GRA

GIBRALTAR REGULATORY AUTHORITY

Data Sharing Code of Practice

Gibraltar General Data Protection Regulation & Data Protection Act 2004

30th September 2021

Code of Practice IR01/21 (v2)

FOREWORD

In 2017, the Gibraltar Regulatory Authority, as the Information Commissioner, published its first Data Sharing Code of Practice. The Information Commissioner has decided to update its Code of Practice to reflect developments in the manner data is shared as well as recent changes in Gibraltar's data protection legislation, which now consists of both the Gibraltar General Data Protection Regulation ("Gibraltar GDPR") and the Data Protection Act 2004 ("DPA").

The legislation in Gibraltar maintains the data protection standards that applied in Gibraltar as a result of EU Law i.e. the EU General Data Protection Regulation 2016/679 and the Law Enforcement Directive 2016/680, prior to Brexit and the end of the transition period.

This Code aims to provide organisations with information on how they can share personal data in a fair, safe and transparent manner and guide them through the practical steps they need to take to share personal data while protecting individuals' rights and freedoms.

This Code also aims to dispel many of the misunderstandings regarding data sharing and provide clarity and guidance on how personal data can be shared in compliance with data protection law.

Version History

Date	Version	Comment
18/08/2021	1	Data Sharing Code of Practice issued
30/09/2021	2	Amendments made to the code to reflect the enactment of the Data Sharing (Public Authorities) Act 2021: 1. At page 6, the following text was introduced in relation to express powers: *"For example, specific gateways exist under the Data Sharing (Public Authorities) Act 2021 ("DSA"). Under the DSA there is a framework providing a legal gateway for data sharing for defined purposes between specified public authorities, for the public benefit."* 2. New section titled "DATA SHARING ACROSS THE PUBLIC SECTOR" introduced as section 16. See page 29.

SUMMARY

This Code provides detailed guidance and good practice for the sharing of personal data between organisations. It also provides a general framework which organisations can use to develop their own data sharing arrangements and ensure compliance with the Gibraltar General Data Protection Regulation **(the "Gibraltar GDPR")** and the Data Protection Act 2004 **("DPA").**

Data sharing

- Whilst there is no formal definition within the law, the scope of this Code is defined by section 130 of the DPA as "the disclosure of personal data by transmission, dissemination or otherwise making it available".

- Data sharing can be systematic (i.e. routine data sharing) and/or exceptional (i.e. one-off decisions to share data).

Data sharing and the law

- Organisations should consider the legal implications beyond data protection prior to sharing personal data. Any legal constraints and/or legal powers to share data must be considered to ensure that the data sharing complies with the lawfulness principle under Article 5(1)(a) of the Gibraltar GDPR or section 44 of the DPA.

- Compliance with the lawfulness principle is in addition to identifying a lawful basis for the data sharing.

The data protection principles and the lawful basis

- Sharing personal data must be legitimate under the Gibraltar GDPR and DPA. Organisations must therefore rely on a lawful basis under the Gibraltar GDPR for the sharing of personal data. This does not apply to the processing of personal data by competent authorities under part 3 of the DPA. However, competent authorities will still need to comply with section 44 of the DPA.

- The sharing of personal data must also comply with the data protection principles under Article 5 of the Gibraltar GDPR or sections 43 to 49 of the DPA for data processed under part 3 of the DPA.

Rights of individuals

- The Gibraltar GDPR and DPA provide individuals with certain rights over the processing of their personal data. Organisations must allow individuals to exercise their rights and should have procedures in place for dealing with complaints and queries from individuals in respect of the sharing of their data.

- When data sharing involves solely automated processing, Article 22 of the Gibraltar GDPR and sections 17, 58 and 59 of the DPA should be taken into consideration, and relevant measures should be documented in a data sharing arrangement.

Data Protection Impact Assessment ("DPIA")

- Organisations are obliged to carry out a DPIA for data sharing that is likely to result in a high risk to individuals. However, even where a DPIA is not legally required, it is recommended that a DPIA is carried out as this will allow organisations to demonstrate compliance with data protection law and ensure fairness and transparency, which will promote trust in the proposed data sharing.

Data sharing agreements

- It is good practice to have a written data sharing agreement in place as this will set out the purpose of the data sharing, cover what happens to the data at each stage, set standards and help the organisations involved in the sharing to be clear about their roles and responsibilities. A data sharing agreement can also help organisations meet their obligations under the Gibraltar GDPR and/or DPA and will assist in demonstrating compliance.

- Once a data sharing arrangement is in place it should be reviewed on a regular basis, in particular when there is a change in circumstances or in the rationale for the data sharing.

Law enforcement processing

- Where a competent authority shares personal data with another competent authority for law enforcement purposes, Part 3 of the DPA will apply. However, competent authorities should note that they may also process personal data for general purposes under the Gibraltar GDPR and Part 2 of the DPA rather than for law enforcement purposes. In these cases, data sharing arrangements should distinguish between data processed under the Gibraltar GDPR and Part 2 of the DPA, and data processed under Part 3 of the DPA, with appropriate measures implemented in accordance with the corresponding requirements.

Sharing personal data in databases and lists

- The transfer of databases or lists of individuals from one organisation to another is a form of data sharing.

- An organisation that receives a database or list is responsible for ensuring the integrity of the personal data provided and is responsible for compliance with the Gibraltar GDPR and DPA for the data received, including responding to any complaints or queries from individuals in respect of their data.

Data sharing and children

- Organisations should not share children's personal data unless they have, and can demonstrate, compelling reasons to do so, taking into account the best interests of the child. The best interests of the child should be the primary consideration for organisations who are thinking of sharing children's personal data.

Data sharing in an urgent situation or in an emergency

- Urgent or emergency situations may arise that an organisation may have not envisaged. In these situations, the organisation should only share data where it is necessary and proportionate to do so. The organisation should, where possible, prepare for these situations by planning ahead and training members of staff accordingly.

CONTENTS

1. INTRODUCTION

The Information Commissioner[1] recognises that under the right circumstances and for the right reasons, data sharing between organisations can be beneficial to society and individuals. In every case, the rights of citizens under the Gibraltar General Data Protection Regulation **(the "Gibraltar GDPR")** and the Data Protection Act 2004 **("DPA")** must be respected, and organisations have to comply with their obligations under the Gibraltar GDPR and DPA.

It is important for organisations to understand what can be done legally, and what cannot be done. This will help individuals and organisations from being disadvantaged as a result of excessive caution or carelessness in disclosure. It is important to note that where unjustified disclosures occur, serious harm to individuals and society may be caused. The responsible sharing of information is in the interest of the public in general, as well as in the interest of the individuals and organisations involved.

Individuals expect their information to be handled responsibly in accordance with the law. Amongst other things, this requires individuals to be informed about how their information is being used, including any disclosures.

This Code provides good practice for the sharing of personal data and delivers a general framework, which organisations can use to develop their own data sharing arrangements. Each organisation must adapt it in accordance with their circumstances, taking into account the nature of the data involved and type of data sharing (e.g., frequency (ad hoc or routine), electronic/hard copies, etc).

Adopting the recommendations in this Code will help organisations operate in a compliant manner and avoid the operation of insecure data sharing arrangements that can be detrimental to society and individuals, and generate public distrust.

The Gibraltar GDPR and DPA does not prevent organisations from data sharing. Data protection law is an enabler for fair and proportionate data sharing, rather than a blocker. It provides a framework within which organisations can share data without it being at the expense of an individual's privacy and data protection rights.

Note: There are some differences between the requirements that apply to law enforcement bodies processing personal data under part 3 of the DPA and the requirements that apply to all other organisations under the Gibraltar GDPR. However, many of the requirements in both regimes are similar. Footnotes are used throughout this Code to refer to the relevant provisions in the Gibraltar GDPR and DPA, which readers may find useful to identify the requirements that apply to law enforcement bodies processing personal data under part 3 of the DPA (i.e. where references to the DPA are made) and those that apply to all other entities (i.e. where references to the Gibraltar GDPR are made).

[1] The Information Commissioner is the Chief Executive Officer of the Gibraltar Regulatory Authority.

2. ACKNOWLEDGEMENTS

Where appropriate the Information Commissioner will seek to ensure that locally published codes of practice are consistent with those published by fellow Information Commissioners in other jurisdictions.

As well as reflecting the existing data protection standards and practices in Gibraltar, parts of this document reflect and/or incorporate the recommendations from the United Kingdom's Information Commissioner's Office.

The following document was used in the production of this Code:

(a) Information Commissioner's Office

'Data sharing code of practice' 17th December 2020 – 1.0.53
https://ico.org.uk/media/for-organisations/data-sharing-a-code-of-practice-1-0.pdf

3. USING THIS CODE

This Code is the Information Commissioner's interpretation of the Gibraltar GDPR and DPA's requirements for the sharing of personal data and represents good practice. However, the Code is not mandatory, and organisations may find alternative ways of complying with the law. Where an organisation does not follow the Code and does not have alternative measures in place to meet the Gibraltar GDPR and DPA's requirements, there may be a significant risk of breaching the law.

The Code will largely apply to all data sharing regardless of the sector (e.g. public or private), scale, and context. However, each organisation needs to consider how it may need to adapt its data sharing arrangements to its circumstances.

The Code is complementary to other guidance published by the Information Commissioner about data protection. While the Code stands as the main guide to data sharing, it does not seek to reproduce other guidance, and organisations may need to refer to other guidance on the Information Commissioner's website (e.g. guidance on data protection impact assessments and guidance on exemptions).

The Code is particularly relevant for organisations that carry out routine data sharing, where organisations should establish rules and agree procedures in advance. Where the data sharing is ad hoc or one off, the disclosure is unlikely to be covered by any routine arrangement or agreement. It is still possible to share data in this situation, but organisations should carefully assess the risks every time. The Information Commissioner recommends that organisations make plans to cover such contingencies. Sometimes an organisation may have to make a decision quickly about data sharing in conditions of real urgency or emergency. Organisations should not be put off from data sharing in a scenario like this; in an urgent situation the organisation should assess the risk and do what is necessary and proportionate.

Organisations who intend to share personal data should use this Code to help them –

- identify factors that need to be considered;
- understand when it is appropriate to share data; and,
- implement data protection compliant arrangements for the sharing of data.

In using this Code, organisations may, amongst other things, benefit in the following ways –

- improved understanding of compliant data sharing arrangements;
- improved compliance and mitigation of data protection risks;
- improved protection of individuals and their data;
- greater trust in the organisation by the pubic and customers;
- increased data sharing when it is necessary, to help deliver modern, efficient services;
- enhanced relationships and trust with data sharing partners;
- greater confidence within the organisation about the data sharing's compliance;

- robust and demonstrable compliance with the law; and,
- reduced reputational risk when data breaches occur.

Benefits of data sharing examples:

Public and social sector

An integrated care record is set up to share patient records between health and social care staff. The sharing of personal data between the public and social sectors has allowed for a more complete picture of a patient's health, coordinated and safe care, better decision making for patients' care and reduced inconvenience to patients as they only need to explain their medical situation once.

Nursery

A private nursery obtained information regarding the behaviour of an adult towards a child and found a concerning pattern. The nursery shared the information with authority safeguarding leads to protect the child and others, and to investigate the adult's behaviour.

Health care

Several health professionals from different organisations were involved in providing health and social care to a group of individuals. They exchanged information about recent changes in behaviour from one of the individuals being cared for and identified a pattern of evidence which indicated that the individual could be a victim of abuse. To safeguard the individual, the health professionals shared this information with the individual's social worker for further investigation.

Organisations should use the Code to help review and, where necessary, update data sharing arrangements.

This Code has been prepared and published by the Information Commissioner under section 130 of the DPA. Section 134 of the DPA provides that –

- this Code is admissible in evidence in legal proceedings; and,
- the Information Commissioner may consider this Code in carrying out his functions under the DPA, Gibraltar GDPR and the Communications (Personal Data and Privacy) Regulations 2006. The Information Commissioner will therefore take this Code into account when assessing an organisation's compliance with data protection law for the sharing of personal data, and in the use of his enforcement powers.

If an organisation does not comply with this Code or shares personal data in breach of this Code, it may result in a breach of the Gibraltar GDPR and/or DPA. In the event of a breach, the Information Commissioner may consider taking enforcement action against the organisation, in accordance with the powers granted to him under the DPA. This may involve commencing legal proceedings against the organisation or other use of the Information Commissioner's enforcement powers.

4. WHAT IS MEANT BY "DATA SHARING"?

There is no formal definition of data sharing within the legislation, although the scope of this Code is defined by section 130 of the DPA as "*the disclosure of personal data by transmission, dissemination or otherwise making it available*". This includes for example –

- providing personal data to a third party by any means;
- receiving personal data as a joint participant in a data sharing agreement;
- two-way transmission of personal data; and,
- providing a third party with access to personal data on or through IT systems.

The following examples illustrate a range of data sharing types within the scope of the Code –

- a reciprocal exchange of data;
- one or more organisations providing data to a third party or parties;
- several organisations pooling information and making it available to each other or to a third party or parties;
- routine data sharing on a systematic basis for an established purpose;
- exceptional, one-off or ad-hoc disclosures; and,
- one off data sharing in an urgent or emergency situation.

It is important to distinguish between data sharing that is systematic (i.e. routine data sharing) and exceptional (i.e. one-off decisions to share data).

For the avoidance of doubt, this Code does not deal with the transfer of personal data between a data controller and a data processor, which should be carried out under a written contract as per Article 28 of the Gibraltar GDPR and section 68 of the DPA.

The Code only applies to the sharing of personal data. Neither the Gibraltar GDPR, the DPA, nor this Code, applies to sharing information that does not constitute personal data. Some sharing doesn't involve personal data; for example, if an organisation is sharing information that cannot identify anyone (e.g. anonymised data).

5. DATA SHARING AND THE LAW

Organisations planning to share data need to consider legal implications beyond data protection, before doing so. This could include legislation that forms the basis of the activity that the organisation undertakes, as well as legal constraints from statutory prohibitions on sharing, copyright restrictions or a duty of confidence[2]. Independent legal advice may need to be sought on these issues.

5.1 LAWFULNESS

Any legal constraints and/or legal powers to share data are important factors that must be considered, to ensure that the data sharing is lawful in a general sense in order to comply with the lawfulness principle under Article 5(1)(a) of the Gibraltar GDPR or section 44 of the DPA.

Compliance with the lawfulness principle is in addition to identifying a lawful basis for the data sharing. The lawful basis should not be confused with general lawfulness or legal powers that are beyond the Gibraltar GDPR and the DPA. However, there is a link between lawfulness and the lawful basis - if you do not have a lawful basis to share data, you will be in breach of the lawfulness principle.

5.2 THE PUBLIC SECTOR

Before deciding to share data, a public sector organisation needs to identify and document the legislation that is relevant to them. In this respect it is important to note that –

- government departments headed by a Minister could have common law powers to share information; and,

- other public sector organisations generally derive their powers from statute.

In many cases, public organisations may find that the law that relates to them does not refer to "data sharing". However, the law is likely to define the organisation's functions or purposes. In these cases, public sector organisations will need to identify if the proposed data sharing is within its defined purposes/functions. Generally, "powers to share" exist in one of the following forms –

- Express obligations: this is where an organisation is legally obliged to share data. Where these obligations exist, they usually relate to highly specific circumstances.

- Express powers: this is where organisations have an express power to share data in particular circumstances. For example, specific gateways exist under the Data Sharing (Public Authorities) Act 2021 ("DSA"). Under the DSA there is a framework providing a legal gateway for data sharing for defined purposes between specified public authorities, for the public benefit.

[2] A duty of confidence may arise from a written and transparent statement, or it may be implied by the content of the information or the circumstances in which the information was collected (e.g. medical or banking information)

- Implied powers: where the legislation is silent on the issue of data sharing, it may be possible to rely on an implied power to share information derived from the express provisions of the legislation. Express statutory powers may be taken to authorise an organisation to do things that are reasonably incidental to those which are expressly permitted.

Public authorities are likely to rely on the public task lawful basis in Article 6(3) of the Gibraltar GDPR. This requires the legal power to be laid down by law; however, it does not need to be contained in an explicit piece of legislation, but could be a common law task, function, or power. Public authorities can rely on this power to share data so long as it is sufficiently foreseeable and transparent. Whatever the source of the power to share information, public authorities must check that the power covers the specific disclosure or data sharing arrangement. If it does not, the public authority must not share the information unless, in the particular circumstances, there is an overriding public interest in a disclosure taking place.

5.3 PRIVATE AND SOCIAL SECTOR ORGANISATIONS

Before deciding to share data, private organisations are advised to check their constitutional documents, such as their memorandum and articles of association, to make sure that there are no restrictions to the proposed data sharing. Industry specific regulation or guidance may also need to be considered.

5.4 THE RIGHT TO PRIVACY

It is important to note that individuals in Gibraltar have a right to their personal privacy **(the "Right to Privacy")** under the Gibraltar Constitution 2006[3]. As a constitutional right, any other laws (of a lower authority such as Acts and Regulations) which are in contradiction with the Right to Privacy could be held to be invalid. It must nevertheless be noted that the Right to Privacy is not absolute and that it may be lawfully limited for legitimate aims, as specified in the Constitution. For example, the interests of defence, the prevention of disorder or crime, the economic well-being of Gibraltar, etc.

[3] Section 7, Gibraltar Constitution 2006

6. THE DATA PROTECTION PRINCIPLES AND THE LAWFUL BASIS

For the sharing of personal data to be legitimate under the Gibraltar GDPR and DPA, organisations must rely on a lawful basis under the Gibraltar GDPR (this does not apply to the processing of personal data by competent authorities under part 3 of the DPA. However section 44 of the DPA would need to be complied with). The processing must also comply with the "data protection principles" in Article 5 of the Gibraltar GDPR, or sections 43 to 49 of the DPA for data processed under part 3 of the DPA.

The following emphasises some points in relation to the requirements, which should be given particular attention when data sharing is proposed.

6.1 THE DATA PROTECTION PRINCIPLES

6.1.1 Purpose specification and limitation[4]

The organisations involved in the data sharing should clearly establish why the data sharing initiative is necessary, the specific aims of the sharing and the expected benefits for individuals or for society more widely. This should be documented in precise terms so that all parties are absolutely clear as to the purposes for which data may be shared and shared data may be used.

Furthermore, it should be clearly stated that the data is not to be used further, in a manner incompatible with the stated purpose(s).

6.1.2 Fairness and transparency[5]

Articles 5(1)(a), 12, 13 and 14 of the Gibraltar GDPR and sections 44 and 53 of the DPA include requirements relating to lawfulness, fairness and transparency.

Organisations must treat individuals fairly and not use their data in ways that would have unjustified adverse effects on them. Organisations must also ensure that it is reasonable and proportionate to share personal data, and before sharing data, inform individuals of the purpose of processing in a way that is transparent, accessible, and easy to understand.

The information that must be provided to individuals is normally provided in "privacy notices"[6] at the point of data collection. Amongst other things, the privacy notice should –

- identify the organisation that is collecting the information;
- explain why the information is going to be shared, including when; and,

[4] Article 5(1)(b) of the Gibraltar GDPR and section 43 of the DPA

[5] Articles 5(1)(a), 12, 13 and 14 of the Gibraltar GDPR and sections 44 and 53 of the DPA

[6] See the Gibraltar Regulatory Authority's website for guidance on Privacy Notices

- identify with whom the information is going to be shared.

The privacy notice should be provided at the outset when the person's personal data is collected. If the data has already been collected, then individuals need to be provided with the information above as soon as it is decided that the data is going to be shared or as soon as possible afterwards.

When creating its privacy notice, an organisation should give due consideration to factors such as, the amount of data sharing that it is involved in, the complexity of the data sharing, and nature of data shared. Organisations need to ensure that individuals can find the information they want, that it is clear, and that it is tailored to the circumstances.

It is a matter for data controllers to determine the manner in which they will provide the privacy notice; for example, it can be actively provided by sending out an email (or through other means) or it can simply be made readily available for people to access if they want to. Ultimately, the methods used should be proportionate to the data sharing. The need to actively communicate a privacy notice is particularly important when –

- the organisation shares special categories of personal data, data relating to criminal convictions and offences or data that would constitute "sensitive processing" under Part 3 of the DPA;

- the data sharing is likely to be unexpected or objectionable;

- sharing the data, or not sharing it, will have a significant effect on the individual;

- the sharing is particularly widespread, involving organisations individuals might not expect; and,

- the sharing is being carried out for a range of different purposes.

Providing a privacy notice is primarily the responsibility of the organisation that collects the data initially. However, the organisations involved in the data sharing should work together to ensure that the individuals concerned know who has, or will have, their data and what it is being used for. Each organisation should therefore implement a privacy notice that informs individuals about their data processing (including the data that they collect and receive).

The organisations that are the recipients of personal data, should check the privacy notice of the organisations that are the providers of the data, to ensure that individuals have been appropriately notified that the data will be disclosed to them.

6.1.3 Accuracy[7]

The Gibraltar GDPR and the DPA require organisations to ensure that the data held and shared is accurate and complete and, where necessary, kept up to date.

It is important that before sharing data, organisations take reasonable steps to ensure that the data shared is accurate, which are proportionate to the nature of the data that is to be

[7] Article 5(1)(d) of the Gibraltar GDPR and section 47 of the DPA

shared. Extra care should be taken before sharing sensitive data, in particular where inaccuracies could have detrimental effects on individuals.

Organisations should adopt procedures to periodically check the quality of the data shared.

In addition, organisations should have measures in place to amend and update data after it has been shared. This might be because a data subject notifies of an inaccuracy or otherwise updates their details because of a change in their circumstances.

6.1.4 Data minimisation[8]

Having established a clear objective(s) for the data sharing, the organisations involved should identify the data that needs to be shared and with whom. This should strictly be the minimum necessary to achieve the desired objective.

Organisations should agree and document which datasets need to be shared, to prevent the disclosure of irrelevant or excessive information. The documentation should explain the types of data that will be shared. This may need to be quite detailed, because in some cases it will be appropriate to share certain details held in a file about someone, but not other, more sensitive, material.

In some cases, it may be appropriate to attach 'permissions' to certain data items, so that only certain members of staff, for example ones that have received appropriate training, are allowed to access them.

It is also important to identify precisely when information should be shared, including whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.

It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data. If the objectives of the data sharing can be achieved with anonymised data, this needs to be identified.

6.1.5 Storage limitation[9]

Retention periods for data shared and received by each of the organisations involved in the data sharing should be established.

It could be useful to implement a system whereby once the need to use the data has passed, the information is deleted, and a formal note of the deletion is sent to the organisations involved.

It is important to note that paper records can cause particular problems, as it can sometimes be easy to overlook the presence of old paper records in archives or filing systems – and they may well contain personal data subject to the Gibraltar GDPR and DPA.

[8] Article 5(1)(c) of the Gibraltar GDPR and section 46 of the DPA

[9] Article 5(1)(e) of the Gibraltar GDPR and section 48 of the DPA

Organisations should attempt to have common rules for the retention and deletion of shared data items. Procedures should be implemented to deal with cases where different organisations may have different statutory or professional retention or deletion rules.

If organisations can remove all identifying information from a dataset so that it no longer constitutes personal data, then it can be retained indefinitely.

6.1.6 Security[10]

Organisations are required to have appropriate organisational and security measures in place to protect personal data from being accidentally or deliberately compromised. Whilst organisations may be aware of their own security arrangements to protect personal data, ensuring that the data remains protected when data is shared raises new challenges.

The security measures must be "appropriate" to the nature, scope, context and purpose of the processing and the risks posed to the rights and freedoms of individuals.

Adopting a 'data protection by design and default' approach and undertaking a Data Protection Impact Assessment **("DPIA")** will allow organisations to effectively consider the security measures to put in place in respect of any data sharing initiative.

Amongst the security measures that organisations implement, the Information Commissioner recommends that each organisation implements (and documents) the following measures –

- Identify the personal data that the organisation receives from other organisations, making sure its origin is known and whether any conditions are attached to its use.

- Identify the personal data that the organisation shares with other organisations, who has access to it and what it will be used for.

- Identify and assess whether the organisation shares any data that is particularly sensitive. If so, establish a suitably high level of security to this processing activity.

- Identify who in the organisation has access to information that other organisations have shared with the organisation and ensure that 'need to know' principles are adopted. Avoid giving all staff access to shared information if only a few of them need it to carry out their job. Likewise, identify the specific organisations that have access to the data, including the relevant staff within those organisations that are permitted access (excluding any other persons).

- Identify the effect that a security breach could have on individuals.

- Identify the effect that a security breach could have on the organisation (e.g., costs, reputational damage, loss of trust from customers or clients). This can be particularly acute where an individual provides their data to an organisation, but a third-party recipient organisation then loses the data.

- Identify and distinguish between data that is collected by the organisation directly from data subjects and data that is obtained from another organisation and ensure that staff are aware of this for these to be treated accordingly.

[10] Articles 5(1)(f) and 32 of the Gibraltar GDPR and sections 49 and 75 of the DPA

- Design and organise the organisation's security to fit the type of personal data it discloses or receives and the harm that may result from a security breach.

- Identify the staff members in each of the organisations involved in the data sharing that are responsible for ensuring information security. Periodic meetings should be established to ensure appropriate security is maintained.

- Establish appropriate monitoring and auditing procedures.

- Establish procedures and rules to respond to any failure to adhere to a data sharing agreement swiftly and effectively.

- Staff training and awareness: staff that are likely to make decisions about data sharing or who have access to shared data should be trained on the data sharing arrangements in place, to ensure the proper and responsible use of data.

  The focus of the training should be enabling staff to make informed decisions about whether or how to share data, and how to treat the data they are responsible for. Individuals with overall responsibility for data sharing will need a higher degree of training, than others. For example, they would need to understand –

  - the relevant law surrounding data sharing, including the Gibraltar GDPR and DPA;

  - any relevant professional guidance or ethical rules;

  - data sharing agreements and the need to review them;

  - how different information systems work together;

  - security and authorising access to systems holding shared data;

  - how to conduct data quality checks; and,

  - retention periods for shared data.

- Have common technical and organisational security arrangements, including for the transmission of the data and procedures for dealing with any breach of the agreement.

- Detail the processes that will be used to share the information. This should consider the security of the transmission or accessing of the data; common rules for security should be established.

Every organisation that shares data should ensure that the recipient(s) has appropriate security measures in place to ensure that the personal data continues to be protected. To this end, a set of security standards must be agreed and signed up to by all the parties involved in a data sharing agreement.

Establish clear instructions about the security steps which need to be followed when sharing data by a variety of methods (for example phone, fax, email, or face to face).

6.1.7 Accountability[11]

The accountability requirement means that organisations are responsible for compliance with the Gibraltar GDPR and/or the DPA. Organisations must be able to demonstrate that compliance. The importance of accountability cannot be overstated. To be effective, organisations must embed the message of accountability in the culture and business of the organisation, from board level through to all employees and contractors. This will inevitably involve appropriate training as well as the adoption of a data protection by design and by default approach.

Maintaining relevant documentation to evidence compliance and justify the approach taken is particularly important for accountability. It is important to note the requirements to maintain records of processing activities under Article 30 of the Gibraltar GDPR and section 70 of the DPA, as well as the logging requirements relating to automated processing systems under section 71 of the DPA.

It is also important to note the requirement to implement appropriate data protection policies as well as the requirement to have these reviewed and updated under Article 24 of the Gibraltar GDPR and section 65 of the DPA.

A data sharing agreement is one example of good practice to demonstrate compliance with the abovementioned requirements.

Further to the maintenance of documentation, a Data Protection Officer **("DPO")** plays a key role in accountability and should be involved from the outset in any plans to enter into a data sharing arrangement. The DPO advises on data protection law to ensure compliance, and provides advice in relation to decisions made about data sharing. The DPO may also be the point of contact for individuals to exercise their data protection rights. As good practice, organisations should document the advice received from the DPO.

6.2 THE LAWFUL BASIS[12]

Having established a specific purpose, or purposes, for the data sharing, each organisation involved in the data processing should clearly identify and establish the legal power (see preceding section 5) and legitimising condition(s) that they will rely on for the data sharing.

The lawful bases are different for –

- general processing under the Gibraltar GDPR and Part 2 of the DPA; and,
- law enforcement processing under Part 3 of the DPA.

Organisations must establish the lawful basis that applies to the data sharing and be able to demonstrate that this has been considered and established before the sharing commences.

[11] Article 5(2) of the Gibraltar GDPR and section 43(3) of the DPA

[12] Articles 6, 9 and 10 of the Gibraltar GDPR and section 44 of the DPA

If consent is to be a basis for disclosure, then the organisations could create a model consent form. Organisations would need to address issues surrounding the withholding or retraction of consent.

Further guidance about the lawful basis is available on the Information Commissioner's website.

6.3 THE RIGHTS OF INDIVIDUALS

The Gibraltar GDPR and DPA give individuals certain rights over their personal data. To allow individuals to exercise their rights under the Gibraltar GDPR and DPA, organisations should –

- have policies and procedures in place that allow individuals to exercise their rights easily;
- provide details of how individuals can exercise their rights in the privacy information provided to them;
- make the exercise of individual rights as straightforward as possible; and,
- where several organisations are sharing data, make it clear in the privacy information provided to individuals at the time of collection of their data, who they should contact to exercise their rights.

In a data sharing agreement, it is good practice to provide a single point of contact for individuals to allow them to exercise their rights over the data that is being shared. This avoids individuals having to make multiple requests to several organisations in respect of their rights. However, organisations should note that individuals may choose to exercise their rights against any controller if they wish to do so.

Further, organisations should also have procedures in place for dealing with complaints and queries from individuals in respect of the sharing of their personal data.

Processing involving automated decision-making, including profiling, may result in a high risk to individuals. Where data sharing involves solely automated processing, Article 22 of the Gibraltar GDPR and sections 17, 58 and 59 of the DPA should be taken into consideration and relevant measures documented in the data sharing agreement. In these cases, organisations will need to carry out a DPIA to demonstrate that they have considered the risks and taken measures to mitigate said risks. Where the processing includes profiling, organisations must inform individuals that they have a right to object to the processing[13].

6.4 EXEMPTIONS

Whilst the Gibraltar GDPR and DPA provide a framework of rights and duties that organisations must comply with generally, it includes some exemptions to these obligations to accommodate special circumstances. The exemptions from particular provisions in the Gibraltar GDPR are detailed in Schedules 2 and 3 of the DPA and are separate to the exceptions already built into certain Gibraltar GDPR provisions.

[13] Article 21 of the Gibraltar GDPR

However, it is important to note that the exemptions can be relied on to the extent that compliance with the law would likely prejudice the purpose of the processing. For example, the police might ask an organisation to give them information about an ex-employee who they suspect of being involved in a serious assault. If informing the ex-employee that they have given the police this information would tip the individual off and be likely to prejudice the investigation, because the suspect might abscond for example, then the organisation could rely on an exemption so that it does not need to comply with the "fairness and transparency" principle.

Where an organisation decides to apply an exemption, it should document the reasons for the decision. The organisation must be able to justify any decision to apply an exemption to the Information Commissioner or the courts.

Generally, the Information Commissioner's view is that exemptions could be relied on in ad hoc cases, but it will be very difficult for exemptions to be justified in the case of ongoing or systematic data sharing.

Further guidance on exemptions is available on the Information Commissioner's website.

7. DATA PROTECTION IMPACT ASSESSMENTS

The Information Commissioner recommends that organisations carry out a DPIA, even if they are not legally required to do one, as this will allow organisations to demonstrate compliance with data protection and ensure fairness and transparency, which will promote trust in the proposed data sharing. Further, a DPIA will allow organisations to assess the risks involved in the proposed data sharing and determine what safeguards should be implemented.

Organisations should note that under Article 35 of the Gibraltar GDPR or section 73 of the DPA they are obliged to carry out a DPIA for data sharing that is **likely to result in a high risk to individuals**. However, if an organisation is confident that the type of data sharing proposed is unlikely to result in high risk, it will not be legally required to carry out a DPIA.

Guidance about DPIAs including tools to help identify when a DPIA is required is available on the Information Commissioner's website. It is worth noting that the Information Commissioner's guidance identifies "datasets that have been matched or combined" as processing that increases the risk of the processing. Data sharing is thereby considered likely to increase data protection and privacy risks.

8. DATA SHARING AGREEMENTS

Organisations are responsible for ensuring compliance with the Gibraltar GDPR and DPA and should ensure that they have measures in place to control the data sharing. It is good practice to have a written data sharing agreement.

Data sharing agreements set out the purpose of the data sharing, cover what happens to the data at each stage, set standards and help all the parties involved in the sharing to be clear about their roles and responsibilities. Having a data sharing agreement in place helps organisations meet their obligations under the Gibraltar GDPR and/or DPA and will be particularly useful to demonstrate accountability.

Drafting and adhering to a data sharing agreement does not provide immunity from breaching the law or from the consequences of doing so. However, the Information Commissioner will take into account the existence of any relevant data sharing agreement should an investigation or assessment take place. A data sharing agreement may therefore mitigate the risk of enforcement action where a breach occurs.

Government departments and certain other public bodies (for example, regulators, law enforcement bodies and executive agencies) may enter into 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.

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 binding on all the organisations involved in a data sharing initiative, the agreement should be drafted in clear, concise language that is easy to understand.

An agreement will help justify the data sharing and demonstrate that the organisations involved have been mindful of, and have documented, the relevant compliance issues. In order to adopt good practice and to comply with the Gibraltar GDPR and DPA, the Information Commissioner would expect a data sharing agreement to address and document the following –

- The organisations involved. The agreement should clearly identify all the organisations that will be involved in the data sharing and should include contact details for their key members of staff. It should also contain procedures for including additional organisations in the data sharing arrangement and for dealing with cases where an organisation needs to be excluded from the sharing.

- The data. The agreement should set out the types of personal data that are going to be shared. This may need to be detailed, because in some cases it will be appropriate to share only certain information held in a file about an individual, omitting other more sensitive material. In some cases, it may be appropriate to attach 'permissions' to certain data items, so that only particular members of staff or staff in specific roles are allowed to access them (for example, staff who have received appropriate training).

- Key executives. The nominated "data sharing executive" for each organisation alongside the contact details of the DPO.

- Lawful basis and principles. Each organisation's position and measures adopted to comply with the data protection aspects identified earlier in subsections 6.1 and 6.2.

- Individuals' rights. Procedures to ensure compliance with the rights of individuals under data protection law such as ensuring compliance with access requests. For example, the agreement should explain what to do when an organisation receives a request for access to shared data or other information. In particular, given data subjects can contact any controller involved in the sharing, it should make clear that one staff member (generally a DPO in the case of personal data) or organisation takes overall responsibility for ensuring that the individual can easily gain access to all their personal data that has been shared.

- Review/termination. The procedures to review the effectiveness/termination of the sharing agreement, as well as provisions relating to the addition of new organisations to the data sharing arrangement.

- Sanctions. Sanctions for failure to comply with the agreement or breaches by individual staff.

- Interoperability. Interoperability measures to ensure that organisations are using compatible datasets and are recording data in the same way.

The following are practical issues that should also be addressed by the data sharing agreement –

- Have detailed advice in respect of which data they can share to prevent irrelevant or excessive information being disclosed;

- Make sure the shared data is accurate and up to date;

- Record data in the same format, abiding by open standards when applicable;

- Have common rules for the retention and deletion of shared data;

- Have common technical and organisational security arrangements, including the transmission of data and procedures for dealing with data breaches;

- Ensure members of staff are properly trained and fully aware of their responsibilities for any shared data they have access to;

- Have procedures for dealing with data subjects' rights, complaints or queries from members of the public;

- Have a timescale for assessing the effectiveness of the data sharing initiative and compliance with the data sharing agreement; and,

- Have procedures for dealing with the termination of the data sharing initiative, including the deletion or return of the shared data.

9. DATA SHARING EXECUTIVES

Each organisation involved in a data sharing arrangement should appoint a senior, experienced individual to have overall responsibility for information governance, ensuring compliance with the law, and advising staff on making decisions relating to data sharing. The data sharing executive should have appropriate seniority and influence to make authoritative decisions about data sharing.

10. PERIODIC REVIEWS

Once a data sharing arrangement is in place it should be reviewed on a regular basis, in particular when a change in circumstances or in the rationale for the data sharing arises. When a changes occurs, it should be reflected in the arrangement to ensure that such sharing can still be justified. If it cannot be justified, it should stop. The following should be considered as part of the review –

- Is the data sharing still meeting the stated objectives?
- Do the safeguards in place still match the data protection and privacy risks?
- Is the data still needed? The data may not be needed because it is simply no longer necessary or because the data sharing is making no impact upon the stated aim and therefore the sharing is no longer justified.
- Does the privacy notice and any data sharing agreements in place still accurately explain the data sharing being carried out?
- Are the information governance procedures still adequate and working in practice? All the organisations involved in the data sharing should check -
    - whether it is necessary to share personal data at all, or whether anonymised information could be used instead;
    - that only the minimum amount of data is being shared and that the minimum number of organisations, and their staff members, have access to it;
    - that the data shared is still of appropriate quality;
    - that retention periods are still being applied correctly by all the organisations involved in the sharing;
    - that all the organisations involved in the sharing have attained and are maintaining an appropriate level of security;
    - that staff are properly trained and are aware of their responsibilities in respect of any shared data they have access to;
    - that the information being shared is accurate (carry out periodic sampling); and,
    - that there is ongoing interoperability.

If significant changes are going to be made to the data sharing arrangements, then those changes need to be publicised appropriately. This can be done by updating websites, sending emails directly to individuals or, if appropriate, placing advertisements in local newspapers.

The periodic reviews should be documented and should identify the individuals involved.

11. INTEROPERABILITY

Organisations may use different hardware, software, or other arrangements to store and process data (for example, organisations may record an individual's date of birth differently). It is important to ensure that data sharing occurs in a format(s) that is usable and appropriate to all and that safeguards are in place to protect against any issues that may arise from the use of different formats, such as the mismatch or corruption of records. Organisations should not misjudge the importance of this as it could affect the ability to perform the intended purpose of the data sharing and have detrimental effects on individuals.

12. LAW ENFORCEMENT PROCESSING

The Information Commissioner acknowledges that there may be compelling reasons for a competent authority[14] to share data for law enforcement purposes[15] (for example, to protect the public, support ongoing policing activities or in an emergency situation).

Other than data processing for law enforcement purposes, competent authorities should note that they are also likely to process personal data for general purposes under the Gibraltar GDPR and Part 2 of the DPA (for example, for human resources matters). Where applicable, data sharing arrangements should distinguish between data processed under the Gibraltar GDPR and Part 2 of the DPA, and data processed under Part 3 of the DPA, with appropriate measures implemented in accordance with the corresponding requirements.

- **Data sharing - Part 3 to Part 3 of the DPA:** If a competent authority shares personal data with another competent authority for law enforcement purposes, Part 3 of the DPA will apply.

- **Data sharing - Part 3 to Part 2 of the DPA:** In some cases, a competent authority may share data (that it is processing for law enforcement purposes) to a recipient where the disclosure is not for law enforcement purposes or where the recipient is not a competent authority. In practice, Part 3 of the DPA allows for the sharing of data with a third party or for data to be repurposed internally, and then be used for general processing purposes under the Gibraltar GDPR and Part 2 of the DPA. However, a competent authority must determine whether the processing of such data for non-law enforcement purposes is "*authorised by law*"[16]. The question of "*authorised by law*" will, in part, depend on the specific laws to which the relevant competent authority is subject. Competent authorities should start by identifying the reason and lawful basis for the sharing.

Example

The police may provide information to the civil courts about child protection proceedings. Both the police and the court are competent authorities, but since the court proceedings are civil rather than criminal, the disclosure by the police is not in the context of law enforcement purposes. This is the case even though the reason for the police disclosing the information is to protect life, which is a policing purpose.

- **Data sharing – Part 2 to Part 3 of the DPA:** If an organisation is not a competent authority, it may share data for law enforcement purposes with a competent authority in

[14] For the definition of 'competent authority' under Part III of the DPA, see section 39(1) and schedule 7 of the DPA.

[15] Part III, section 40 of the DPA defines 'law enforcement purposes' as the "*purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*".

[16] Part III, section 45(2)(a) of the DPA.

compliance with the Gibraltar GDPR and Part 2 of the DPA. However, the organisation must still have a lawful basis for the sharing of data.

Requests for information received by an organisation from a competent authority must be reasonable in the context of their law enforcement purpose and should clearly explain the necessity for the request. Where necessary in the circumstances, an organisation may also rely on the 'crime and taxation' exemption under schedule 2 of the DPA. This includes exemption from transparency obligations, and most individuals' rights, to the extent that the application of said provisions is likely to prejudice the prevention or detection of crime.

If an organisation is not a competent authority and is disclosing information about an individual's criminal offences and convictions (including allegations that the individual has committed an offence), the organisation must comply with Article 10 of the Gibraltar GDPR. Further, the organisation must meet a relevant condition in schedule 1 of the DPA. In this scenario, the most likely condition is in section 10 of schedule 1 of the DPA (i.e. disclosures which are necessary for the purposes of the prevention or detection of unlawful acts, and where asking for an individual's consent would prejudice those purposes).

Personal data of witnesses, victims, bystanders, and other individuals who are not the offender or alleged offender is not considered 'criminal offence' data and a schedule 1 condition is not required for the processing and sharing of said data. However, if the data being shared includes special category data, a condition under Article 9 of the Gibraltar GDPR needs to apply, together with a condition in schedule 1 of the DPA.

Part 2 of Schedule 1 of the DPA requires organisations to have an appropriate policy document to cover their data processing under said part. However, an organisation disclosing data to a competent authority in reliance on the condition in section 10, part 2 of schedule 1 of the DPA does not need to have a policy document to cover that disclosure.

- **Rights of individuals - Part 3 of the DPA:** There are differences in the availability of individual rights for law enforcement processing. For example, some individual rights under the Gibraltar GDPR, such as the right to object and the right to data portability, do not exist under Part 3 of the DPA. Further, there are exemptions and restrictions that can, in certain circumstances, be legitimately applied to prevent individuals from exercising their rights if there is a likely prejudice to the law enforcement purposes.

- **Accountability – Part 3 of the DPA:** Section 43(3) of the DPA states that the controller is responsible for and must be able to demonstrate compliance with the provisions under Part 3 of the DPA. The controller must also put in place appropriate technical and organisational measures that ensure and demonstrate compliance. This may include, policies and procedures, including 'data protection by design and default'. Further, the controller must also maintain relevant documentation of data processing activities[17].

[17] See section 70 of the DPA.

13. SHARING PERSONAL DATA IN DATABASES AND LISTS

The transfer of databases or lists of individuals is a form of data sharing, whether for money or other consideration, and whether for profit or not. Examples of organisations involved in this type of data sharing may include the following:

- Data brokers;
- Credit reference agencies;
- Marketing agencies;
- Franchised businesses;
- Clubs and societies;
- Charities and voluntary groups; and,
- Political parties.

An organisation that receives a database or list is responsible for ensuring the integrity of the data provided. The organisation is also responsible for compliance with data protection law for the data received as well as responding to any complaints received from individuals in respect of the data. The organisation should make appropriate enquiries and checks, including the following:

- confirm the source of the data;
- identify the lawful basis relied on when the data was obtained and that any conditions about that lawful basis were complied with;
- check what information was provided to individuals at the time of handing over their data;
- verify how and when the data was initially collected;
- check for records of consent if consent is the lawful basis relied on;
- review the privacy information provided to individuals at the time their data was collected, and thereafter;
- check that the data is accurate and up to date; and,
- ensure that the data received is not excessive or irrelevant to the purpose of processing.

It is good practice for the organisation receiving the data to have a written contract in place with the organisation providing the data. In terms of transparency, the organisations involved in the data sharing must inform individuals that their data is being shared and for what purposes[18]. There are exceptions to these requirements, for example, where the information has already been provided to individuals. However, it is the organisation's responsibility on receiving the data to be satisfied that this has been done.

[18] Articles 13 and 14 of the Gibraltar GDPR. For processing under Part III of the DPA, see section 53(1) and 53(2) of the DPA

14. DATA SHARING AND CHILDREN

If you are considering sharing children's personal data, you must take extra care. Organisations should not disclose children's personal data unless they have, and can demonstrate, compelling reasons to do so, taking into account the best interests of the child. An example of a compelling reason is data sharing for safeguarding purposes or for official national statistics of good quality information about children. However, selling children's personal data for commercial reasons is unlikely to amount to a compelling reason for data sharing.

The best interests of the child should be the primary consideration. This concept comes from the United Nations Convention on the Rights of the Child, which declares that "*In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.*" In essence, the best interests of the child are whatever is best for that individual child.

The following should be considered when data sharing involves children's personal data:

- Do not share personal data unless there is a compelling reason to do so.
- Carry out a DPIA, to assess and mitigate the risks to the rights and freedoms of children, which arise from data sharing.
- Balance the best interests of the child against the rights of others. For example, it is unlikely that the commercial interests of an organisation will outweigh a child's right to privacy. Considering the best interests of the child should form part of an organisation's compliance with the lawfulness, fairness, and transparency requirements.
- Provide privacy information that is clear and presented in plain, age-appropriate language.
- Carry out due diligence checks on the organisations with whom data will be shared.
- Ensure that any default settings relating to data sharing specify the purpose of the sharing and who the data will be shared with.
- Consent is not the only lawful basis to use. Other lawful bases might be more appropriate. If an organisation relies on consent for data sharing, it must consider the competence of the child to give their own consent, and whether that consent is freely given (for example, whether there is an imbalance of power). Further, where the sharing is necessary for the performance of a contract, the organisation should consider the child's competence to enter into a contract.

Where the organisation is a provider of an online service, it must comply with the requirements at Article 8 of the Gibraltar GDPR.

15. DATA SHARING IN AN URGENT SITUATION OR IN AN EMERGENCY

Urgent or emergency situations may arise that an organisation may have not envisaged. In these situations, an organisation should only share data where it is necessary and proportionate to do so. Examples of emergency situations include:

- preventing serious physical harm to an individual;
- preventing loss of life;
- protection of public health;
- safeguarding vulnerable adults or children;
- responding to an emergency; or,
- an immediate need to protect national security.

In an urgent or emergency situation, an organisation will have to take decisions rapidly. The organisation should, where possible, prepare for these situations by planning ahead and training members of staff accordingly. This will allow the organisation to establish the data it holds, the data it may need to share and prevent any delays when sharing data in an urgent or emergency situation. As part of compliance with the accountability principle, the organisation should document the action taken in respect of any shared data, in response to an urgent or emergency situation.

16. DATA SHARING ACROSS THE PUBLIC SECTOR

Her Majesty's Government of Gibraltar has introduced a framework for sharing personal data for defined purposes across specific parts of the public sector, under the DSA. The aim of the DSA is to ensure clarity and consistency in how the public sector shares personal data and to improve public services through the better use of data whilst ensuring data protection and privacy.

The DSA provides gateways to allow specific public authorities to share data with each other. Some of these gateways enable the sharing of personal data, whilst others allow the sharing of non-identifying data. The objectives and purposes for data sharing under the DSA's powers are tightly defined.

The powers to share information under the DSA must be consistent with this Code, and other codes of practice issued by the Information Commissioner under section 135 of the DPA, so far as they apply to the personal data being shared.

17. THINGS TO AVOID

Organisations should NOT do the following –

- Mislead individuals about whether there is an intention to share their information. For example, not telling individuals about an intention to share their personal data because it is thought that they may object.

- Share excessive or irrelevant information about individuals. For example, routinely share details about individuals that are not relevant to the purpose that the information is being shared for.

- Share personal data when there is no need to do so. For example, where anonymised statistical information can be used to plan service provision.

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

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

- Have 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, faxing sensitive personal data to a general office number, sending unencrypted sensitive personal data via email, or having ineffectual access controls.

ANNEX A: DATA SHARING CHECKLIST

The following checklist is a step-by-step guide for organisations to use when deciding whether to share personal data. It highlights what an organisation should consider to ensure that data sharing is compliant with data protection law, and that it meets individuals' expectations.

This checklist should be used in conjunction with this Code and other guidance issued by the Information Commissioner.

Is the sharing of data justified?

Organisations should consider the following -

- □ What is the purpose of sharing data?
- □ What are the potential benefits and risks to individuals and/or society of sharing or not sharing data?
- □ Is it fair to share individuals data?
- □ Is it necessary and proportionate to share individuals data?
- □ What is the minimum data that needs to be shared to achieve the purpose?
- □ Can the purpose be achieved without sharing data or by sharing less data?
- □ What safeguards can be put in place to minimise the risks or potential adverse effects of the sharing?
- □ Is there an applicable exemption in the DPA?

Is a DPIA needed?

Organisations should consider whether they need to carry out a DPIA -

- □ Is the sharing of data likely to result in a high risk to individuals?
- □ What are the risks of sharing data? Can safeguards be put in place to mitigate those risks?

What should be considered prior to sharing data?

As good practice, organisations should implement a data sharing agreement which should cover the following -

- □ What data will be shared?
- □ Does the sharing involve special category data? If so, what additional safeguards will be put in place?
- □ How will the data be shared?
- □ What security measures will be put in place? Are these appropriate to the data being shared?
- □ What is to happen to the data at every stage?
- □ Who will have access to the data? What access controls will be put in place?
- □ What organisations are involved in the sharing of data? Are these clear on their roles and responsibilities?
- □ What privacy information will be provided to individuals? Is the information concise, transparent, easily accessible and uses clear and plain language?
- □ Is data obtained from other sources other than the individual?
- □ What arrangements will be put in place to comply with individuals' data protection rights?
- □ What measures will be put in place to ensure that the shared data is accurate and up to date?

- □ What technical and organisational measures will put in place for the sharing of data? Are these appropriate to the data being shared?
- □ Are there common retention periods for the shared data? Are there procedures for the secure deletion of data?
- □ Are there procedures for the regular review of the data sharing agreement?

What about the accountability principle?

Organisations should consider the following -

- □ What are the roles and responsibilities of the organisations involved in the data sharing? Can they demonstrate compliance with the Gibraltar GDPR and DPA?
- □ What documentation will be maintained for the data sharing operations?
- □ Has a 'data protection by design and default' approach being taken?
- □ Do the technical and organisational measures in place implement data protection principles and safeguard individuals' rights?
- □ Have members of staff, who have responsibilities and make decisions about the shared data, received training that is appropriate to the data being shared?

What is the lawful basis for the sharing of data?

To determine the lawful basis, organisations should consider the following -

- □ What is the nature, scope and context of the data and the purpose for sharing it?
- □ Is any of the data either special category data or criminal convictions data? If so, what additional conditions need to be met?
- □ Where legitimate interests are the lawful basis for the sharing of data, has a legitimate interests assessment being carried out?

Are there any powers to share data?

Whilst the position will be different for organisations in the public and private sectors, organisations should consider the following -

- □ What type of organisation it is and are there any relevant functions or powers for data sharing?
- □ What is the nature of the data that is to be shared?
- □ Are there any legal requirements that need to be met when sharing data (for example, copyright or a duty of confidence, or any prohibitions)?
- □ Is there a legal obligation or other legal requirement about sharing data (for example, a statutory requirement, a court order or common law)?

What should be documented when deciding to share data?

Organisations should document their decision and reasoning, whether they decide to share or not share data. If an organisation decides to share data, they should document the following -

- □ The justification for sharing;
- □ The data that was shared and the purpose;
- □ The organisation(s) with whom the data was shared;
- □ When and how the data was shared;
- □ If data was shared based on consent, a record of how consent was obtained;

- The lawful basis for processing and any additional conditions applicable for the sharing of data;
- Individuals' rights;
- DPIA reports (where applicable);
- Compliance with any advice provided by the DPO (where applicable);
- Evidence of the steps taken to comply with the Gibraltar GDPR and DPA; and
- When and how the organisation reviewed and updated the accountability measures at appropriate intervals.

IMPORTANT NOTE

All organisations that process personal data need to be aware that the Gibraltar GDPR and the DPA will apply directly to them. The responsibility to become familiar with the Gibraltar GDPR and the DPA and comply with its provisions lies with the organisation.

Where necessary, the Information Commissioner will review this Code in accordance with any updates or other developments. In the event of any conflict or inconsistencies between this Code and the Gibraltar GDPR and the DPA, the Gibraltar GDPR and the DPA will take precedence.

CONTACT US

Gibraltar Regulatory Authority
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar

(+350) 20074636
privacy@gra.gi
www.gra.gi