Data Protection Due Diligence Guidance - What We Require

This document outlines Dubai Holding's key data protection requirements for service providers and provides guidance corresponding to each section of the due diligence assessment.

Section 1 - Scope

Will you be viewing, collecting, processing and/or have access to personal data?

✅ Answer Yes. If you have received a due diligence assessment, Dubai Holding is aware that personal data is in scope.

Section 2 - Data Transfers

Will any personal data be transferred across borders?

❌ If your operation is UAE-only, the answer will be No.

✅ If you have staff / contractors, parts of your company (e.g., affiliates) or other companies / sub-processors working outside the UAE, the answer is likely to be Yes. Remote access (e.g. VDI access, overseas support teams, remote / offshore resources and cloud storage) constitutes a cross-border data transfer.

Section 3 - Sub-Processors

Will any data be shared with any third parties (e.g., sub-processors)?

❌ If your services do not rely on any other companies, the answer will be No.

✅ If your services will involve other group companies (parent or subsidiary) or third-party companies, the answer is Yes. We require:

- full legal names of all companies involved;
- their locations;
- their relationship to your company; and
- whether there is a data processing agreement in place between your company and those companies.

Section 4 - Certifications

Are your operations certified?

✅ If you have relevant certifications or accreditations, such as those listed below, please share them with us.

- ISO 27001
- ISO 27701
- SOC 2 Type II

Section 4 - Internal Policies

Do you have a documented privacy programme and policy? Do you have a data breach policy?

- ✅ We expect to see a signed internal privacy policy and data breach policy (if separate). At a minimum, we will accept the front page, contents page and evidence of when it was operationalised (usually the approval page). Your policy regarding data breaches should include a mechanism and timeframes for notifying clients.

- ❌ We do not need to see your public-facing online privacy policy and will not accept a pure IT security policy.

Section 4 - Internal Procedure

Do you have documented procedures that operationalise your policies?

- ✅ We expect to see a signed internal procedural document demonstrating how your privacy policies are implemented in practice. For example, process workflows, data retention schedules, and DSAR procedures.

Section 5 - Privacy Training

Do you provide your staff with regular privacy or data protection training?

- ✅ We expect to see evidence of your organisation's standalone privacy or data protection training. We will accept screenshots of the training or a training contents page, or signed attendance registers or completion certificates.

- ❌ We will not accept evidence of pure IT security training.