|  |
| --- |
| **[DIFC SAMPLE TEMPLATE]** |

**[ENTITY NAME]**

**GOVERNMENT**

**DATA SHARING policy**

**Regarding this template:** Due to DIFC’s historical reliance on UK and EU data protection and privacy principles and the interpretation thereof by the UK authorities, from a common law perspective, this guidance template should be read in conjunction with any existing UK and EU laws and guidance or templates on the same topic, with which the DP Law is also aligned.

***This document expresses no opinion on lawfulness of specific business activities, does not have the force of law, and is not intended to constitute legal advice****. Please contact legal counsel for assistance in determining your data protection and privacy policies in respect of the issues under discussion to ensure compliance with the applicable laws and regulations. The Commissioner does not make any warranty or assume any legal liability for the accuracy or completeness of the information herein as it may apply to the particular circumstances of an individual or a firm.*

**Please note**: Notes to user are in BLUE and COMPANY related requirements for completion are highlighted in YELLOW. Links to guidance, policy templates, and the DIFC DP Law are also provided.

Please remove this page in your company’s final version.

**Contents**

[1 Policy statement 4](#_Toc113442977)

[2 Compliance and Administration 5](#_Toc113442978)

[3 General Definitions 6](#_Toc113442979)

[4 Data protection principles - general 7](#_Toc113442980)

[5 Disclosure / sharing of Personal Data with Government Entities 13](#_Toc113442981)

[6 Making and Dealing with Personal Data sharing requests and prevailing laws 13](#_Toc113442982)

[7 Rights of Redress 17](#_Toc113442983)

[8 Data Sharing Process Considerations 18](#_Toc113442984)

[9 Governance, Review and Monitoring 20](#_Toc113442985)

[10 Confidential Commercial Information 20](#_Toc113442986)

[11 Questions about this Policy 21](#_Toc113442987)

[Appendix A – Data Sharing Checklist 22](#_Toc113442988)

# Policy statement

## [Entity Name] [and/or its subsidiaries and affiliates, including [*Insert names of Subsidiaries/Affiliates, if applicable*] ([collectively] “[Company]”[[1]](#footnote-2), “we” or “us”) [is]/[are] committed to safeguarding the privacy of the Personal Data that we gather.

## This Government and Public Authority Data Sharing Policy applies to Personal Data and to the ethical, legal management of that Personal Data in any form – whether oral, electronic or written – when shared, whether by statute or voluntarily with another entity endowed with legislative and / or judicial powers or that of an authority empowered to provide public security, utilities and social services (“Government Entity” or “Government Entities”), including but not limited to entities such as the Dubai International Financial Centre Authority (“DIFCA”), the Dubai Financial Services Authority (“DFSA”), Dubai Government, the Government of the UAE, other free zone authorities or international public authorities, as well as law enforcement and public utilities service providers. This policy shall be read in conjunction with relevant DIFC or other authority’s guidance on this topic.

## This policy gives effect to [Company]’s commitment to protect any Personal Data, including that of its employees and third parties, and has been adopted by [Entity Name] [, as well as all its subsidiaries, affiliates and related entities]. “Personal Data”, further defined below, for the purposes of this policy includes individuals’ names, dates of birth and other personal information from which they can be identified.

## This policy and any other documents referred to in it sets out the lawful basis on which we will process Personal Data we collect from any Data Subjects, or that is provided to us by Data Subjects or other sources, and the purposes for which it is collected. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store Personal Data.

## The main criterion for sharing information with specified recipients in line with this policy is that the sharing of information is consistent with and aligned to the purposes set out in primary relevant legislation as well as to the data protection principles. It is key to place the same importance on the benefits that citizens can derive from better and timelier government and public services as a result of legal, ethical information sharing as it is on protecting the privacy of citizens’ data. This policy supports the approach of factoring in ethical considerations around the use of data to achieve the objective of any data sharing request and looking to provide the minimum amount of Personal Data possible.

## This policy may be amended at any time.

# Compliance and Administration

## Our clients and employees have rights with regard to the way in which their Personal Data is collected, stored and processed. We recognise that the fair and lawful treatment of this data will maintain confidence in [Company] and will support successful operations.

## All [Company] employees and its contractors must comply with this policy when processing Personal Data on [Company]’s behalf, including when requested to share data with a Government Entity. Any breach of this policy may result in disciplinary action.

## The Personal Data, which we hold in relation to our clients, employees, suppliers and other third parties is subject to certain legal safeguards specified in the Data Protection Law, DIFC Law No. 5 of 2020 (as amended) (the “DP Law 2020”) or as per applicable data protection laws and regulations, (“Applicable Laws”, and together with the DP Law 2020, the “Data Protection Laws”. Specifically, this policy sets out the detailed guidance for compliance with Article 28 of the DP Law 2020.

## The [[Company]’s Data Protection Officer (“DPO”]/[*Insert [Company] officers responsible for data protection compliance (the “Compliance Officer”*] [is]/[are] responsible for ensuring compliance with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the [DPO]/[Compliance Officer], who can be reached at [*Insert email address or contact information.]*

# General Definitions

## Data is information which is processed i) by means of equipment operating automatically in response to instructions given for that purpose, or ii) on paper or as part of a paper-based filing systems intended for processing electronically.

## Data Subjects include all living individuals about whom we hold Personal Data. All Data Subjects have legal rights in relation to their Personal Data.

## Controllers are the people who or organisations which determine the purposes for which, and the manner in which, any Personal Data is processed. They are responsible for establishing practices and policies in line with the Data Protection Laws. We are the Controller of all Personal Data used [in our business for our own commercial purposes].[[2]](#footnote-3)[[3]](#footnote-4)

## Processors include any person or organisation that is not a data user that processes Personal Data on our behalf and on our instructions. Employees of Controllers are excluded from this definition but it could include suppliers that handle Personal Data on [Company]’s behalf.

## Data Protection Principles are those principles on which data protection laws and policies are founded, as set out in Section 4 of this policy.

## Personal Data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal Data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

## Processing is any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Processing also includes transferring Personal Data to third parties.

## Public Authority is defined in Presidential Directive 4 of 2022 as any recognised Government Entity, including government bodies, authorities, law enforcement agencies or other similar regulatory authority established in a country or jurisdiction, including Third Countries, that administers policies, laws and regulations of the country or jurisdiction.

## Special Category Data is information revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life. It may only be processed under strict conditions, including requiring the explicit consent of the person concerned.

# Data protection principles - general

## The [Company] may in the ordinary course of business collect and process information about anyone who:

* + 1. is employed by us, including contractors and temporary employees;
    2. uses our websites [mobile applications, call-centre];
    3. attends our business development, marketing or other [Company] sponsored events;
    4. contacts us for information about products and services;
    5. interacts and communicates with us in a business capacity;
    6. provides or handles information relating to suppliers and other third parties;
    7. [ ]; and
    8. [ ].

## Such information may include, but is not limited to:

* + 1. Name, gender, home address, and telephone number, date of birth, marital status, emergency contacts;
    2. Residency and visa status, nationality and passport information;
    3. Emirates ID number, banking details;
    4. Information required to comply with laws, the requests and directions of law enforcement authorities or court orders (i.e. debt payment information);
    5. Information captured on security systems, including CCTV and key card entry systems;
    6. Voicemails, emails, correspondence and other work product and communications created, stored and transmitted by an employee using [Company]’s computer or communications equipment;
    7. Employee information;
    8. [ ]; and
    9. [ ].

## Anyone processing such information, including Government Entities, must adhere to the following principles of lawfulness, transparency and accountability, as per Article 9 of DP Law 2020:

### Personal Data must be processed lawfully, fairly, and in a transparent manner in relation to the Data Subject.

### Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

### Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

### Personal Data must be accurate and, where necessary, kept up to date.

### Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed.

### Personal Data must be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

### The Controller shall be responsible for and be able to demonstrate compliance with these principles.

## Fair processing

### The Data Protection Laws are not intended to prevent the processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject.

### For Personal Data to be processed lawfully by us, they must be processed on the basis of one of the legal grounds set out in the Data Protection Laws. These include, among other things, the Data Subject's consent to the processing, or that the processing is necessary for the performance of a contract with the Data Subject, for the compliance with a legal obligation to which the Controller is subject, or for the legitimate interest of the Controller or the party to whom the data is disclosed. When sensitive Personal Data is being processed, additional conditions must be met.

### When processing Personal Data as Controllers in the course of our business, [Company] and its employees will ensure that those requirements are met.

### In the absence of any other applicable basis for fair and lawful processing of Personal Data, [Company] processes Personal Data on the basis that the processing is necessary for the purposes of pursuing [Company]’s legitimate interests or those pursued by a third party or parties to whom the Personal Data is disclosed, except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject's particular situation.

## Processing for limited purposes

### We may for various reasons collect and process Personal Data. This may include data we receive directly from a Data Subject and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

### We will only process Personal Data for specific purposes or for any other purposes specifically permitted by the Data Protection Laws. We will notify those purposes to the Data Subject through any applicable means, such as an online privacy notice.

## Adequate, relevant and non-excessive processing

### We will only collect Personal Data to the extent that it is required for the specific purpose notified to the Data Subject.

## Accurate, Complete and Up-to-Date data

### We will ensure that Personal Data we hold is accurate and kept up to date. We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

## Timely processing

### We will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required or which a Data Subject has asked that we destroy or modify.

### We will conduct timely reviews of our processing operations with respect to data that is collected and stored in our systems. Such reviews will include but are not limited to understanding where our data is processed, who our sub-processors are (if any) and any recipients of our data and the purposes for which they are processing it, if such information may legally be made available to us.

### We will to the extent required by law comply with any statutory retention periods.

## Data security

### We will take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

### We will put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data will only be transferred to a Processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

### All [Company] employees are responsible for ensuring the security of our systems by adhering to this and related policies including [Company] IT and Security policies, which contain details about appropriate use and security of the devices and systems that are in [Company] IT environment.

## Transferring Personal Data

### We may transfer any Personal Data we hold within the DIFC. In relation to Personal Data that i) we transfer out of the DIFC or ii) specifically to the UK, or a country within the European Economic Area ("EEA"), we may subsequently transfer that Personal Data to another country provided that certain conditions set out in Articles 26 or 27 of the DP Law 2020 apply, including but not limited to:

* + 1. The country to which the Personal Data are transferred ensures an adequate level of protection in accordance with Article 26 of the DP Law 2020.
    2. The Data Subject has given his consent.
    3. The transfer is necessary for one of the reasons set out in the Data Protection Laws, including the performance of a contract between us and the Data Subject, or to protect the vital interests of the Data Subject.
    4. The transfer is legally required on substantial public interest grounds or for the establishment, exercise or defence of legal claims.

## Accountability to Data Subjects

### Our use or disclosure of Personal Data must be necessary for the purpose(s) or compatible with the purpose(s) for which we collect and keep the data. Except in certain limited circumstances (including where we are required by law) we should only use and disclose the data in ways consistent with that purpose(s).

### We will inform Data Subjects who provide us with or inform us about their Personal Data regarding:

* + 1. The purpose or purposes for which we intend to process that Personal Data.
    2. How we process their Personal Data, including information about third party suppliers who process it on our behalf.
    3. The types of third parties, if any, with which we will share or to which we will disclose their Personal Data.
    4. The means, if any, with which Data Subjects can limit our use and disclosure of their Personal Data.
    5. Any other rights they have with respect to our use of their Personal Data in line with the Data Protection Laws.
    6. The methods and mechanisms we have in place to be transparent with and accountable to the Data Subject.
    7. The [Company]’s role as a Controller of their Personal Data and how to reach the [Compliance Officer] [and] / [or] [DPO].

# Disclosure / sharing of Personal Data with Government Entities

## We may share Personal Data we hold with another Controller such as a Government Entity upon request by such entities, provided a legitimate basis to do so exists and it is undertaken in accordance with Article 28 of the DP Law 2020. In determining the validity and proportionality of the request, we shall ensure that, inter alia, it:

### has a valid legal basis (i.e. a legally valid warrant, court order, or other specific judicial or regulatory mandate, amongst others);

### comes from a public entity that has the authority to make such request;

### is not overly broad or vague, as to cover every possible information over the Data Subjects, without rationale; and

### is properly served, as per the applicable law.

## As such, having provided for the requirements of Article 28, we may also disclose Personal Data we hold to such entities when we are under a duty to disclose or share a Data Subject's Personal Data in order to comply with any legal obligation, or in order to enforce or apply any contract with the Data Subject; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of national security, taxation transparency, fraud protection and credit risk reduction.

## We may share Personal Data we hold with selected third parties for the purposes including but not limited to fulfilling contractual requirements and obligations arising in law.

# Making and Dealing with Personal Data sharing requests and prevailing laws

## While requests to share Personal Data for whatever reason may often be low risk, strict adherence to the Data Protection Principles is required, with certain, limited exceptions.

## Exceptions exist in i) Dubai Law No. 9 of 2004, which clarifies that any legal or regulatory exceptions to the powers and authority of the DIFC must be specifically stated in relevant legislation, and ii) in Federal Law No. 8 of 2004, which carves out any action that is not covered by civil or commercial law, depending on the circumstances.

## Where there is a risk to national security, public safety or the financial and economic infrastructure of the UAE that results in a data sharing request from a Government Entity, the application of relevant laws should be considered to ensure disclosures are made appropriately, if at all, and do not conflict with said laws to the extent legally possible, as follows:

### DP Law 2020, subject to any limited exemptions set out therein

### UAE Cyber Security Law

### UAE Federal and international laws on Anti Money Laundering, Tax evasion and base profit erosion

### Telecoms Regulatory Authority (TRA) Law / Lawful Interception related laws

### Anti-Terrorism, law enforcement and crime prevention laws

### UAE Anti-Hate / Anti-Discrimination Law

### UAE Weapons Law

### Dubai Data Law

[LIST OTHERS AS APPLICABLE]

## As a Controller we may decide to disclose information and / or participate in a data sharing arrangement, to the extent permissible by the Data Protection Laws. Where a conflict of Data Protection Laws and other laws such as those in Section 6.1 exists such that Personal Data protection or indeed protection of the person him or herself to whom the data belongs may be negatively impacted by the requirement or request to share such data, and notwithstanding Section 5.2, primary consideration must be given to consultation with the requesting entity to ensure a very strictly construed interpretation of the request is agreed and / or rejected where allowable.

## Wherever possible and practical, consideration should be given to data matching processes that restrict the amount of personal information shared. Providing large data sets may be considered where it would otherwise be inefficient or difficult to achieve the objective of the data sharing in through minimization.

## Ensure that data sharing proposals made and received are balanced and proportionate, applying a reasonable analysis to the type and circumstances of the request.

## Consider implementing data sharing agreements to support compliance with Data Protection Laws.

## Before establishing a data sharing agreement, we shall be satisfied that:

### all parties recognize the actual benefits and who will receive them as well as how they will be measured;

### the purpose of the data sharing falls within the purposes outlined in legislation (or regulations for defined public services objectives);

### there is clear documentation of, and accountability for, making the decision to share data;

### information sharing will be physically and/or technically possible and be compliant with Data Protection Laws and other relevant legislation;

### strict compliance with applicable security guidelines to safeguard against any misuse or loss of data, including having secure methods in place for transferring data;

### as the Controller, it is appropriate to engage in data sharing, for example there are no perceived conflicts of interest or risk to the Data Subjects rights and freedoms; and

### the minimum required information will be disclosed.

## Disclosures may only be made for the purpose of meeting the objectives limited to and consistent with the purposes of the Government Entity’s powers. What constitutes fair processing and limited, consistent purposes in this regard will vary from case to case, but a key consideration will be the reasonable expectation of the individual whose data it is as to how their data would be handled or whether it would be disclosed. Transparency as to how the data is being processed, including willingness of the entities sharing the data to publicly provide data sharing activity details is also key.

## All transfer and disclosure processes must be suitable for the types of data proposed to be disclosed before any data is shared.

### We shall discuss with the proposed recipients their arrangements for securely receiving, handling and managing the data and make an assessment of the suitability of the systems and processes (which should be described in the data sharing agreement).

### In considering whether to share information, we shall also consider whether conditions need to be imposed on the future use and retention of the data, to be clearly specified in any sharing agreements prior to sharing information.

## We shall use reasonable endeavours to ensure that entities processing data on our behalf meet one or more of the legitimate processing requirements set out in Article 9 and where applicable Article 10 of the DP Law 2020 depending on the data being shared.

## Where a data sharing proposal is received stating that information is to be disclosed to a body which is not a Government Entity / Public Authority, but fulfils a public function, an assessment should be made of any conflicts of interest and identify whether there are any unintended risks involved with disclosing data.

### Non-public entities can only participate in a data sharing arrangement once their sponsoring Government Entity / Public Authority has assessed their systems and procedures to be appropriate for secure handling data.

### Details will need to be set out in the [privacy impact assessment](https://www.difc.ae/business/operating/data-protection/accountability/#s4) (PIA) along with a statement of compliance with Data Protection Laws in the data sharing agreement.

## As per Article 28(1)(c) of the DP Law 2020, where reasonably practicable, we shall obtain appropriate written and binding assurances from the Government Entity / Public Authority that it will respect the rights of Data Subjects and comply with the general data protection principles set out in Part 2 of the DIFC DP Law 2020. Such written assurances could come in many forms, including:

### a basic data sharing Memorandum of Understanding;

### an annex to the DIFC Standard Contractual Clauses;

### a simple email agreement citing Article 28 of the DP Law 2020; or

### a full data protection agreement.

## To ensure proper due diligence in dealing with the transfer request, we shall consider when making the transfer decision:

### whether the jurisdiction is included in the [List of international jurisdictions approved by DIFC Commissioner of Data Protection](https://www.difc.ae/business/operating/data-protection/data-export-and-sharing/#s3) (the “**Commissioner**”) on transferring personal data;

### the level of risk in exporting to that jurisdiction, as identified in the DIFC’s Ethical Data Management Index; and

### conducting and documenting an assessment of the importing Government Entity / Public Authority based on the DIFC Ethical Data Management Risk Index (EDMRI)+ Assessment of Importing Entities, which gives the Commissioner’s view of potential for risks in an importing entity’s compliance environment.

# Rights of Redress

## It is important that checks are made on the accuracy and quality of data prior to transferring it, in line with the general data protection principles set out in Section 4 above.

## In instances where issues or conflicts arise following the transfer of data, redress procedures aligned with Articles 32 to 40 as well as Part 9 of the DP Law 2020 are required to allow for inaccurate data to be corrected or for other Data Subjects’ rights such as access, objection or erasure to be enforceable by all bodies holding the information.

## Organisations involved in data sharing activities should agree the process of recording and capturing corrections across all systems where the data is or will be held for auditing purposes and contacting the Data Subject where appropriate and set the details out in a data sharing agreement.

# Data Sharing Process Considerations

## Carefully consider why any data sharing activities are to be undertaken. In addition to the conditions and obligations set out in Article 28, please review the Data Sharing Checklist available in [Appendix A](#_Appendix_A_–).

## Maintain an audit trail of decisions to ensure that informed decisions on data sharing are made at the right level in the organization.

## Conducting a PIA of the proposal should be one of the first steps taken. It will help to assess the potential benefits against the risk or potential negative effects, such as an erosion of personal privacy.

### A PIA is a process that helps identify and reduce the privacy risks of a data share. A PIA should be reviewed at critical milestones and updated where necessary, for example the type of data collected materially changes and processing could impact the rights and freedoms of individuals.

### A privacy notice describes all the privacy information an organization collects, makes available or provides to individuals or third parties and what it does with Data Subjects’ personal information. In exercising these powers to share data, please ensure that suitably worded privacy notices are published and made available to the public. The Commissioner’s privacy notices guidance provides information on the content of these notices, as well as where and when to make them publicly available.

## Government Entity data sharing proposals and requests require a number of documents to be produced and ideally should be made available to the general public for review and comment where possible. These documents are:

### A business case for the data sharing arrangement (this can be co-developed by all the organisations involved and redacted to ensure information impacting national security or other sensitive information is not revealed);

### Data sharing agreement(s), which may or may not be legally binding and that ensure information will be retained securely and deleted once it has been used for the purpose for which it was provided, prevent accidental loss, destruction or damage of information, allow for sanctions and remedies for unlawfully or inappropriately processing data, and ensure only people with a genuine business need have access to the information; and

### Security plan requiring all parties to adhere to specific technical and organizational protocols, appropriate incident response and resolution management policies, and data storage, retention and disposal policies.

# Governance, Review and Monitoring

## Respond swiftly and effectively to any complaints, objections or requests under the right of access to personal information and periodically run checks to ensure data security best practice is adhered to.

## Where data quality issues are identified, the governance structure supporting the data sharing arrangement should take immediate steps to identify and manage the risks associated with the use of that data and any remedial action required.

## Data Subjects should be able to access data sharing activity information to understand what information is being shared and for what purposes.

## A person or persons responsible for reviewing any data sharing proposals made, received and actioned will oversee any data sharing activities (“Data Sharing Reviewer”). The Data Sharing Reviewer(s) will also be responsible for collating the evidence which will inform the DIFC Commissioner’s review of the functioning of the data sharing activities from time to time, to be determined on a reasonable basis.

## Any serious Personal Data security breaches (i.e., breaches that compromise a Data Subject’s confidentiality, security or privacy) need to be reported immediately to the Commissioner, any relevant data protection or other authority, such as law enforcement where necessary. In certain instances, such breach shall be also communicated to the Data Subject:

### as soon as practicable, when the breach is likely to result in a high risk to the security or right of the affected Data Subject; or

### promptly, if there is an immediate risk of damage to the affected Data Subject.

# Confidential Commercial Information

## Where confidential commercial information is requested directly or it may included in Personal Data that has been requested by a Government Entity, [Company] must ensure that any legally binding or other confidentiality obligations are adhered to in the final determination of which and / or how much data may be shared. Please contact [a senior manager] [or] [*Insert [Company] Department or Officer responsible for legal/compliance matters*] for further assistance to help make such determination.

# Questions about this Policy

## If you have any questions about this Policy, or any concerns or complaints with regard to the administration of this policy, please contact [*Insert [Company] Department or Officer responsible for legal/compliance matters*].

## Complaints or further escalation about any data sharing practices or activities conducted by [Company] whether in accordance with this policy or not can be made to the [*Insert Officer / Head of Department responsible for hearing complains*] and finally to the Commissioner, as per Parts 8 and 9 of DP Law 2020.

# Appendix A – Data Sharing Checklist

**Checklist - points to consider**

Why share

● For what purpose and public function is the information being requested?

● Are there any other benefits of the data exchange for the receiving party or any other public body?

● What are the implications of not sharing information? Such as:

o Increased risk that people do not receive the support or the services they require in a timely manner;

o Risk that burdens will be placed on people to repeatedly supply information to access the services they require; and

o Risk of wasting taxpayers’ money by jeopardizing public finances or commercial projects.

What to share

● What exact data items are required and why?

● Can we redact any part of the data transferred so we transfer only the minimum necessary data needed to comply (i.e., by narrowly interpreting the request)?

● Are there any express legal restrictions in place on the disclosure and use of the data involved and are there any legal obligations on the recipient of the data to provide it to any other bodies?

● How regularly and in what volume is it proposed to share the data?

● Are there any ethical issues with the proposed data sharing arrangement?

How to share

● What methods or technology can be used to minimize the amount of information shared and risk of data loss (e.g., using aggregate data, derived data or the use of a look-up process, in preference to bulk data sharing)?

● What procedures will be in place to correct any inaccurate data identified during the data sharing process and the process for capturing the changes made for auditing purposes?

● What are the conditions for processing information, will Data Subjects be aware that their data is being processed and will procedures for dealing with access requests, queries and complaints be in place?

● Information handling responsibilities, including details of any Processors, contractors or subcontractors;

● Security considerations, e.g. the use of secure transfer mechanism, and encryption;

● For audit purposes document the process and methods of exchange, how exchanges are logged, what information is stored and who has access to it;

● Standards and levels of expected operational service;

● Termination arrangements;

● Minimizing cost of providing/transferring the data;

● Issues, disputes and resolution procedures;

● Sanctions for failure to comply with the agreement or breaches by individual staff;

● Is there a time-limit suggested for using the data and if so how will the data be deleted; and

● Periodic reviews of effectiveness and necessity of data sharing arrangement.

1. This policy has been drafted on the assumption that the entity is a company based in the DIFC. Change the reference accordingly to “the Foundation”, “the Association” or “the NPIO”, throughout the document, in case the entity is not a company. [↑](#footnote-ref-2)
2. You may Change the reference accordingly to “the Processor” throughout the policy, in case the entity is fulfilling the role of a Processor, rather than a Controller. [↑](#footnote-ref-3)
3. If the entity if Foundation or NPIO etc., it shouldn’t refer to business and commercial but to a more general, non-commercial term. [↑](#footnote-ref-4)