Cross-Border Data Transfers – Key Considerations

Disclaimer: *This document is provided as guidance only and does not constitute legal advice. Service Providers should not rely solely on this guidance and are advised to seek their own independent legal advice in relation to their specific circumstances.*

Introduction

As part of Dubai Holding's data protection requirements and due diligence process, we need to understand how our Service Providers (including their staff or contractors in a third country location) will access or process personal data.

This document explains:

- What counts as a cross-border data transfer
- Why remote access from outside the UAE is treated as a transfer
- What information and evidence we seek from Service Providers before granting access

Our goal is to ensure compliance with data protection laws and protect the personal data of our customers.

A. Why Remote Access Counts as a Cross-Border Data Transfer

Dubai Holding processes personal data on behalf of customers that are subject to the EU General Data Protection Regulation (GDPR), China Personal Information Protection Law (PIPL), and KSA and UAE Personal Data Protection Laws. Where personal data originating from the European Economic Area (EEA) has been lawfully transferred to and is now hosted on systems in the United Arab Emirates (UAE), Dubai Holding remains bound by a range of data protection requirements regarding onward transfers of that data to other third countries.

> **Under the GDPR, a transfer of personal data occurs not only when data is physically moved or copied to another location, but also when personal data is *accessed by or made accessible to* another jurisdiction.**

This means that when personnel located outside the UAE are granted remote access to Dubai Holding systems containing personal data of customers, this constitutes an onward transfer under the GDPR and equivalent data protection laws.

The European Data Protection Board (EDPB) has confirmed this broad interpretation of the concept of a 'transfer', noting that **remote access from a third country** (e.g. VDI

access, overseas support teams, remote / offshore resources and cloud storage) qualifies as a transfer of personal data, even if the personal data itself remains physically stored in one place. This interpretation is consistent with the approach taken under other data protection regimes, including:

- Kingdom of Saudi Arabia - The Saudi Data & AI Authority (SDAIA) issued its Risk Assessment Guideline which explicitly identifies remote access as a form of cross-border transfer requiring appropriate safeguards and risk assessment.
- China – The Personal Information Protection Law (PIPL) defines cross-border data transfers broadly and prevailing industry practice considers remote access to constitute a transfer.

This means that if your team, affiliates or contractors will access any personal data internationally, we must ensure that appropriate safeguards are in place.

B. Due Diligence Requirements – What We Require

Before proceeding with any engagement involving the processing of personal data by Service Providers, we require clarity on the below matters. This information enables us to assess whether appropriate safeguards are in place to support a lawful cross-border data transfer.

Identities of all legal entities	The full legal name, registered address, and corporate status of entities that will be involved in providing services or accessing personal data. This is essential to identify the legal entities that will be acting as a data processor or sub-processor.
Relationship between entities	The corporate relationship between the UAE-based entity and the entity/entities abroad. Specifically, whether the entities are subsidiaries of the same group of companies, affiliates, branch offices or independent third parties.
Governance between entities	Where the entities are independent, confirmation of a data processing agreement between the entities. Where the entities are part of the same group of companies, an explanation on how the group governs data transfers (e.g. Standard Contractual Clauses or Binding Corporate Rules). Technical and organisational controls that are enforced.
Transfer Impact Assessment	Sight of the Transfer Impact Assessment (TIA) undertaken by the data processor in relation to the cross-border transfer. The TIA should consider, among other things, the nature of the data, the purposes of the processing, the legal framework (including any

	laws permitting government access to data), and the technical and contractual safeguards in place to mitigate identified risks.
Shared infrastructure and systems	Confirmation of whether the entities share any technology infrastructure, including (without limitation) Microsoft Outlook, SharePoint, Teams, or other cloud-based collaboration tools. It is important for us to understand which systems are shared, who has access to them, and what technical and organisational measures are in place to restrict, monitor and secure access to personal data.

C. Service Provider Due Diligence Checklist

During the due diligence process, please provide the following information and evidence:

- ☐ Full legal name, registered address, and corporate status of all entities that will be providing services or accessing personal data.
- ☐ Confirmation of the corporate relationship between the UAE-based entity and the other entities involved (e.g., subsidiaries, affiliates, branch offices, or independent third parties).
- ☐ Details of the lawful transfer mechanism(s) in place to govern the transfer of personal data between the entities (e.g., Standard Contractual Clauses, Binding Corporate Rules, or other approved mechanisms).
- ☐ A copy of the TIA conducted in respect of the transfer of personal data, including the technical and contractual safeguards in place to mitigate any identified risks.
- ☐ A list of all the data processor's systems and infrastructure (including cloud-based tools such as Microsoft Outlook, SharePoint, Teams, or similar platforms) that are shared with, or accessible by, personnel abroad, and which may contain personal data processed on behalf of Dubai Holding.
- ☐ Details of the technical and organisational controls implemented to restrict, monitor, and secure access to personal data by personnel abroad.