# Key Data Protection Contractual Clauses

## A. Introduction

Dubai Holding applies data protection clauses to all service providers who handle personal data on its behalf or in connection with the provision of services. These clauses ensure compliance with applicable data protection laws and protect the personal data of Dubai Holding's customers and employees.

The specific contractual clauses applied to a service provider depend on:

- The **processing role** of the parties (i.e., whether the service provider acts as a data processor on behalf of Dubai Holding, or as an independent data controller in its own right); and
- The **assessed risk level** of the processing activity (standard or elevated risk), as determined via Dubai Holding's service provider due diligence assessment process.

This document summarises the key contractual obligations that service providers can expect to see in their data protection clauses with Dubai Holding. Since these clauses align with applicable data protection laws and regulations, they should not require amendment for compliance purposes.

## B. Overview of Key Clauses

The following section summarises the key data protection obligations that Dubai Holding includes in its service provider agreements. Where noted, additional requirements may apply depending on the risk level of the processing activity.

1. **Purpose Limitation and Processing Instructions**

- Service Providers acting as Processors must only process personal data in accordance with Dubai Holding's documented instructions and solely for the purpose of providing the contracted services.
- Processing for any other purpose is prohibited unless required by law (in which case the Service Provider must notify Dubai Holding in advance).

2. **Data Security**

- Service Providers must implement and maintain appropriate technical and organisational controls to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access.
- For elevated risk engagements, the clauses specify additional measures including:

- Implementation of controls comparable to the Dubai Holding standards published at https://privacy.dubaiholding.com/en/controls/technical-organisational-controls;
- Pseudonymisation / encryption of personal data;
- Measures to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems;
- The ability to restore availability and access to personal data in a timely manner; and
- Regular testing and evaluation of the effectiveness of security controls.

- For Controller-to-Controller arrangements, both parties must implement appropriate controls in accordance with data protection laws.

**3. Confidentiality and Personnel**

- All personnel authorised to process personal data must be bound by obligations of confidence equivalent to those in the data protection clause.
- For elevated risk engagements, Service Providers must additionally provide regular data protection training to all personnel involved in the services.
- Personal data must not be disclosed to any employee, director, agent, contractor, or third party except as necessary for the performance of the services, to comply with law, or with Dubai Holding's prior written consent.

**4. Data Subject Rights**

- Service Providers must promptly notify Dubai Holding (via privacyoffice@dubaiholding.com) on receipt of any request, complaint, or claim relating to data subject rights.
- Service Providers must cooperate with and assist Dubai Holding in responding to such requests where required.

**5. Sub-Processors**

- Service Providers may not engage any sub-processor to process Dubai Holding personal data without prior written consent. Authorised sub-processors must be disclosed at the outset of the engagement.
- Where consent is granted (elevated risk): sub-processors must be bound by data protection terms no less protective than those with Dubai Holding, including equivalent Standard Contractual Clauses for cross-border data transfers.
- Service Providers remain fully liable for the acts or omissions of sub-processors.

**6. Cross-Border Data Transfers**

- For standard engagements: Personal data must not be processed outside the UAE, EU/EEA, or UK unless legally required (with notice to Dubai Holding).

- For elevated risk engagements: Processing outside the UAE, PRC, KSA, EU/EEA, or UK requires Dubai Holding's prior written consent and the use of an approved transfer mechanism (e.g., Standard Data Protection Clauses, Binding Corporate Rules, or an adequacy decision).
- Where transfers are authorised by Dubai Holding, the relevant Standard Data Protection Clauses are incorporated by reference and accessible via Dubai Holding's Privacy Centre (https://privacy.dubaiholding.com/en/international-transfer-agreements):
    - UK International Data Transfer Agreement;
    - EU Standard Contractual Clauses;
    - PRC Standard Contract for Outbound Transfer; or
    - KSA Standard Contractual Clauses.
- Service Providers must implement and maintain technical and organisational controls comparable to Dubai Holding's standards published for such transfers.
- If a transfer mechanism becomes unlawful, the parties must use best endeavours to agree an alternative. If no lawful transfer is possible, transfers must cease immediately.

**7. Data Breach Notification**

- Service Providers must notify Dubai Holding promptly and without undue delay of any actual or suspected personal data breach at privacyoffice@dubaiholding.com.
- Service Providers must cooperate fully with any breach investigation and take all necessary steps to remediate and prevent re-occurrence.

**8. Audit and Accountability**

- Service Providers must comply with all reasonable requests from Dubai Holding to verify and evidence compliance with data protection obligations.
- For elevated risk engagements: Dubai Holding (or its qualified representatives) may conduct periodic security scans, inspections, and/or audits of the Service Provider's systems and processes, subject to reasonable advance notice (except where a breach is suspected or a regulator instructs otherwise). The clauses additionally require service provider assistance with Dubai Holding's data protection impact assessments.
- Dubai Holding may share audit findings with group companies, professional advisors, and regulators.
- If an audit reveals non-compliance, the Service Provider must promptly resolve it at its own cost and reimburse Dubai Holding's reasonable audit costs.

**9. Data Retention and Deletion**

- On termination or expiry of the agreement, Service Providers must promptly and securely delete or return (at Dubai Holding's option) all personal data, including copies, processed on its behalf.
- Retention is permitted only where strictly required by law (with notice to Dubai Holding) or where metadata is retained for the duration of a cycle.
- For elevated risk engagements, the Service Provider must certify in writing (if requested) that deletion has been completed by it and each sub-processor.

**10. Liability and Indemnity**

- Service Providers agree to indemnify Dubai Holding in respect of all data protection losses arising from any breach of the data protection clauses caused by the Service Provider, its employees, subcontractors, or agents. Data protection losses include costs, claims, settlements, regulatory fines, penalties, data subject compensation, and costs of rectification or restoration.

## C. Risk-Based Application of Clauses

Standard Processing

- Applies to straightforward processing activities with limited data categories and limited exposure to international data protection laws.
- Usually, personal data that consists of purely UAE data subjects.
- Cross-border transfers are generally not permitted under these clauses.

Elevated Risk Processing

- Applies where the processing involves sensitive data categories, large volumes of personal data, cross-border transfers, or complex sub-processing arrangements.
- A comprehensive set of data protection clauses is applied, including detailed security specifications, cross-border transfer mechanisms, accountability and governance provisions, and enhanced audit rights.

Controller-to-Controller Arrangements

- Where the Service Provider acts as an independent controller (rather than a processor), a separate template applies that addresses:
    - Each party's independent controller responsibilities;
    - Mutual breach notification;
    - Mutual indemnity; and
    - Cross-border transfer mechanisms.