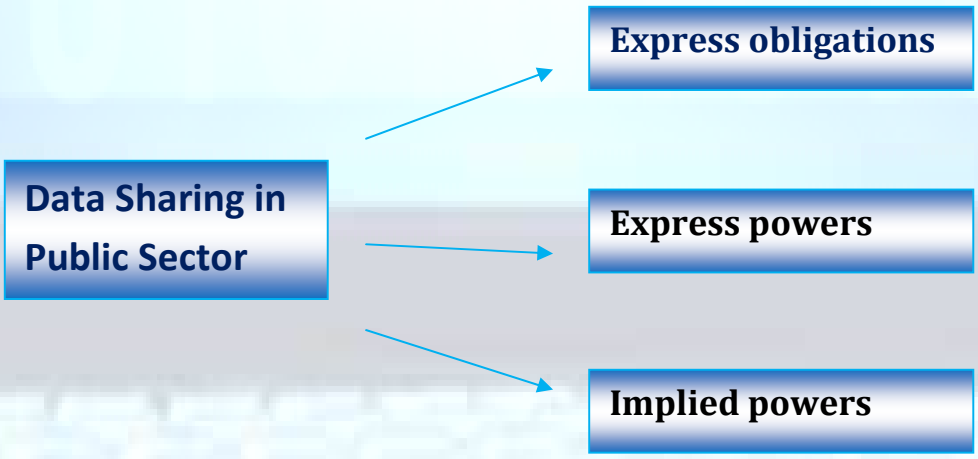
Express obligations –For instance, a public body may be legally obliged to share specific information with an organisation.

Express powers – A public body may be granted express power to share information by law to allow disclosure of information for specific purposes. Express statutory obligations and powers to disclose information are commonly called "gateways".

Implied powers – Often, the legislation regulating a public body's activities is silent on the issue of data sharing. In these circumstances it may be possible to rely on an implied power to share information derived from the express provisions of the legislation. This is because express statutory powers may be taken to authorise the organisation to do other things that are reasonably incidental to those which are expressly permitted.

To decide if you can rely on an implied power, you will need to identify the activity to which the proposed data sharing would be "reasonably incidental", and then check that the organisation has the power to engage in that activity.

Whatever the source of an organisation's power to share information, you must check that the power covers the particular disclosure or data sharing arrangement in question – otherwise, you must not share the information unless, in the particular circumstances, there is an overriding public interest in a disclosure taking place. Whilst a disclosure in the public interest may be a legal defense in a particular case, it does not constitute a legal power to share data.

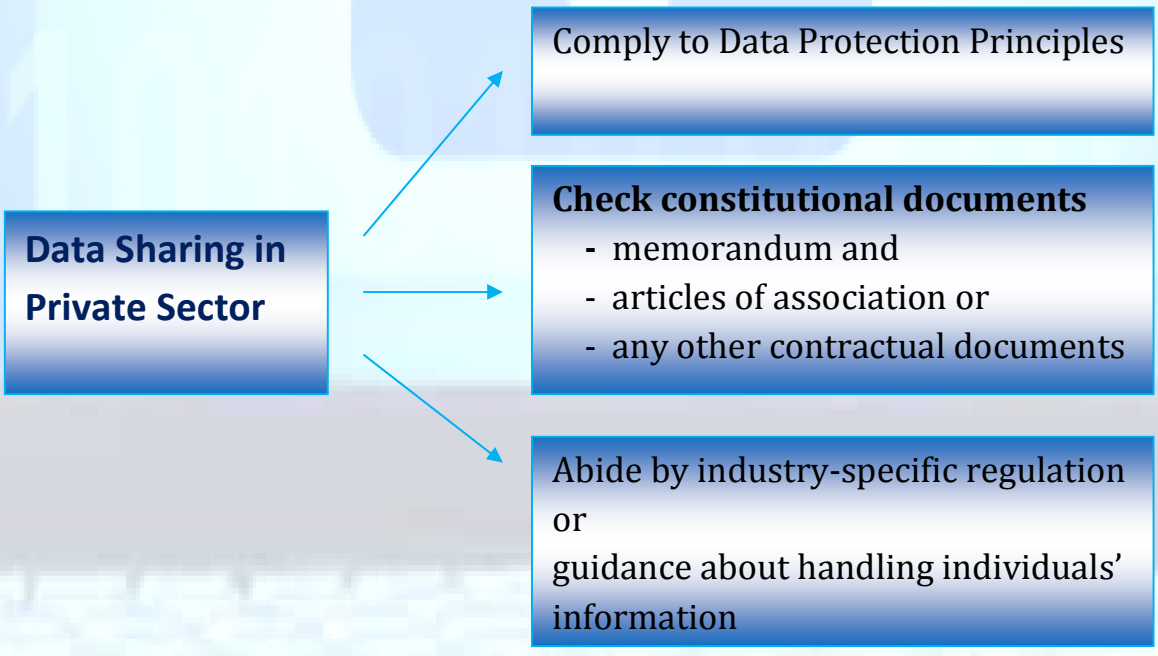


Private and Third Sector Organisations

The legal framework that applies to private and third sector organisations differs from that which applies to public sector organisations, which may only act within their statutory powers.

However, all organisations are required to comply fully with data protection principles. It is advisable for a company to check its constitutional documents, such as its memorandum and articles of association or any other contractual documents, to make sure there are no restrictions that would prevent it from sharing personal data in a particular context.

Private and third sector organisations should also have regard to any industry-specific regulation or guidance about handling individuals' information as this may affect the organisation's ability to share information.



Sharing with a 'data processor'

This guide is mainly about sharing personal data between data controllers – i.e. where organisations determine the purposes for which and the manner in which the personal data is processed.

However, there is a form of data sharing where a data controller shares data with another party that processes personal data on its behalf. In the DPA, these organisations are termed 'data processors'.

The DPA draws a distinction between one data controller sharing personal data with another, and a data controller sharing data with its data processor. The DPA requires that a data controller using a data processor must ensure, in a written contract, that:

- the processor only acts on instructions devolving from the data controller; and
- it has appropriate security and organisational measures in place equivalent to those imposed upon the data controller by the seventh data protection principle.

Thus, a data processor involved in data sharing does not have any direct data protection responsibilities of its own; they are all imposed on it through its contract with the data controller.

Data Sharing with a Data Processor

A data controller using a data processor must ensure, in a written contract, that:

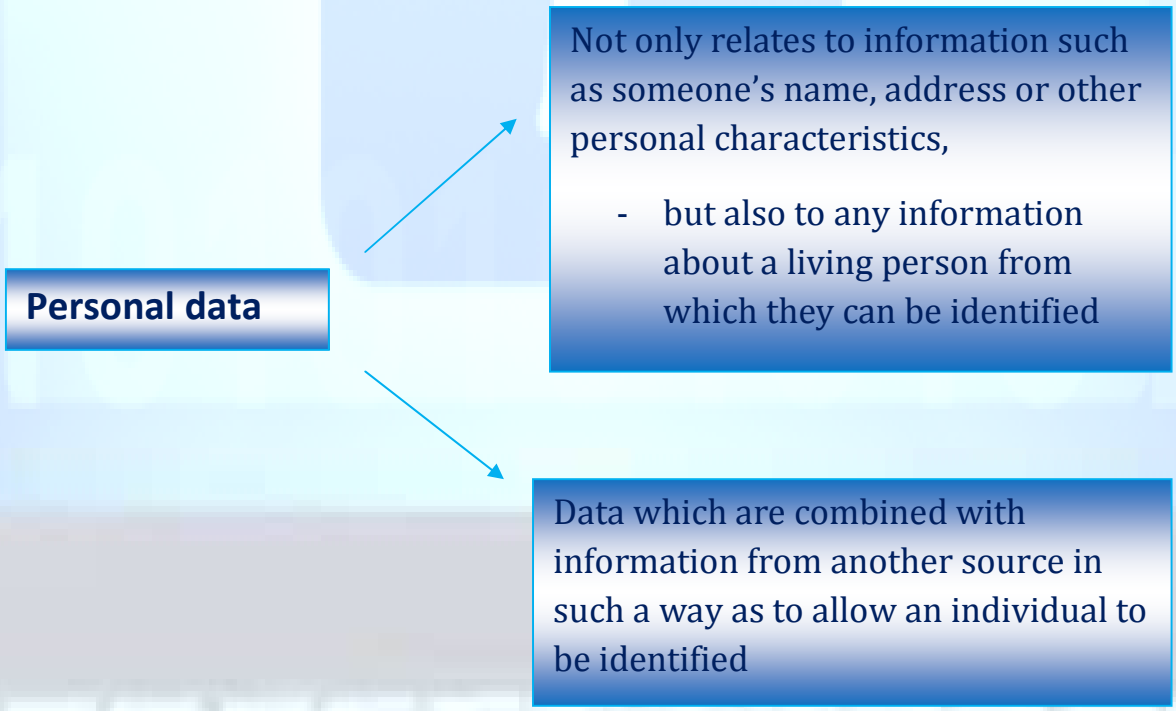
- the processor only acts on instructions devolving from the data controller; and
- it has appropriate security and organisational measures in place equivalent to those imposed upon the data controller by the seventh data protection principle.

A data processor involved in data sharing

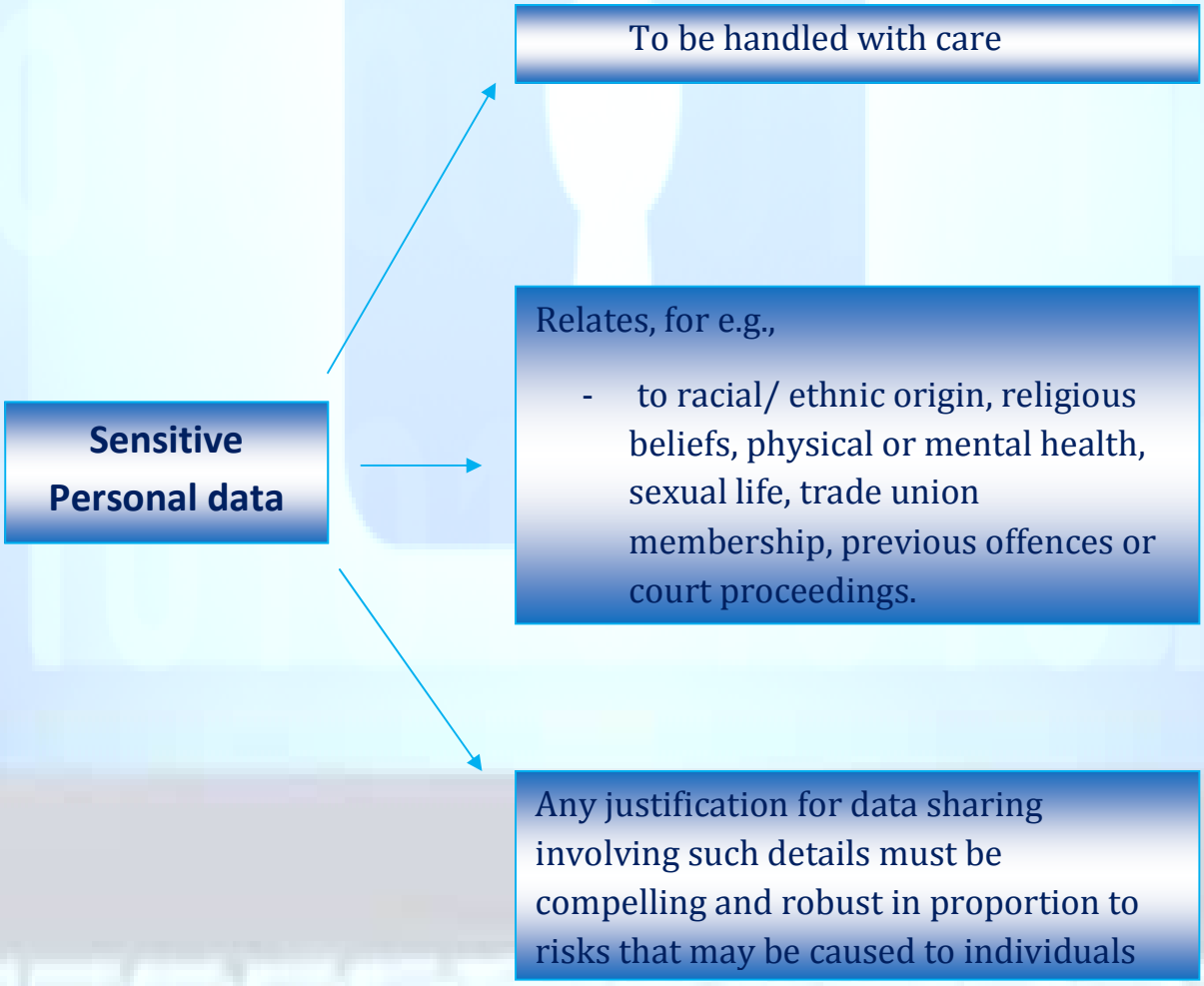
- does not have any direct data protection responsibilities of its own; they are all imposed on it through its contract with the data controller

Personal data:-

First, there is a need to understand that 'personal data' not only relates to information such as someone's name, address or other personal characteristics, but also to any information about a living person from which they can be identified. This means, for example, that even in making a request for statistical data from another organisation, there could still be a risk of disclosing the people concerned (eg, where there are very small numbers of the specified population in a particular neighbourhood). Data primarily not personal can also become 'personal' if they are combined with information from another source in such a way as to allow an individual to be identified.

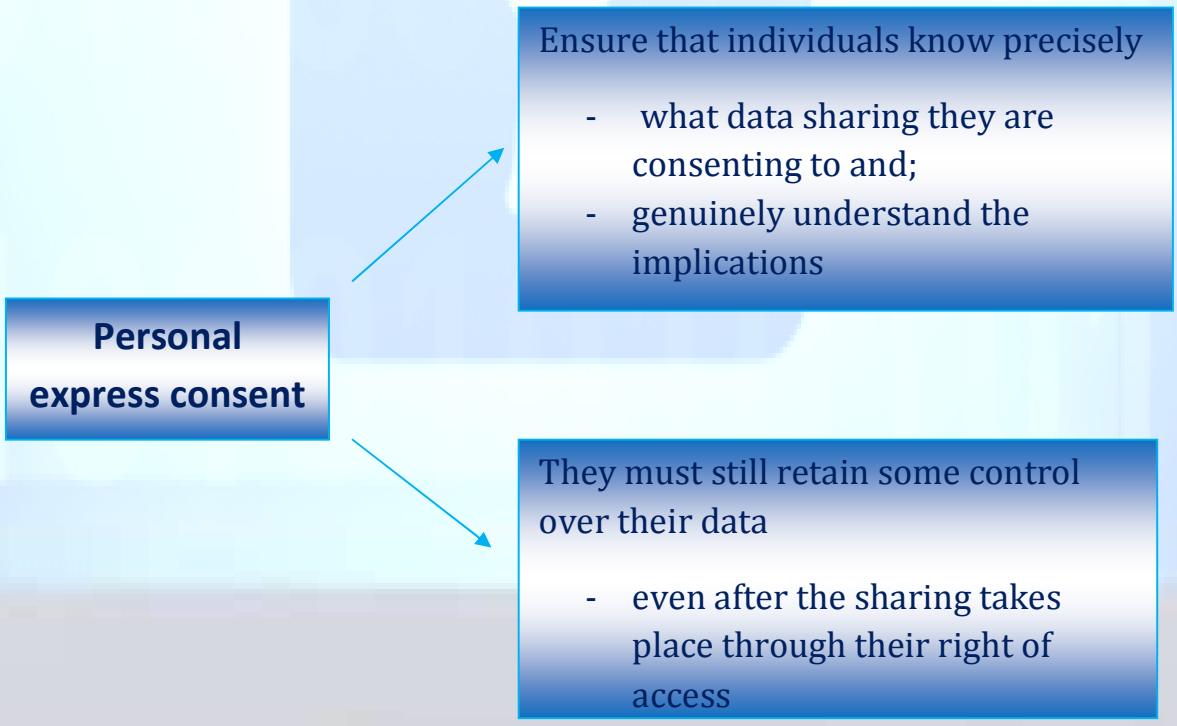


Secondly, 'sensitive personal data' have to handled with care. Such data relates, for e.g., to racial/ ethnic origin, religious beliefs, physical or mental health, sexual life, trade union membership, previous offences or court proceedings. It is necessary to avoid the interests of the individual being prejudiced in any way by the use of shared data. Any justification for data sharing involving such details must be compelling and robust in proportion to those risks.



The importance of personal express consent:-

If you are going to rely on consent as your legal justification for sharing, you must ensure that individuals know precisely what data sharing they are consenting to and genuinely understand the implications. They must still retain some control over their data even after the sharing takes place through their right of access. Please consult the guidance "A Practical Guide for Data Controllers and Processors" (volume 1) developed by this office to understand when the processing of personal data may take place and the guidelines (volume 3) "Data Protection-Your Rights" to understand the right of access to personal data by individuals.



Legal Disclosures under the DPA:-

Section 29 of the DPA further highlights the criminalisation of unlawful disclosures of personal data where any data controller who, without lawful excuse, discloses personal data in any manner that is incompatible with the purposes for which the data was collected, he is committing an offence, liable on conviction to a fine not exceeding Rs 200,000 and to imprisonment not exceeding 5 years.

Section 52 of the DPA also provides an exemption from the listed principles in the section for disclosures of personal data required by law or in connection with legal proceedings. Part VII of the DPA on exemptions further explained in Volume 1 of the guidelines referred to above is also relevant to understand when disclosures may be effected.

Data Sharing Agreements:-

Data Sharing Agreements can be drafted in various flexible ways, depending on the scale and complexity of the data sharing endeavour in question. They represent a set of common rules binding on all the organisations involved in a data sharing initiative. The agreement should be drafted in clear, concise language that is easily understood.

Data Sharing Agreements

- depends on the scale and complexity of the data sharing
- represent a set of common rules binding on all the organisations
- must be drafted in clear, concise language that is easily understood

Protocols typically cover topics such as:-

- the purpose, objectives and scope of the data sharing;
- principles and relevant legislative powers;
- partner undertakings; risk management/ indemnity; and
- DPA compliance (including information security).

Data Sharing Protocols may additionally be developed to strengthen data sharing agreements, clarifying the process and types of information that may be exchanged. Developing a protocol may assist in managing the potential uncertainties about what can be shared, by whom and under what circumstances, and reduce apprehensions about what is legal and what is not.

Protocols typically cover topics such as:-

- the purpose, objectives and scope of the data sharing;
- principles and relevant legislative powers;
- partner undertakings; risk management/ indemnity; and
- DPA compliance (including information security).

A data sharing agreement should, at least, document the following issues:

- 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 to be shared- Could the objective be achieved without sharing the data or by anonymising it?;
- data quality – accuracy, relevance, usability etc;
- data 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; and
- your agreement should also deal with the main practical problems that may arise when sharing personal data. This should ensure that all organisations involved in the sharing:

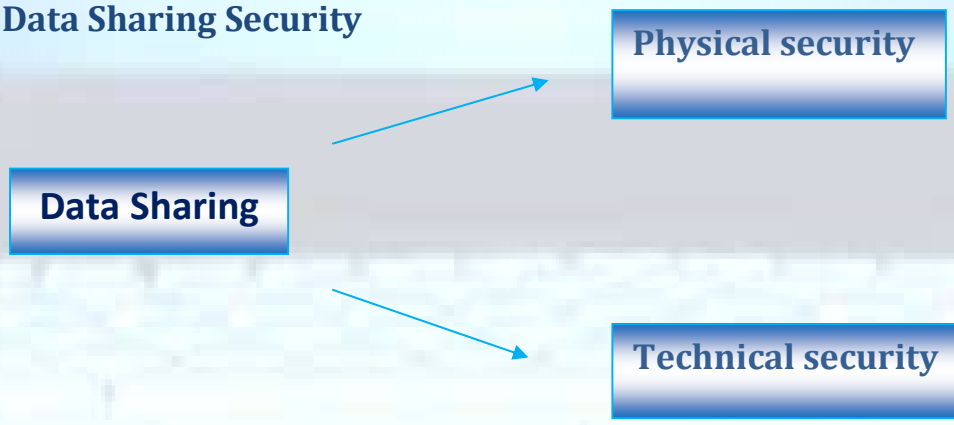
✓ have detailed advice about which datasets may be shared, to prevent irrelevant or excessive information being disclosed;

✓ make sure that the data being shared is accurate, for example by requiring a periodic sampling exercise;

✓ are using compatible datasets and are recording data in the same way.

- The agreement could include examples showing how particular data items – for example dates of birth – should be recorded;
- The agreement must have common rules for the retention and deletion of shared data items and procedures for dealing with cases where different organisations may have different statutory or professional retention or deletion rules;
- The agreement must have common technical and organisational security arrangements, including for the transmission of the data and procedures for dealing with any breach of the agreement;
- The agreement must have a timescale for assessing the ongoing effectiveness of the data sharing initiative and of the agreement that governs it; and

- The agreement must develop systems to facilitate data sharing. Build the need for data sharing into data capture and IT/ database systems design. This will avoid later costs and reduce risks of resistance to data sharing.
- Staff should be aware of security policies and procedures and be trained in their application. In particular you will need to:
    - design and organise your security to fit the type of personal data you disclose or receive and the harm that may result from a security breach;
    - be clear about which staff members in the organisations involved in the sharing are responsible for ensuring information security.
    - They should meet regularly to ensure appropriate security is maintained.
    - Have appropriate monitoring and auditing procedures in place; and
    - be ready to respond to any failure to adhere to a data sharing agreement swiftly and effectively.
- Finally, are you required to update your notification requirements with the DPO?



Physical security

- **Do you have good quality access control systems for your premises?**
- **How are visitors supervised?**
- **Is paper based information stored and transferred securely?**
- **Are laptops and removable media such as discs and memory sticks locked away at night?**
- **Do you dispose of paper waste securely, for example by shredding?**
- **Do you advise staff on how to use their mobile phones securely and minimise the risk of them being stolen?**

Technical security

- **Is your technical security appropriate to the type of system you have, the type of information you hold and what you do with it?**
- **If you have staff that work from home, do you have security measures in place to ensure that this does not compromise security?**
- **How is encryption of personal data implemented and managed?**
- **Have you identified the most common security risks associated with using a web-product – e.g. a website, web application or mobile application?**
- **How do you control access to your systems?**
- **Do you set privileges to information based on people's need to know?**
- **What measures are in place for the security of information in transit?**

Respect the need for privacy of the individual

The use of 'mitigation measures' which compensate partially or wholly for possible negative impacts. Examples include:

- minimising the retention of personal data and adopting 'destruction schedules'
- limiting the use of information to a very specific purpose, with organisational and technical safeguards preventing its broader application
- incorporating a complaints handling system, backed by sanctions and enforcement powers.

When sharing personal data there are some practices that you should avoid. These practices could lead to regulatory action:

- Misleading individuals about whether you intend to share their information. For example, not telling individuals you intend to share their personal data because you think they may object.
- Sharing excessive or irrelevant information about people. For example, routinely sharing details about individuals that are not relevant to the purpose that the information is being shared for.

- Sharing personal data when there is no need to do so – for example where anonymised statistical information can be used to plan service provision.

- Not taking reasonable steps to ensure that information is accurate and up to date before you share it. For example, failing to update address details before sharing information, leading to individuals being pursued at the wrong address or missing out on important information.

- Using incompatible information systems to share personal data, resulting in the loss, corruption or degradation of the data.

- Having inappropriate security measures in place, leading to loss or unauthorised disclosure of personal details. For example, sending personal data between organisations on an unencrypted memory stick which is then lost or faxing sensitive personal data to a general office number.