CONTROLLER AND PROCESSOR AGREEMENTS AND OBLIGATIONS

Commissioner of Data Protection

CONTENTS

1. Introduction

The goal of the DIFC Commissioner of Data Protection (the **Commissioner**) in producing this guidance is to assist Controllers and Processors subject to the Data Protection Law, DIFC Law No. 5 of 2020 (the "DPL") and the Data Protection Regulations issued pursuant to the DPL (the "Regulations") about the obligations and contracting requirements set upon them primarily by way of Articles 23 to 25.

If you require further information or clarification about anything provided in this guidance document or any other guidance referenced herein, please contact the Commissioner's Office either via the DIFC switchboard, via email at commissioner@dp.difc.ae or via regular mail sent to the DIFC main office. Also, you may wish to refer to the DIFC Online Data Protection Policy.

2. Scope

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 has been adapted from and should be read in conjunction with existing UK guidance, as well as with EU laws and guidance on the same topic, with which the DP Law is also aligned.

Please note that ***this guidance 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.*

3. Overview

This guidance addresses contractual content, obligations and liabilities between Controllers and Processors in detail. It will help both Controllers and Processors to understand what needs to be included in a written agreement and why. It will also help Processors to understand their responsibilities and liabilities under the DIFC DP Law 2020.

Contracting parties should, if required, seek advice from their own trade or professional organisations, and obtain professional advice on updating existing contracts and agreeing the terms of new contracts with respect to data protection obligations that must be included. The commercial aspects of the written agreement are a matter for the parties, so long as contractual requirements embedded in commercial aspects that impact the Processing of Personal Data, if any, comply with the DIFC DP Law 2020.

4. Written Agreements

The DIFC DP Law 2020 says that a written agreement / contract is needed in two circumstances – where data is shared between Controllers, and where data is shared from a Controller to a Processor for processing. From the outset, it is important to note that in line with Article 24(10), both a Controller and Processor are in breach the DP Law 2020 if they commence mutually agreed Processing activity without a written agreement referred to in Articles 24(1) and 24(3).

Controllers

A Controller, or an entity that alone or jointly with others, determines the purposes and means of the processing of personal data, may wish to hand personal data over to other Controllers so it may determine what to do with such data for its own purposes. An example of this is where one government authority may share personal data it has in its database with another government authority that express a need for it, but for a different purpose. Rather than obtain it directly, they may receive it from the original collecting entity. Bear in mind there are obligations that still must be met with respect to lawful processing bases when such data sharing occurs. Please review available Lawful Processing guidance available on the DIFC DP Guidance website to help you understand these parallel obligations.

Article 23(2 and 3) state:

> *(2) Joint Controllers shall, by way of legally binding written agreement, define their respective responsibilities for ensuring compliance with the obligations under this Law. Such agreement shall clarify the process for ensuring that a Data Subject can exercise his rights under this Law and for*

providing a Data Subject with the information referred to in Articles 29 and 30.

(3)The written agreement referred to in Article 23(2) or an appropriate summary shall be made available to an affected Data Subjects [if requested].

Article 23(2) could be complied with not only by a direct contract between the Controllers, but also by other legally binding contractual arrangements (for example, a set of contracts between multiple parties) provided the Processor is ultimately bound, as a matter of contract law, to each Controller in respect of the particular processing.

Processors

It is common practice for a Controller to engage a Processor to process personal data on its behalf – for example, to take advantage of the Processor's expertise and experience in a particular type of processing operation, technology, or business activity. Processors, or entities that process personal data on behalf of the Controller, have obligations to the Controllers, to Data Subjects, and if a Sub-processor, to the primary Processor, as well.

Articles 24(1 to 4) state:

(1) Where Processing is to be carried out on behalf of a Controller by a Processor, the Processing shall be governed by a legally binding written agreement between the Controller and the Processor. A Controller shall only enter into agreements with Processors that provide sufficient assurances to implement appropriate technical and organisational measures that ensure the Processing meets the requirements of this Law and protects a Data Subject's rights.

(2) A Processor may not engage another Processor to act as a Sub-processor without the prior written authorisation of a Controller. A Controller may only give a general written authorisation where it has ensured that conditions are in place to enable appointed Sub-Processors (present or future) to provide the assurances under Article 24(1). If a general written authorisation has been given, a Processor shall inform a Controller of any intended changes concerning the addition or replacement of a Sub-processor. A Processor shall take into account any good faith objection raised by a Controller to such intended changes.

(3) Subject to Article 24(2), a Processor may not engage a Sub-processor for carrying out specific Processing activities on behalf of the Controller, unless a legally binding written agreement containing the requirements set out in Article 24(5) is in place with such Sub-processor that ensures a full delegation of the obligations that the

Processor owes to the Controller under the agreement with the Controller in respect of such specific Processing activities.

(4) Where a Sub-processor fails to fulfil its data protection obligations under an agreement or Applicable Law, the Processor that engaged it shall remain fully liable to a relevant Controller for the performance of the Sub-processor's obligations.

Key Take-aways

The key take-aways of Articles 23 and 24 are:

- A written, legally binding agreement is required at every level. Always.
- Prior authorisation to engage a Sub-processor is required at every level. Always.
- Clear setting out of responsibilities and / or instructions is required at every level. Always.
- Assurances set out in Article 24(1) are required at every level. Always.
- In the end, at least one party to the written agreement will be accountable for liabilities (even in some cases, third party liabilities). Always.

These are quite high standards. It demonstrates how important it is to operationalise the legal requirements provided throughout DP Law 2020 by way of a well-written contract. This doesn't mean that there isn't room for creativity or finding practical solutions to potential contracting problems – provided your thinking and decision-making is documented, and risk about your contracting approach is assessed and, importantly, mitigated.

Some useful tips to meet these very high standards are set out below.

- Evaluate any Processors before engaging with them to ensure they will comply with the requirements of either the DIFC DP Law 2020 or an equivalent law that imposes obligations to maintain appropriate technical and organisational measures in its own organisation and with respect specifically to the processing services they will perform.
- Every time a Processor uses another Processor (a Sub-processor), there must be a written agreement between the Processor and the Sub-processor. The terms of the contract that relate to Article 24 must offer an equivalent level of protection for the personal data as those that exist in the written agreement between the Controller and the Processor.
- (When in doubt,) Conduct a Data Protection Impact Assessment

- Complete the Ethical Data Management Risk Index+ assessment questions to help you make this determination. (Incidentally, it doesn't hurt to do this when dealing with Joint or Co-controllers as well!). Some considerations may be:
    - the extent to which they comply with industry standards, if these apply in the context of the processing;
    - whether they have sufficient technical expertise to assist the Controller, i.e., in carrying out obligations under Parts 2 to 7 of the DIFC DP Law 2020 (technical measures, breach notifications and DPIAs);
    - providing the Controller with relevant documentation, i.e., their privacy policy, record management policy and information security policy; and
    - adherence to an approved code of conduct or a certification scheme (if or when they become available).

- Utilise other assessment tools such as those offered on the DIFC DP Guidance website, on the Tools & Templates page under Data Protection Assessment Tools

- Standardise contract or other legal templates, and consider getting legal advice or support to draft them

- Develop a Partner or Third Party Code of Conduct that includes terms about data protection law compliance, privacy enhancing technology and trained, and information security. Ensure that Joint or Co-Controllers and Processors agree to sign up to it.

- Check in now and then – utilise any regulatory compliance audit clauses in your legal templates, and if you don't have audit clauses, add them.

- Review the data protection clauses of any standard contract templates and update them accordingly.

- Where the other party to the agreement appears hesitant to include such clauses, consider whether they can be trusted to keep the Personal Data of the relevant entity secure and available for Data Subjects when they exercise their rights to access it or restrict its further processing.

- Do all of the above!!

5. Contents of Written Agreements

Details about the Processing

Article 24(5) states that the written agreement must include the following details about the processing:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of Data Subject; and
- the Controller's obligations and rights.

The Controller therefore needs to be very clear from the outset about the extent of the processing it is contracting out.

Minimum Required Terms

The minimum terms required for each Processor or Sub-processor written agreement are set out in Article 24(5)(b), as follows:

> *(i) Process Personal Data based on documented instructions from a Controller, including sharing of Personal Data in response to a request made by a Requesting Authority (as described in Article 28), or transfers of Personal Data to a Third Country or an International Organisation, unless required to do so by Applicable Law to which the Processor is subject;*
>
> *(ii) where Applicable Law, as referred to in Article 24(5)(b)(i), applies:*
>
> > *(A) inform any relevant counterparty; or*
> >
> > *(B) where there is a chain of Processors and Sub-processors, ensure that the Controller is notified, unless the Applicable Law in question prohibits such information being provided on grounds of Substantial Public Interest;*
>
> *(iii) ensure that persons authorised to Process relevant Personal Data are under legally binding written agreements or duties of confidentiality;*
>
> *(iv) take all measures required pursuant to Article 14;*

(v) comply with the conditions referred to in Articles 24(2) and (3) for engaging any Sub-processor;

(vi) assist a relevant counterparty by providing appropriate technical and organisational measures for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights, having taken into account the nature of the Processing;

(vii) assist a relevant counterparty in ensuring the Controller's compliance with the obligations pursuant to Articles 14, 20, 21, 41 and 42, taking into account the nature of Processing and the information available to the Processor;

(viii) delete or return all Personal Data to the Controller, at the Controller's option, or make the same available for return to a relevant counterparty after the end of the provision of services relating to Processing, and delete existing copies unless Applicable Law requires storage of the Personal Data;

(ix) make available to the Controller, relevant counterparty, or the Commissioner (upon request) all necessary information to demonstrate compliance with the obligations in this Article 24; and

(x) permit and provide reasonable assistance with audits, including inspections, conducted by:

(A) a relevant counterparty;

(B) another auditor mandated by a relevant counterparty; or

(C) the Commissioner.

Key take-aways

Processing only on the Controller's documented instructions

Under Article 24(5)(b)(i) the written agreement must say that the Processor may only process personal data in line with the Controller's documented instructions (including when responding to an Article 28 request or making an international transfer of personal data) unless it is required to do otherwise by applicable law.

The written agreement may include details of these instructions specified or those instructions may be provided separately.

An instruction can be documented by using any written form, including email. The instruction must be capable of being saved, so that there is a record of the instruction.

This contract term should make it clear that it is the Controller, rather than the Processor, that has overall control of what happens to the personal data. However, if a Processor acts outside of the Controller's instructions in such a way that it decides the purpose and means of processing, including to comply with a statutory obligation, then it will be deemed a Controller in respect of that processing and will have the same liability, in other words, it will assume all responsibilities and obligations, of a Controller.

Confidentiality

Under Article 25, a further obligation of confidentiality is established. It says:

> *A Controller or Processor, and where applicable, a Joint Controller or a Sub-processor, shall take steps to ensure that any person acting under its respective authority that has access to Personal Data shall not Process it except on the instructions of the Controller, unless it is required to do so under Applicable Law.*

This obligation, which should be included in any written agreements, should cover the Processor's employees as well as any temporary workers and agency workers who have access to the personal data.

Appropriate accountability measures

Under Article 24(5)(b)(iv) the written agreement must oblige the Processor to take all security measures required pursuant to Article 14. This primarily includes taking measures that will ensure the security of processing.

Both Controllers and Processors are obliged under Article 14(2)(b) to put in place appropriate technical and organisational measures to ensure the security of any personal data they process. Such measures may include, as appropriate:

- encryption
- pseudonymisation;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore access to personal data in the event of an incident; and
- processes for regularly testing and assessing the effectiveness of the measures.

Adherence to an approved code of conduct or certification scheme may be used as a way of demonstrating compliance with security obligations. Codes of conduct and

certification may also help Processors to demonstrate sufficient guarantees that their processing will comply with the DIFC DP Law 2020.

Breach of written agreements

Article 24(9) and 24(10) state the following, which all parties should remember while drafting the written agreement:

> (9) If a Processor infringes this Law by determining the purposes and means of Processing, the Processor shall be considered to be a Controller in respect of that Processing and will assume all the responsibilities and obligations of a Controller.
>
> (10) Both a Controller and Processor are in breach of this Law if they commence mutually agreed Processing activity without a written agreement referred to in Articles 24(1) and 24(3).

Data Subjects' rights

Under Article 24(5)(b)(vi) the written agreement must provide for the Processor to take "appropriate technical and organisational measures" to help the Controller respond to requests from individuals to exercise their rights.

This provision stems from Part 6 of the DIFC DP Law 2020, which describes how the Controller must enable Data Subjects to exercise various rights and respond to requests to do so, such as subject access requests, requests for the rectification or erasure of personal data, and objections to processing. For more information, please read our guidance on individuals' rights.

Assisting the Controller

Under Article 24(5)(b)(vii) the written agreement must say that, assist a relevant counterparty in ensuring the Controller's compliance with the obligations pursuant to Articles 14, 20, 21, 41 and 42, taking into account the nature of Processing and the information available to the Processor. The Processor must also provide assistance with audits and inspections, as well as make available to the Controller, relevant counterparty or the Commissioner (upon request) all necessary information to demonstrate compliance with the obligations in Article 24.

As such, the written agreement must be as clear as possible about how the Processor will help the Controller meet its obligations.

End-of-contract provisions

Under Article 24(5)(b)(vii) the written agreement must say that at the end of the agreement term, the Processor must:

- at the Controller's choice, delete or return to the Controller all the personal data it has been processing for it; and
- delete existing copies of the personal data unless applicable requires it to be stored.

It should be noted that deletion of personal data should be done in a secure manner, in accordance with applicable security requirements. For more information, please review DIFC Information Security measures in place and consider using this approach as a starting point.

The written agreement must include end of contract provisions to ensure the continuing protection of the personal data after the agreement or relationship ends. This reflects the fact that it is ultimately for the Controller to decide what should happen to the personal data being processed, once processing is complete.

The practical reality is that it may not be possible for data in backups or archives to be deleted immediately on termination of an agreement. Provided appropriate safeguards are in place, such as the data being put immediately beyond use (see Article 22(3)), it may be acceptable that the data is not deleted immediately if the retention period is appropriate and the data is subsequently deleted as soon as possible, i.e., on the Processor's next deletion/destruction cycle.

6. Recommended Clauses

While Article 24(8) of the DP Law 2020 permits the Commissioner to publish recommended contractual clauses for written agreement under Articles 23 and 24, which are available in the Article 24 Contract Clauses & DIFC Abbreviated SCCs (the "Article 24 Guidance"). As set out in Article 24(8), the incorporation of such clauses in an applicable written agreement shall be sufficient to discharge the obligations in Articles 24(5)(b)(i) to 24(5)(b)(x) inclusive.

The table below maps the recommended clauses provided in the Article 24 Guidance with Article 24(5)(a)(i) to 24(5)(a)(iv) and Article 24(5)(b)(i) to 24(5)(b)(x).

Recommended Clause	Wording	DPL or A. 24 Reference
1.1	*[The definitions set out in Schedule 1, Section 3 of the Data Protection Law, DIFC Law No. (5) of 2020 shall apply to all relevant capitalized terms in this Clause.]*	None
1.2	*[Unless otherwise agreed on a case-by-case basis, the parties agree to share, at no cost and free from any charge, information, trends, reports, and other such data as may be necessary to achieve the purpose of their co-operation. In particular, the parties may share information and documents in relation to capital markets or technical assistance under the principle of professional secrecy and reciprocity.]*	None
1.3	*Any exchange and/or processing of Personal Data, shall take place in accordance with the provisions of the [DP Law] [Data Protection Legislation].*	None
1.4	*To the extent permitted by the laws of a Party subject to a government data sharing request, ("Requesting Party"), the Requesting Party shall inform the Party providing the relevant information ("Providing Party") about how or where the requested information will be stored or utilized, and any assurances that will further safeguard the requested information.*	Article 24(5)(b)(i) Article 24(5)(b)(ii) Aligns with Article 28
1.5	*Unless otherwise agreed in advance, neither party may appoint a Sub-processor of Personal Data processed pursuant to this [Agreement / MOU] without the prior written consent of the other party [which shall not be unreasonably withheld]. Any such appointment must include a written agreement containing all necessary controls and safeguards [as set out in Article 24 of the DP Law].*	Article 24(3) Article 24(5)(b)(v)

Recommended Clause	Wording	DPL or A. 24 Reference
1.6	*Both parties shall ensure that any person(s) authorized to process the Personal Data in accordance with this [Agreement / MOU] have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality [as set out in Article 25 of the Data Protection Legislation].*	Article 24(5)(b)(iii)
1.7	*Both parties shall implement appropriate compliance, technical and organizational measures to ensure the security of the Personal Data obtained or processed for the purposes of this [Agreement / MOU], including conducting risk or processing impact assessments as needed and assisting with audits or inspections conducted by an appropriate, recognised third party, and agree to notify any reportable Personal Data Breaches to the appropriate parties, [including the Commissioner of Data Protection or the Data Subject].*	Article 24(5)(b)(iv) Article 24(5)(b)(vi) Article 24(5)(b)(vii) Article 24(5)(b)(viii)
1.8	*Regarding any promotion or marketing activity performed under this [Agreement / MOU], both parties shall comply with applicable direct marketing laws, if any.*	None
1.9	*Without prejudice to the generality of this Clause [X.3], each party will ensure that it has all necessary and appropriate contractual clauses, consents and notices in place generally, and specifically to enable exercise of applicable Data Subjects' rights (including assisting with responses) or to support lawful processing of Personal Data for the duration and purposes of this [Agreement / MOU].*	Article 24(5)(b)(i) Article 24(5)(b)(vi) Article 24(5)(b)(x)
1.10	*Where Personal Data is transferred outside the DIFC to parties in jurisdictions that do not have a data protection law equivalent to that of the Data Protection Legislation in accordance with Article 26 of the Law, [or where an existing law may not be fully enforced such that it impacts accountability of the [THIRD PARTY]], the parties agree to supplement this Clause [X] with applicable standard contractual data sharing clauses approved in accordance with Article 27 and the DIFC Data Protection Regulations 2020.*	Article 24(5)(b)(i)
Additional clauses to address remaining issue / where not otherwise included		
1.11	*All Parties shall comply with [DIFC Data Protection Law, DIFC Law No. (5) of 2020 and its obligations thereunder] [in addition to applicable [Data Protection Legislation]].*	Article 24(5)(a)(iv)
1.12	*This Agreement shall be entered into by [X], in its capacity as [Controller/Processor] and [X], in its capacity as [Processor/Sub-Processor] of Personal Data whereby [X] will process Personal Data on behalf of and in accordance with the instructions of [Controller/Processor] for the duration of this [Agreement / MOU] or until termination or expiry [in accordance with Clause [X] of this [Agreement / MOU]].*	Article 24(5)(a)(i) Article 24(5)(b)(i)

Recommended Clause	Wording	DPL or A. 24 Reference
1.13	*For the purposes of this Agreement, the [Processor/Sub-processor] agrees to process the following Personal Data for the specified purposes:* *[list type of Personal Data and purpose for Processing]*	Article 24(5)(a)(ii) Article 24(5)(a)(iii)
1.14	*The [Processor/Sub-processor] will process the Personal Data set out in Clause [X] which relates to the following categories of Data Subjects:* *[set out list of Data Subjects, i.e., employees, clients, suppliers, contacts, etc].*	Article 24(5)(a)(iii)

There are other good examples of contract clauses available that will meet the above requirements. Please have a look at the clauses approved by the Danish Data Protection Authority for use in such instances.

https://edpb.europa.eu/sites/default/files/files/file2/dk_sa_standard_contractual_clauses_january_2020_en.pdf

7. Controller's Liability When Engaging Processors

A Controller is primarily responsible for its own compliance and ensuring the compliance of its Processors. This means that, regardless of the terms of the written agreement with a Processor, the Controller may be subject to any of the corrective measures and sanctions set out in the DIFC DP Law 2020. These include orders to bring processing into compliance, claims for compensation from a Data Subject and administrative fines. For more details about how we exercise our powers, please see the Fines and Sanctions guidance on the DIFC DP Guidance website.

An individual can bring claims directly against a Controller if the processing breaches the DIFC DP Law 2020, in particular where the processing causes the individual damage. A Controller will be liable for any damage (and any associated claim for compensation payable to an individual) if its processing activities infringe the DIFC DP Law 2020.

However, a Controller will not be liable for damage resulting from a breach of the DIFC DP Law 2020 if it can prove it was not in any way responsible for the event giving rise to the damage. If a Processor is involved in the processing, the individual making the claim for compensation can claim against either party, because in the

first instance, among others, the DIFC DP Law 2020 applies to the other party by way of Article 6(3)(b). If a Controller has to pay full compensation for damage suffered by individuals, it may be able to claim back all or part of the amount of compensation from a Processor involved in the processing, to the extent that the Processor is at fault.

8. Processor and Sub-processor Autonomy and Responsibilities

A Processor may make its own day-to-day operational decisions, but Article 24 says it should only process personal data in line with a Controller's instructions, unless it is required to do otherwise by applicable law (in that case it must inform the Controller of this legal requirement before the processing, unless that law prohibits it doing so on important grounds of public interest). This is also a required contract term.

If a Processor acts outside of a Controller's instructions in such a way that it decides the purpose and means of processing, then it will be a Controller and will have the same liability as a Controller.

In addition to the contract terms, a Processor also has direct responsibilities and liabilities under the DIFC DP Law 2020. When drawing up and negotiating a written agreement for data processing, it is good practice for all parties to make sure they understand this.

The parties may also wish to explicitly cover this in the written agreement, although the DIFC DP Law 2020 doesn't require it. For example, they may wish to include a clause specifying that nothing in the written agreement relieves the Processor or Controller of its own direct responsibilities and liabilities under the DIFC DP Law 2020 – and to say what these are.

A Processor may be contractually liable to the Controller for any failure to meet the terms of their agreement. This will of course depend on the exact terms of that agreement. It will also be subject to the relevant investigative and supervisory powers of the Commissioner's Office and may be subject to administrative fines or other penalties.

An individual can also bring a claim directly against a Processor in court. A Processor can be held liable under Article 64 to pay compensation for any damage caused by processing, including non-material damage such as distress. A Processor will only be liable for the damage if:

- it has failed to comply with DIFC DP Law 2020 provisions specifically relating to Processors; or
- it has acted without the Controller's lawful instructions, or against those instructions.

It will not be liable if it can prove it is not responsible for the event giving rise to the damage.

If a Processor is required to pay compensation, but is not wholly responsible for the damage, it may be able to claim back from the Controller, the share of the compensation for which they are responsible. Both parties should seek professional legal advice on this.

If you are a Sub-processor, you will be liable for any damage caused by your processing only if you have not complied with the DIFC DP Law 2020 obligations imposed on Processors or you have acted contrary to lawful instructions from the Controller, relayed by the Processor, regarding the processing.

If you are a Processor and use a Sub-processor to carry out processing on your behalf, you will be fully liable to the Controller for the Sub-processor's compliance with its data protection obligations. This means that, under Article 24(4), if a Sub-processor is at fault, the Controller may claim back compensation from you for the Sub-processor's failings. You may then claim compensation back from the Sub-processor.

A Sub-processor may also be contractually liable to the Processor for any failure to meet the terms of the agreement. This will of course depend on the exact terms of that agreement.

A Processor or Sub-processor must immediately inform the Controller or Processor (as applicable) whether, in its opinion, the Processing activity infringes the DP Law 2020.

Controllers, Processors and Sub-processors should seek their own legal advice on issues of liability and the contracts between Controllers and Processors and Processors and Sub-processors.

9. Questions and Comments

Please contact the DIFC Commissioner of Data Protection either via the DIFC switchboard, via email at commissioner@dp.difc.ae or via regular mail sent to the DIFC main office for any clarifications or questions related to this document. You may also wish to refer to the DIFC Online Data Protection Policy.