

Remote Pro Ai

Data Processing Agreement — key terms (summary)

How we process client personal data, transfer it lawfully, secure it and manage subprocessors, in plain language.

Version 2026.10 · last legal review: pending counsel

A summary of the key terms published on remote-pro.ai — not the operative agreement.

Published October 2026 · Source: the published text at remote-pro.ai/en/legal/dpa · SHA-256 of the source text 70f68c9f1883ab3a

Contents

- | | |
|--|--|
| 1. How we handle personal data in your engagement | 6. Technical and organisational measures |
| 2. In short | 7. Clause outline |
| 3. Saudi PDPL: transfers on contractual safeguards | 8. Subprocessors, region by region |
| 4. UAE PDPL, DIFC and ADGM in one annex | 9. Questions |
| 5. GDPR: SCCs and a published transfer assessment | |

How we handle personal data in your engagement

The DPA governs personal data our engineers process for you: you are the controller, we are the processor. Annexes cover Saudi PDPL, UAE PDPL, DIFC, ADGM and GDPR.

Key terms at a glance

1. **Roles:** client as controller, Remote Pro Ai as processor for engagement data.
2. **Instructions:** we process personal data only on the client's documented instructions.
3. **Personnel:** everyone with access is bound by confidentiality and has passed background checks.
4. **Security:** technical and organisational measures listed in Annex 3 and reviewed every year.
5. **Location:** processing region and residency pattern fixed in the Statement of Work.
6. **Subprocessors:** general authorisation, 30 days' notice of changes and a right to object.
7. **Breach notification:** to the client within 24 hours of confirming a personal-data breach.
8. **Assistance:** support for data-subject requests, DPIAs and regulator enquiries.
9. **Saudi transfers:** Saudi standard contractual clauses plus a transfer risk assessment.
10. **UAE transfers:** UAE PDPL terms; DIFC or ADGM clauses where those regimes apply.
11. **EU and UK transfers:** GDPR SCCs (Module 2) with a transfer impact assessment; UK Addendum.
12. **Audit:** reports in the Trust Center, plus on-site audit with 10 working days' notice.
13. **Return and deletion:** data returned or deleted at the end of the engagement, with written confirmation.
14. **Government requests:** client notified unless the law forbids it; overbroad requests challenged where lawful.

15. Liability: a separate data-protection liability cap of 24 months' fees, above the 12-month cap in the MSA.

In short

The Remote Pro Ai Data Processing Agreement (DPA) governs personal data our engineers process for clients. The client is the controller; Remote Pro Ai is the processor. It includes annexes for Saudi PDPL, UAE PDPL, DIFC and ADGM, and GDPR, with standard contractual clauses for transfers. Personal-data breaches are reported to the client within 24 hours of confirmation.

You decide why and how personal data is used. We process it only on your instructions, wherever the contract says.

Saudi PDPL: transfers on contractual safeguards

Where personal data leaves the Kingdom, we rely on Saudi standard contractual clauses and a documented risk assessment.

The Saudi Personal Data Protection Law (PDPL), supervised by SDAIA, restricts transfers of personal data outside the Kingdom. For transfers to our Cairo team, the annex uses the standard contractual clauses issued under the PDPL transfer regulation, in the module matching the transfer, together with a transfer risk assessment.

- No adequacy claim is made for Egypt, the UAE or any other destination
- Pattern A or B keeps data in-Kingdom; remote access is assessed and logged
- Processor support for the controller's 72-hour notification duty to SDAIA
- Arabic version prevails for contracts under Saudi law

UAE PDPL, DIFC and ADGM in one annex

The annex follows the regime that applies to your entity: federal, DIFC or ADGM.

- **Federal:** UAE Federal Decree-Law No. 45 of 2021, with safeguards for destinations lacking adequate protection.
- **DIFC:** DIFC Data Protection Law No. 5 of 2020, with DIFC standard contractual clauses.
- **ADGM:** ADGM Data Protection Regulations 2021, with ADGM standard contractual clauses.
- **Hosting:** Pattern B in a UAE cloud region on request, recorded in the Statement of Work.

GDPR: SCCs and a published transfer assessment

Remote access from Cairo to EU data is a transfer. We cover it with SCCs and supplementary measures.

When EU clients use Remote Pro Ai engineers, access from Egypt to EU personal data is a restricted transfer under the GDPR. The annex incorporates the European Commission's 2021 standard contractual clauses, Module 2 (controller to processor), and Module 3 for onward transfers to subprocessors.

Transfer impact assessment summary

- **Destination:** Egypt, which has no EU adequacy decision; Egypt's Personal Data Protection Law No. 151 of 2020 considered
- **Data minimisation:** Pattern A or B keeps EU data in EU systems; no bulk storage in Egypt
- **Supplementary measures:** encryption in transit and at rest, zero-trust access, session logging, key custody by the client where possible
- **Government access:** policy to notify, challenge and disclose the minimum required
- **UK:** International Data Transfer Addendum for UK GDPR transfers

Technical and organisational measures

The controls in Annex 3, summarised. Evidence is available in the Trust Center under NDA.

- **Access:** SSO with MFA, least privilege, just-in-time privileged access, quarterly access reviews
- **Devices:** managed devices with disk encryption and remote wipe; no personal devices for client data
- **Network:** zero-trust access, client VDI where required, no split tunnelling
- **Encryption:** TLS 1.2 or higher in transit; AES-256 at rest on Remote Pro Ai systems
- **Development:** secrets scanning, static analysis and dependency scanning on every commit
- **AI tools:** approved tools only, zero-retention modes, no client code in consumer AI tools
- **People:** 5-gate vetting, background checks, confidentiality terms and annual security training
- **Monitoring:** centralised logs, alerting and incident response with 24-hour client notification
- **Continuity:** documented business-continuity and disaster-recovery plans, tested every year
- **Offboarding:** access removed on the last working day through a logged checklist

Clause outline

The PDF and DOCX files of this text are a key-terms summary, in English and Arabic (version 2026.10; last legal review: pending counsel). They are not the operative DPA, which is issued with your quotation after counsel review. This outline shows the structure.

1. Definitions and scope
2. Roles of the parties
3. Processing instructions
4. Confidentiality of personnel
5. Security of processing
6. Subprocessors
7. International transfers
8. Data-subject requests
9. Personal-data breaches
10. DPIAs and prior consultation
11. Audits and information
12. Government access requests
13. Return and deletion

14. Liability

15. Term and precedence

Annex 1: Description of processing · Annex 2: Subprocessor register · Annex 3: Technical and organisational measures · Annex 4: Saudi PDPL terms · Annex 5: UAE PDPL, DIFC and ADGM terms · Annex 6: GDPR SCCs and UK Addendum · Annex 7: Egypt PDPL terms · Annex 8: US state privacy terms (CCPA)

Version 2026.10 · published October 2026 · last legal review: pending counsel

Subprocessors, region by region

The register is Annex 2 of this DPA and lives in the Trust Center, with 30 days' notice before changes.

Questions

Is Remote Pro Ai a controller or a processor?

For personal data our engineers handle inside your systems, you are the controller and Remote Pro Ai is the processor, acting only on your documented instructions. For our own business data, such as your account contacts and invoices, Remote Pro Ai is the controller, and the privacy notice explains how we handle it.

Does Saudi data leave the Kingdom?

Only if your contract allows it. With Pattern A or B, data stays in your environment or your in-Kingdom cloud region. Where remote access from Cairo counts as a transfer, the Saudi annex applies standard contractual clauses and a transfer risk assessment. We make no adequacy claims for any destination.

Why do you need SCCs if EU data stays in the EU?

Under the GDPR, an engineer in Egypt viewing EU personal data is a transfer, even if the data never leaves an EU server. The Module 2 SCCs and the transfer impact assessment cover that access, and supplementary measures such as encryption, zero-trust access and logging reduce the risk further.

How quickly will you tell us about a breach?

Within 24 hours of confirming a personal-data breach that affects your data. The notice includes what happened, the data involved, the likely impact and the steps taken, followed by updates as the investigation continues. This gives you time to meet your own regulatory deadlines, such as 72 hours under the GDPR and the Saudi PDPL.

Can we object to a new subprocessor?

Yes. We give 30 days' notice before a new subprocessor processes your personal data. You can object on reasonable data-protection grounds during that period. We then work with you on an alternative; if none is possible, you can end the affected service without penalty, as set out in the DPA.