Master Service Agreement

Version: 28102026

1. Definitions

For the purposes of this Master Service Agreement:

- **“Agreement”** means the applicable Proposal, Service Order, Statement of Work, this Master Service Agreement, and any other document expressly incorporated into the agreement between the parties.
- **“Client”** means the individual or entity purchasing or receiving the Services.
- **“Company”** means AI Geeks Limited.
- **“Services”** means the services provided by the Company under the Agreement.
- **“Deliverables”** means any project-specific work product created for the Client under the Agreement, including, where applicable and forming part of the agreed scope, software source code, configuration, database schemas, design assets, documentation, and other project-specific outputs expressly developed for the Client.
- **“Company Personnel”** means employees, contractors, consultants, developers, project managers, designers, engineers, and other personnel engaged by the Company.
- **“Third-Party Services”** means external products or services used in connection with the Services, including cloud services, software licences, APIs, AI services, automation platforms, messaging services, monitoring tools, security services, databases, storage, and other technology services.
- **“Third-Party Service Costs”** means charges incurred from Third-Party Services.
- **“Business Hours”** means 9:00 a.m. to 5:00 p.m., Monday to Friday, UAE time, excluding UAE public holidays.
- **“Out-of-Hours”** means any time outside Business Hours, including weekends and UAE public holidays.

2. Provision of Services

The Company will provide the Services described in the applicable Proposal, Service Order, Statement of Work, or service appendix.

The Company may use employees, contractors, consultants, subcontractors, and Third-Party Services to deliver the Services.

The Company determines how its personnel and resources are allocated. The Client is contracting with **AI Geeks Limited**, not with individual Company Personnel.

Unless expressly authorised by the Company in writing, individual Company Personnel cannot amend the Agreement, agree pricing or discounts, waive fees, enter into separate commercial arrangements, or otherwise bind the Company.

3. Fees and Charges

The Client will pay the fees stated in the applicable Proposal, Service Order, Statement of Work, or other agreed commercial document.

Fees may include recurring service fees, project fees, hourly or resource fees, Third-Party Service Costs, administration charges, and additional or out-of-scope work.

All fees are exclusive of VAT and other applicable taxes unless expressly stated otherwise.

4. Third-Party Costs

The Client is responsible for third-party costs reasonably required to provide or operate the Services, including cloud services, software licences, APIs, AI services, messaging services, security tools, and other external technology services.

Where such services are procured, managed, billed to, or paid by the Company on behalf of the Client, they will be recharged at actual cost without mark-up, including any applicable taxes, currency conversion costs, and bank

charges incurred by the Company.

Where reasonably practicable, the Company will notify the Client of any material increase or significant change in Third-Party Service Costs.

Any specific spending limits, approval thresholds or budget controls will be set out in the applicable Proposal or Statement of Work.

Time spent by Company Personnel on procurement, account administration, licence management, vendor coordination, and reconciliation may be charged separately at the Company's applicable standard hourly rates where outside the agreed scope.

Any configuration, integration, management, monitoring, or support provided by the Company may still be charged separately where outside the agreed scope.

5. Payment Terms

Unless otherwise agreed:

- recurring fees may be invoiced monthly in advance;
- usage-based and third-party costs may be invoiced in advance based on estimates or in arrears based on actual usage;
- invoices are due within 14 days;
- all invoices must be paid in full by the due date without withholding, deduction, set-off, or delay;
- any complaint, warranty claim, service issue, or other dispute will be handled separately and does not suspend the Client's payment obligations;
- payment of an invoice does not prevent the Client from subsequently pursuing a valid claim under the Agreement;
- late payments may incur interest at 1% per month, calculated from the due date until payment is received, or the maximum amount permitted by applicable law, whichever is lower; and
- Where permitted by applicable law, the Client will be responsible for reasonable legal, collection and other third-party costs incurred by the Company in recovering overdue amounts.

Where an overdue amount requires formal recovery action, reasonable time spent by Company Personnel on collection, dispute management, recovery or enforcement may be charged at the Company's applicable standard hourly rates.

6. Changes and Additional Work

Work outside the agreed scope may be charged separately.

This may include additional development, features, integrations, migrations, infrastructure changes, specialist work, additional stakeholder management, and Out-of-Hours services.

Where reasonably practicable, the Company gives a written estimate to, and obtains the written approval of the Client before undertaking material additional chargeable work.

Work caused by Client actions, third-party changes, incorrect instructions, unauthorised access, deleted data, configuration changes, or failure to follow Company recommendations may also be charged separately.

The Company is not responsible for delays caused by the Client's failure to provide required information, access, approvals, decisions, credentials, or other dependencies.

Where Client delay materially affects progress, the Company may pause the Services, reallocate resources, and revise delivery dates, milestones, or charges as reasonably required.

7. Client Responsibilities

The Client will:

- provide accurate requirements and information;
- provide timely access, feedback, approvals, and decisions;

- nominate an authorised contact;
- protect credentials and maintain appropriate internal security;
- ensure it has the necessary rights to data and content supplied to the Company;
- ensure its activities comply with applicable law;
- promptly report suspected security incidents;
- avoid unauthorised infrastructure changes;
- ensure third-party developers coordinate relevant technical changes with the Company; and
- pay invoices when due.

The Client remains responsible for its business decisions, application users, data, content, legal obligations, and regulatory requirements.

The Company may refuse, delay, or require written confirmation of any instruction that it reasonably believes may create a security risk, cause data loss, breach applicable law, materially affect service stability, conflict with accepted technical or security practices, or create an unreasonable operational risk.

The Client will be responsible for reasonable losses, claims, liabilities, and costs incurred by the Company arising from Client-provided data, content, materials, instructions, unlawful use of the Services, infringement of third-party rights, or the Client's breach of applicable law or this Agreement, except to the extent caused by the Company's own breach.

8. Primary Authorised Contact

The Client will nominate one Primary Authorised Contact and may nominate one Deputy Authorised Contact who may act where the Primary Authorised Contact is unavailable.

The Client is responsible for coordinating its internal stakeholders and consolidating instructions, approvals, and requirements through the Primary Authorised Contact or, where unavailable, the Deputy Authorised Contact.

Additional Client points of contact may be accommodated where required. Where this results in material additional coordination, administration, meetings, or management effort, the Company may apply additional charges, which will be discussed with the Client in advance.

The Client must promptly notify the Company if either authorised contact changes.

9. Mutual Non-Solicitation and Non-Circumvention

Each Party may communicate with the other Party's personnel in the ordinary course of the relationship between the Parties.
However, without the other Party's prior written consent, neither Party may:

- directly employ, engage, contract with, or enter into any separate commercial arrangement with any employee, contractor, consultant, or other personnel of the other Party who has been involved in the Services or the relationship between the Parties;
- make direct payments or provide compensation to such personnel for separate work or services;
- engage such personnel privately for services that could reasonably be provided through the other Party; or
- knowingly bypass or circumvent the other Party in relation to services, work, opportunities, or commercial relationships.

These restrictions apply regardless of whether a Party approaches the other Party's personnel or the personnel approaches that Party.

If personnel of either Party directly approach the other Party regarding employment, consulting, contracting, side work, or another commercial arrangement outside their existing relationship, the receiving Party must obtain the other Party's written approval before entering into that arrangement.

These restrictions apply during the Agreement and for **12 months after termination or expiry of the Agreement**. General recruitment advertising that is not specifically targeted at the other Party's personnel will not

constitute a breach.

Direct Engagement Fee:

- If either Party directly or indirectly employs, engages, or retains personnel of the other Party in breach of this clause, the breaching Party will pay the other Party a Direct Engagement Fee equal to **12 months of the reasonable market value of that individual's services** at the time of engagement.
- Market value will be assessed by reference to the commercial market rate for a person of comparable role, seniority, experience, and capability and will not be based solely on the salary, contractor fee, or other compensation paid to that individual.
- Where the affected Party has an established external billing rate for the individual or an equivalent role, that rate may be used as evidence of market value.
- The Direct Engagement Fee is intended to compensate the affected Party for recruitment, replacement, training, loss of resource availability, disruption, and loss of commercial opportunity resulting from the direct engagement.

10. Confidentiality

Each party will keep confidential all non-public commercial, technical, financial, security, customer, pricing, and proprietary information received in connection with the Services. Confidential information may only be used for the purposes of performing or receiving the Services.

Disclosure is permitted where required by law or to professional advisers or personnel who reasonably require access and are subject to appropriate confidentiality obligations.

These obligations continue for 24 months after termination, except where information remains protected by law or constitutes a trade secret.

11. Intellectual Property

Unless otherwise stated in a Proposal or Statement of Work:

- the Client retains ownership of materials and intellectual property supplied by the Client;
- the Company retains ownership of its pre-existing intellectual property, methodologies, frameworks, libraries, tools, processes, reusable components, and know-how; and
- ownership or licensing of project-specific Deliverables will be governed by the applicable Proposal or Statement of Work.

All Client data, including data provided by the Client and data generated, collected or derived through the Client's use of the Deliverables or Services, remains the property of the Client. For clarity, this does not transfer ownership of the Company's software, methodologies, algorithms, system-generated technical logs, aggregated or anonymised data that does not identify the Client or any individual, or other Company intellectual property.

Where any Company pre-existing intellectual property, reusable component, library, framework, tool or other Company material is embedded in or reasonably necessary to use the Deliverables, the Company grants the Client a perpetual, worldwide, royalty-free, non-exclusive licence to use, modify and maintain those embedded materials solely for the Client's and its affiliates' internal business operations in connection with the Deliverables. This licence does not permit the Client to sell, sublicense, distribute or commercially exploit those materials separately from the Deliverables.

Client-specific business processes, rules, workflows and operational know-how disclosed by the Client and identified as confidential or proprietary remain the Client's confidential information. This does not restrict the Company from using general concepts, industry-standard practices, independently developed processes, reusable software components, development techniques, or knowledge and experience gained during the engagement, provided the Client's confidential information is not disclosed or reproduced.

The Company will not white-label, rebrand, resell, sublicense, or commercially distribute the Client's Deliverables, products, services, or Client-specific business processes as its own or for any third party without the Client's prior written consent.

Third-party products remain subject to the relevant provider's licence terms.

Unless otherwise agreed in writing, ownership rights in project-specific Deliverables will transfer to the Client only after the Company has received full payment of all amounts due in relation to those Deliverables. Until full payment is received, the Company retains ownership of the Deliverables and grants the Client only such limited rights as are reasonably necessary for review and testing.

Unless expressly included in the applicable Proposal or Statement of Work, the Company is not required to provide internal development tools, deployment pipelines, reusable libraries, templates, methodologies, internal working files, or other Company materials used in producing the Deliverables. However, the Company will provide the source code, build and deployment instructions, configuration information, and documentation reasonably necessary for a competent developer to build, deploy and maintain the Deliverables.

12. Deliverable Completion and Acceptance

A Deliverable, milestone, or scope of work will be considered complete when the principal tasks, functionality, and outputs identified in the applicable Proposal or Statement of Work have been completed and delivered.

The Company will give the Client written notice of completion and may issue the applicable invoice at that point. Issuing the invoice is not conditional on Client acceptance, and the review period below runs in parallel with the payment terms in clause 5.

The Client has 10 Business Days from the notice of completion to either confirm acceptance in writing or raise a written objection identifying specific Acceptance Criteria set out in the applicable Proposal or Statement of Work which have not been met, with sufficient detail to reproduce the issue. If neither is received within that period, the Deliverable is deemed accepted.

An objection is not valid to the extent it relates to:

- minor defects, cosmetic issues, snagging items, documentation, training, or other non-material items;
- additional requests or changes outside the agreed scope;
- warranty items that do not materially prevent use of the Deliverable; or
- matters other than specific unmet Acceptance Criteria.

Where the Client raises a valid objection, the Company will correct the identified items and re-submit the Deliverable, whereupon a further 5 Business Days review period applies to the corrected items only.

Where a valid objection is raised, the Client may withhold 20% of the associated invoice until the identified items are resolved, and the balance falls due in accordance with clause 5. In all other cases the full invoice falls due, and neither the review period nor an invalid objection suspends or delays payment.

Any remaining defects or warranty issues will be addressed separately under clause 24 and, except to the extent of the 20% withholding above, do not suspend or delay the Client's obligation to pay an invoice when due.

If the Client believes that material items within the agreed scope remain incomplete after the review period has closed, this will be handled as a dispute under clause 26 and will not suspend the payment obligation.

13. Systems, Accounts and Access

The Company may administer Client-owned or Company-managed systems and accounts as required to provide the Services.

Where reasonably practicable, app-store developer accounts, cloud hosting accounts, domain registrations, payment gateway accounts and other material production accounts specific to the Client will be established in the Client’s name or transferred to the Client, with the Company granted such administrative access as is reasonably required to provide the Services. Where an account cannot reasonably be held in or transferred to the Client’s name due to provider, technical or operational limitations, the Company will provide reasonable cooperation to facilitate appropriate Client access or transfer when practicable.

Access will be provided based on operational need and appropriate security controls.

The Client must not provide administrative credentials or infrastructure access to unauthorised third parties where doing so may create a security or operational risk.

Third-party developers or providers requiring access must coordinate relevant changes with the Company.

The Company may replace or change Third-Party Services, tools, infrastructure components, or technical architecture where reasonably required for security, availability, supportability, cost, or operational reasons, provided this does not materially reduce the agreed Services. The Company will notify the Client of any material change where reasonably practicable.

The Company may recommend the replacement or upgrade of obsolete, unsupported, insecure, or end-of-life technology. The Company will not be responsible for failures, vulnerabilities, or security issues arising from the Client's decision to continue using such technology against the Company's recommendation.

14. Support and Response Times

Support will be provided during Business Hours unless otherwise agreed.

The Company may designate an official support, project management, or ticketing channel.

Where such a channel has been designated, support requests, defects, incidents, change requests, and other service requests must be submitted through that channel to be treated as formally received.

The Company will use commercially reasonable efforts to acknowledge:

- urgent production incidents within two Business Hours; and
- non-urgent requests within one Business Day.

Acknowledgement means confirmation that the request has been received and is being reviewed. It does not mean resolution.

Resolution times depend on the nature and complexity of the issue, system access, Client cooperation, provider availability, third-party responses, and whether the issue is within the agreed scope.

Unless a separate Service Level Agreement is agreed in writing, response times are targets only and do not create any right to service credits, penalties, refunds, or other compensation.

15. Out-of-Hours and Emergency Services

The Company is not required to respond to Out-of-Hours requests but may do so subject to availability.

Out-of-Hours, weekend, UAE public holiday, and emergency services will be charged at 2× the Company's applicable standard hourly rate, unless otherwise agreed in writing.

Where immediate action is reasonably required to protect systems or data, contain a security incident, prevent material disruption, or restore a critical service, the Company may take reasonable emergency action where appropriate.

16. Third-Party Providers

The Client acknowledges that some Services rely on providers outside the Company's direct control.

The Company is not responsible for circumstances outside its reasonable control, including provider outages, API failures, provider pricing changes, service limitations, account suspension, discontinued products, telecommunications failures, or other external-provider issues.

The Company will use commercially reasonable efforts to assist with relevant third-party issues within the agreed scope.

17. Security Incidents

Where a security incident occurs, the Company may provide investigation, isolation, recovery coordination, and restoration assistance within the agreed scope.

Specialist services such as forensic investigation, regulatory reporting, penetration testing, specialist incident-response consultants, extensive data reconstruction, legal advice, or application-code remediation may be charged separately.

Where a security incident involves Personal Data processed by the Company on behalf of the Client, the Company's notification and cooperation obligations will be governed by the applicable Data Processing Agreement.

18. Data Protection

Each Party will comply with its obligations under applicable data-protection and privacy laws.

Where the Company processes Personal Data on behalf of the Client in connection with the Services, such processing will be governed by the **Data Processing Agreement attached to and forming part of this Agreement**.

For **Software Development Services**, the Data Processing Agreement applies to Personal Data accessed, used, tested, migrated, configured, or otherwise processed by the Company in connection with software development, implementation, integration, testing, support, maintenance, and related development activities.

For **Infrastructure and Hosting Services**, the Data Processing Agreement applies to Personal Data processed in connection with hosting, managed infrastructure, storage, databases, backups, monitoring, logging, security, disaster recovery, production infrastructure, technical support, and related operational services.

Where both Software Development Services and Infrastructure and Hosting Services are provided, the Data Processing Agreement applies to the Processing associated with each respective category of Services.

The Data Processing Agreement will govern matters relating specifically to the Processing of Personal Data, including controller and processor responsibilities, processing instructions, confidentiality, security, subprocessors, international transfers, Personal Data Breaches, assistance, audits, retention, return, and deletion.

To the extent of any conflict between this Agreement and the Data Processing Agreement concerning the Processing of Personal Data, the Data Processing Agreement will prevail only to the extent of that conflict and only in relation to that Processing.

The Client remains responsible for determining and complying with its own privacy and data-protection obligations, including lawful basis, consents, privacy notices, retention requirements, and data-residency requirements.

19. Force Majeure

The Company will not be responsible for any delay, interruption, failure, or inability to perform the Services caused by events outside its reasonable control.

This may include cloud or telecommunications outages, cyberattacks, war, civil unrest, government action, sanctions, natural disasters, power failures, labour disruption, widespread technology failures, supplier failures, or similar events.

Where such an event affects the Services, the Company’s affected obligations will be suspended for the duration of the event and any applicable delivery dates, milestones, or response obligations may be reasonably extended.

The Company will use commercially reasonable efforts to reduce the impact of the event and restore the affected Services where reasonably possible

The Company will notify the Client as soon as reasonably practicable after becoming aware of a Force Majeure

event that materially affects the Services.

If a Force Majeure event continues for more than 45 days and materially prevents performance of the affected Services, either Party may terminate the affected Services, Proposal, Statement of Work, or Service Order by written notice.

20. Suspension

The Company may suspend some or all Services where:

- an invoice remains unpaid for 10 Business Days after written notice from the Company that the amount is overdue;
- the Client's activities are unlawful;
- there is a serious security or operational risk;
- a third-party provider suspends an applicable service;
- continued operation would expose the Company to material unpaid costs;
- unauthorised technical changes create material risk; or
- suspension is required by law, regulation, security requirements, or a provider.

Where reasonably practicable, the Company will notify the Client before suspension. Immediate suspension may occur where reasonably necessary to address a serious security, legal, operational, or financial risk.

Suspension does not waive, reduce, or postpone the Client's obligation to pay amounts already due or any recurring fees, Third-Party Service Costs that continue to be incurred during the suspension.

The Company may require all overdue amounts and applicable charges to be paid before Services are restored. Reasonable work required to suspend, secure, or restore Services may be charged separately.

21. Termination

Unless otherwise agreed, either party may terminate recurring Services by providing at least 30 days' written notice.

The Client remains responsible for:

- all fees payable through the notice period;
- Third-Party Service Costs incurred until the relevant services, subscriptions, accounts, or resources are actually cancelled, transferred, or shut down;
- any committed, prepaid, minimum-term, or non-refundable third-party costs; and
- any transition, migration, handover, data export, account transfer, or other exit-related work performed by the Company.

Termination does not affect any rights, obligations, charges, or amounts that accrued before the effective termination date.

The Company may terminate or suspend some or all Services immediately where:

- An undisputed invoice remains materially overdue after the notice-and-cure period in Clause 20, excluding any amounts genuinely disputed in good faith under the Deliverable acceptance provisions, provided the Client has notified the Company of the specific reasons for the dispute in writing within the applicable acceptance period and paid all undisputed amounts when due;
- the Client commits a material breach of the Agreement and, where reasonably capable of remedy, fails to remedy it within 30 days after written notice;
- the Client's activities are unlawful;
- there is a serious and imminent security, operational, legal, or financial risk that cannot reasonably be mitigated without suspension or termination;
- continued performance would expose the Company to material unpaid costs;
- a Third-Party Service prevents continued delivery; or
- **continued performance would be unlawful.**

Where reasonably practicable, the Company will notify the Client before termination or suspension.

Termination does not relieve the Client of its obligation to pay any outstanding amounts, applicable late-payment charges, recovery costs, Third-Party Service Costs, or other charges due under the Agreement.

Either Party may terminate this Agreement or any applicable Proposal, Statement of Work, or Service Order by written notice if the other Party commits a material breach and, where capable of remedy, fails to remedy that breach within 30 days after written notice, or if the other Party becomes insolvent, enters liquidation or administration, ceases business, or is unable to pay its debts as they fall due.

On termination of any Proposal, Statement of Work, or Service Order, the Client will remain responsible for all amounts properly due for Deliverables delivered, work completed, and work in progress up to the effective termination date, together with any committed or non-cancellable costs. Work in progress may be valued reasonably by reference to applicable milestones, percentage of completion, time incurred, or other relevant evidence of work performed.

Any prepaid amounts relating solely to Services not performed and for which the Company has not incurred or committed costs will be credited or refunded following final reconciliation of the account.

Subject to payment of all amounts properly due, the Company will provide the Client with applicable work in progress, source code and other Deliverables created for the Client to the extent required under Clauses 11 and 22.

22. Exit and Transition

Following termination, the Company will provide reasonable cooperation for an orderly transition.

Transition assistance may include available documentation, credentials, configuration information, account transfer assistance, data export, and coordination with a replacement provider.

Any transition, migration, export, transformation, bespoke extraction, handover, or transfer work may be separately scoped and charged at the Company's applicable rates where such work falls outside the agreed scope.

The Company is not required to complete transfer activities while any invoices or other amounts due under the Agreement remain unpaid.

23. Data Retention Following Termination

Following termination, the Company may retain Client data, backups, systems, and related technical information for up to **30 days** where reasonably required for transition, subject to applicable fees, provider limitations, backup schedules, security requirements, and applicable law.

At the Client's written request, the retention period may be extended for up to an additional **60 days**, for a maximum retention period of **90 days**, provided that all applicable hosting, infrastructure, storage, backup, Third-Party Service, and related operational charges for the extended period are **paid in advance**.

After the applicable retention period, the Company may delete, disable, or allow the expiry of Client data, infrastructure, accounts, backups, subscriptions, or related resources unless otherwise agreed in writing or required by law.

Backup copies may remain until removed through the normal backup-retention cycle.

The Client is responsible for ensuring that all required data, credentials, documentation, and system access have been successfully transferred before the applicable retention period expires.

The Company is not responsible for any loss resulting from the Client's failure to complete its transfer, export, or backup activities within the applicable retention period.

24. Warranties and Service Limitations

The Company will provide the Services with commercially reasonable skill and care.

The Client acknowledges that:

- cloud and technology services may experience interruptions;
- uninterrupted or error-free availability cannot be guaranteed;
- backup systems cannot guarantee zero data loss;
- monitoring cannot guarantee detection of every incident;
- security measures cannot guarantee that a system will never be compromised;
- estimates, recommendations, timelines, forecasts, and technical advice are based on information reasonably available at the time and are not guarantees of a particular outcome; and
- Third-Party Services operate outside the Company's direct control.

The Company is not responsible for failures, delays, losses, or security incidents caused by Client actions, third-party actions, unsupported or obsolete systems, unauthorised changes, compromised Client-controlled credentials, or failure to follow reasonable Company recommendations.

Unless otherwise stated in the applicable Proposal or Statement of Work, project-specific Deliverables include a 30-day warranty from delivery or production release for reproducible defects where the Deliverable materially fails to operate in accordance with the agreed requirements.

The warranty does not cover new requirements, enhancements, changes in scope, Client modifications, third-party changes, misuse, unsupported environments, infrastructure issues, or systems outside the Company's reasonable control. Work outside the warranty scope may be charged separately.

The Company's obligation under the warranty is limited to using commercially reasonable efforts to correct the qualifying defect. The warranty does not create any right to a refund, service credit, or other compensation unless expressly agreed in writing.

Where the Services include artificial intelligence, machine learning, automated recommendations, generative AI, or similar technologies, the Client acknowledges that outputs may contain errors, omissions, inaccuracies, bias, or unexpected results.

The Company does not guarantee the accuracy, completeness, reliability, or suitability of AI-generated outputs.

The Client remains responsible for reviewing and validating AI outputs before relying on them for business, legal, financial, regulatory, operational, or other material decisions.

Unless expressly stated in the Agreement, the Company does not guarantee any specific business result, revenue, cost saving, system performance level, regulatory outcome, or commercial result from the Services.

25. Limitation of Liability

To the maximum extent permitted by applicable law, the Company will not be liable for any indirect, incidental, special, or consequential loss, including loss of profit, revenue, business opportunity, anticipated savings, reputation, goodwill, or indirect business interruption. For clarity, this exclusion does not apply to direct loss or corruption of Client data to the extent directly caused by the Company's breach of this Agreement.

Unless otherwise expressly stated in the Agreement, the Company's total aggregate liability arising out of or in connection with the Services will not exceed the fees actually paid to the Company for the specific Services giving rise to the claim during the three months immediately preceding the event giving rise to the claim.

Third-Party Service Costs, taxes, licences, cloud consumption, pass-through expenses, and other amounts paid or payable to third parties are excluded from the calculation of the liability cap.

The Company will not be responsible for losses, delays, interruptions, security incidents, or additional costs resulting from:

- client instructions, actions, omissions, or decisions;
- unauthorised changes made by the Client or a third party;
- application defects or systems not developed or controlled by the Company;
- unsupported, obsolete, or end-of-life technology;
- Third-Party Service failures;
- compromised credentials or accounts controlled by the Client;
- the Client's failure to follow reasonable technical, security, backup, or operational recommendations;
- data, content, or information supplied by the Client or third parties; or
- events outside the Company's reasonable control.

The Client is responsible for maintaining appropriate insurance and business-continuity arrangements appropriate to its business and risk profile.

Where backup or disaster-recovery services are included in the agreed scope, the Company will provide them in accordance with the applicable Proposal or Statement of Work. Backup and recovery are otherwise the Client's responsibility. In all cases the Client remains responsible for determining whether the agreed backup frequency, retention, and recovery objectives are adequate for its business, and for maintaining any additional or independent copies its risk profile requires.

Nothing in this section excludes or limits liability where such exclusion or limitation is prohibited by applicable law.

26. Dispute Resolution

If the Client disputes an invoice, Deliverable, milestone, scope completion, warranty matter, or other obligation under the Agreement, the Client must notify the Company by email and identify the specific invoice, Deliverable, milestone, requirement, or contractual obligation being disputed, together with the reasons for the dispute and supporting information to reproduce the issue.

The parties will use reasonable efforts to resolve the dispute through good-faith discussions.

If the dispute is not resolved, either party may refer it to a senior authorised representative of each party for escalation. The senior representatives will use reasonable efforts to resolve the dispute within 10 Business Days.

If the dispute remains unresolved, the parties may agree to attempt mediation in Dubai before commencing court proceedings. This does not prevent either party from seeking urgent injunctive or other interim relief.

A dispute does not suspend or delay the Client's obligation to pay invoices when due, unless the Company agrees otherwise by email or a court orders otherwise.

If the dispute cannot be resolved, either party may refer the matter to the courts specified in the Legal Compliance and Governing Law section.

27. Legal Compliance and Governing Law

The Client is responsible for ensuring that its systems, data, applications, business activities, and use of the Services comply with all laws, regulations, licensing requirements, and industry requirements applicable to the Client.

The Agreement will be governed by and construed in accordance with the laws of the **Dubai International Financial Centre (DIFC)**.

The Agreement and all notices, claims, proceedings, and dispute-related communications will be conducted in **English**. Where the Agreement is translated into another language, the English version will prevail in the event of any inconsistency.

The parties agree that any dispute arising out of or in connection with the Agreement will be subject to the exclusive jurisdiction of the **DIFC Courts**.

Where a claim is eligible to be heard by the **Small Claims Tribunal of the DIFC Courts**, the parties expressly elect in writing for the Small Claims Tribunal to have jurisdiction over that claim.

28. Notices
Formal notices relating to termination, suspension, material breach, or legal disputes must be given in writing to the contact details stated in the applicable Proposal, Service Order, or other agreed commercial document.

Email will constitute written notice unless otherwise agreed.

A notice will be considered received when successfully delivered to the recipient's designated email address, unless the sender receives a delivery failure notification.

29. Assignment
Either Party may assign or transfer this Agreement to an affiliate, successor, purchaser of substantially all of its business or assets, or as part of a merger, acquisition, reorganisation or corporate restructuring, by giving written notice to the other Party.

Neither Party may assign or transfer this Agreement to a direct competitor of the other Party without the other Party's prior written consent.

If the Company assigns or transfers this Agreement to a direct competitor of the Client, the Client may terminate the affected Services by written notice, and the exit and transition provisions in Clause 22 will apply.

Any other assignment or transfer requires the prior written consent of the other Party, such consent not to be unreasonably withheld or delayed.

30. Severability and No Waiver
If any provision of the Agreement is found to be invalid, illegal, or unenforceable, the remaining provisions will continue in full force and effect.

A failure or delay by either party to exercise or enforce any right under the Agreement does not waive that right or prevent it from being exercised or enforced later.

No waiver will be effective unless made in writing by an authorised representative of the party granting the waiver.

31. Entire Agreement and Order of Priority

The Agreement constitutes the entire agreement between the parties regarding the Services and replaces any previous discussions, proposals, representations, or understandings relating to those Services, unless expressly incorporated into the Agreement.

No verbal representation, informal communication, email, message, or instruction will amend the Agreement unless the amendment is confirmed in writing by authorised representatives of both parties.

Where documents forming part of the Agreement conflict, the following order of priority applies:

- any amendment to this Agreement signed by authorised representatives of both parties;
- this Master Service Agreement;
- the applicable Statement of Work;
- the applicable Proposal or Service Order;
- any other document expressly incorporated into the Agreement; and
- supporting technical documentation.

Notwithstanding the above, the applicable Data Processing Agreement will prevail over the other documents only to the extent of any conflict relating specifically to the Processing of Personal Data. In all other respects, the order

of priority above will apply.

A Statement of Work, Proposal or Service Order will prevail over this Agreement only where it expressly identifies the clause of this Agreement that it varies, states that it is intended to override that clause, and is signed by authorised representatives of both parties. An amendment to a Statement of Work, Proposal or Service Order has the same priority as the document it amends.

Any provisions which by their nature are intended to continue after termination, including payment obligations, confidentiality, intellectual property, non-circumvention, liability, recovery costs, dispute resolution, and accrued rights, will survive termination of the Agreement.

Each party confirms that the person signing below is authorised to enter into this Agreement on its behalf.
The Effective Date is the date of the last signature below.

Schedule 1 – Data Processing Agreement

to the AI Geeks Limited Master Service Agreement

This Data Processing Agreement ("**DPA**") forms part of the Master Service Agreement ("**MSA**") between **AI Geeks Limited** (the "**Company**" or "**Processor**") and the Client (the "**Client**" or "**Controller**").

This DPA applies where the Company Processes Personal Data on behalf of the Client in connection with any Services provided under the Agreement, including **Software Development Services** and **Infrastructure and Hosting Services**.

No separate signature is required where this DPA is incorporated into an executed MSA, Proposal, Statement of Work, Service Order, Infrastructure Schedule or other document forming part of the Agreement.

1. Definitions and Interpretation

For the purposes of this DPA:

- **"Applicable Data Protection Laws"** means all privacy, data protection, cybersecurity and data-transfer laws and regulations applicable to the relevant Processing from time to time.
- **"Client Personal Data"** means Personal Data Processed by the Company on behalf of the Client in connection with the Services.
- **"Software Development Services"** means software development, design, configuration, implementation, integration, testing, debugging, deployment assistance, migration, maintenance, support and related technical Services.
- **"Infrastructure and Hosting Services"** means hosting, cloud infrastructure, managed infrastructure, storage, databases, backup, disaster recovery, monitoring, logging, security administration, access management, production infrastructure, operational support and related Services.
- **"Subprocessor"** means a third party engaged by or on behalf of the Company to Process Client Personal Data in connection with the Services.
- The terms **Controller, Processor, Data Subject, Personal Data, Processing, Personal Data Breach** and **Supervisory Authority** have the meanings given under Applicable Data Protection Laws, using the closest equivalent meaning where terminology differs between jurisdictions.

Capitalised terms not defined in this DPA have the meanings given in the MSA.

2. Scope and Roles

This DPA applies only to Personal Data Processed by the Company on behalf of the Client in connection with the Services.

The Client determines the purposes and means of the Processing and generally acts as Controller.

The Company Processes Client Personal Data on the Client's documented instructions and generally acts as Processor.

Where the nature of particular Processing results in the Parties having different roles under Applicable Data Protection Laws, those roles will be determined in accordance with the applicable law.

This DPA takes effect when the Company begins Processing Client Personal Data and continues for as long as the Company Processes Client Personal Data in connection with the Services.

3. Application to Software Development Services

Where the Company provides Software Development Services, this DPA applies to Personal Data accessed, viewed, received, transmitted, tested, migrated, configured, modified, supported or otherwise Processed in connection with those Services.

Software Development Processing may include:

- development and configuration;
- integration work;
- testing and debugging;
- migration and data conversion;
- deployment assistance;
- application maintenance;
- technical support;
- troubleshooting; and
- other Processing reasonably necessary to provide the Software Development Services.

Where reasonably practicable, the Company may use anonymised, pseudonymised, synthetic or non-production data for development and testing.

Where access to production Personal Data is reasonably necessary, access will be limited to personnel who reasonably require it to provide the Services.

Software Development Services do not by themselves create any hosting, availability, backup, disaster-recovery, monitoring or infrastructure commitment unless expressly included in the applicable Proposal, Statement of Work or Service Order.

4. Application to Infrastructure and Hosting Services

Where the Company provides Infrastructure and Hosting Services, this DPA applies to Personal Data Processed in connection with:

- cloud hosting;
- application and database infrastructure;
- storage;
- backups;
- disaster recovery;
- monitoring and logging;
- security administration;
- vulnerability management;
- access management;
- production infrastructure;
- system restoration;
- incident response;
- technical support; and
- related operational services.

The specific infrastructure architecture, backup frequency, retention, restore testing, disaster-recovery arrangements, monitoring, service levels, resilience, data residency and security commitments will be governed by the applicable **Infrastructure Schedule, Proposal, Statement of Work or Service Order**.

Nothing in this DPA creates or expands any infrastructure, availability, backup, recovery, monitoring, security or service-level commitment beyond the Services expressly purchased by the Client.

5. Client Responsibilities

The Client remains responsible for determining and complying with its privacy and data-protection obligations, including:

- lawful basis for Processing;
- consents where required;
- privacy notices;
- Data Subject rights;
- retention requirements;

- regulatory requirements;
- data-residency requirements; and
- determining whether the Services are appropriate for the nature and sensitivity of the Personal Data being Processed.

The Client will ensure that it has the right to provide Client Personal Data to the Company and that its instructions comply with Applicable Data Protection Laws.

The Client will not instruct the Company to Process Personal Data in a manner that would knowingly cause the Company to breach Applicable Data Protection Laws.

6. Processing Instructions

The Company will Process Client Personal Data only:

- on documented instructions from the Client;
- as reasonably necessary to provide the Services;
- as authorised by the Agreement; or
- where required by Applicable Data Protection Laws.

The Agreement, applicable Proposal, Statement of Work, Infrastructure Schedule, Service Order and authorised Client communications constitute documented instructions for the purposes of this DPA.

If the Company reasonably believes that an instruction infringes Applicable Data Protection Laws, the Company may notify the Client and suspend the affected Processing until the instruction is clarified, amended or lawfully confirmed.

The Company will not sell Client Personal Data or use Client Personal Data for unrelated commercial purposes.

7. Personnel and Confidentiality

Access to Client Personal Data will be limited to personnel who reasonably require access to provide the Services.

Personnel authorised to Process Client Personal Data will be subject to appropriate confidentiality obligations.

The Company may use employees, contractors, consultants and other authorised personnel to provide the Services.

Such personnel may work from jurisdictions in which the Company operates or engages personnel, subject to the international-transfer requirements of this DPA and Applicable Data Protection Laws.

The Company will maintain appropriate data-protection and security awareness measures for personnel with access to Client Personal Data.

8. Security Measures

The Company will maintain appropriate technical and organisational measures having regard to:

- the nature, scope, context and purpose of the Processing;
- the nature and sensitivity of the Personal Data;
- reasonably foreseeable risks to Data Subjects;
- the Services being provided;
- the state of the art; and
- the cost of implementation.

Measures may include, where appropriate to the Services:

- role-based and least-privilege access;
- authentication and credential controls;
- secure development practices;
- restrictions on production-data access;
- encryption in transit and at rest;
- cloud security controls;
- logging and monitoring;
- vulnerability-management processes;
- backup and recovery controls;
- device-security controls;
- access reviews; and
- incident-response procedures.

Service-specific technical measures are governed by the applicable Proposal, Statement of Work, Infrastructure Schedule or Service Order.

Client-specific controls, certifications, dedicated environments, enhanced logging, bespoke encryption requirements, penetration testing or additional security obligations beyond the Company's standard Services must be expressly agreed in writing and may result in additional charges.

9. Subprocessors and Third-Party Services

The Client gives the Company general written authorisation to use Subprocessors and Third-Party Services reasonably required to provide the Services.

The Company will require Subprocessors that Process Client Personal Data to be subject to appropriate confidentiality, security and data-protection obligations.

The Company remains responsible for the Processing performed by its Subprocessors to the extent required by Applicable Data Protection Laws.

The Company may change or replace Subprocessors in the ordinary course of providing the Services.

Where Applicable Data Protection Laws require notice of a material new or replacement Subprocessor, the Company will provide reasonable prior notice and the Client may object on reasonable and documented data-protection grounds.

The Company will maintain information identifying its material Subprocessors and their primary Processing locations, which may be provided through the applicable Proposal, Statement of Work, Infrastructure Schedule, Service Order, or a Subprocessor list maintained by the Company.

Any Client-specific approval process, fixed notice period, geographic restriction, provider restriction, or data-residency requirement must be expressly agreed in the applicable Proposal, Statement of Work, Infrastructure Schedule or Service Order and may result in additional charges.

10. International Access and Transfers

The Client acknowledges that provision of the Services may involve authorised personnel or Subprocessors accessing Client Personal Data from jurisdictions outside the Client's jurisdiction.

International transfers will be made only where permitted by Applicable Data Protection Laws.

Where required, the Parties will reasonably cooperate to implement an appropriate transfer mechanism, including an adequacy decision, Standard Contractual Clauses, recognised transfer addendum, binding corporate rules, or another legally recognised transfer mechanism.

The primary hosting or Processing location for Infrastructure and Hosting Services will be as specified in the applicable Proposal, Statement of Work, Infrastructure Schedule or Service Order.

Any Client-specific requirement that Client Personal Data be hosted, stored or Processed only within a particular country or region, or that it not be moved outside that location without prior consent, must be expressly agreed in writing.

The Company will not use Client Personal Data to train third-party artificial intelligence or machine-learning models without the Client's prior written authorisation.

Where AI or machine-learning services are included in the Services, the Company may transmit Client Personal Data to approved Third-Party Services only where reasonably necessary to provide the agreed functionality and subject to this DPA, Applicable Data Protection Laws, and any applicable contractual safeguards.

11. Data Subject Requests

Taking into account the nature of the Processing, the Company will provide reasonable assistance to the Client with Data Subject requests where required by Applicable Data Protection Laws and reasonably possible using information and functionality available to the Company.

If a Data Subject contacts the Company directly regarding Client Personal Data, the Company will normally refer the request to the Client unless legally required to respond directly.

The Client remains responsible for determining how to respond to Data Subject requests.

Material development, extraction, investigation, reporting or other work outside the agreed Services may be separately scoped and charged.

12. Personal Data Breaches

The Company will notify the Client **without undue delay** after becoming aware of a confirmed Personal Data Breach affecting Client Personal Data, and within any shorter period required by Applicable Data Protection Laws or expressly agreed in writing.

The Company will provide information reasonably available to it concerning:

- the nature of the breach;
- affected Personal Data;
- affected Data Subjects;
- likely consequences, where reasonably known; and
- measures taken or proposed to investigate, contain or remediate the breach.

The Company will provide reasonable cooperation with investigation, containment and remediation.

Specialist services such as:

- forensic investigation;
- regulatory reporting;
- penetration testing;
- specialist incident-response consultants;
- extensive data reconstruction;
- legal advice; or
- substantial application-code remediation

are outside the standard Services unless expressly included, and may be separately charged except to the extent otherwise required by Applicable Data Protection Laws or directly resulting from the Company's breach of this DPA.

The Company will not notify Data Subjects or a Supervisory Authority on the Client's behalf unless authorised by the Client or required by law.

13. DPIAs and Regulatory Assistance

Taking into account the nature of the Processing and the information available to it, the Company will provide reasonable assistance with:

- data-protection impact assessments;
- consultations with Supervisory Authorities; and
- other regulatory obligations

where required by Applicable Data Protection Laws.

Material work outside the agreed Services may be separately scoped and charged.

14. Compliance Information and Audits

The Company will make available reasonable information necessary to demonstrate compliance with this DPA and Applicable Data Protection Laws.

Where an audit or inspection is reasonably required by Applicable Data Protection Laws, it must, where legally permitted:

- be conducted on reasonable prior written notice;
- take place during normal Business Hours;
- be proportionate to the relevant Processing;
- avoid unreasonable disruption;
- protect the confidentiality and security of other clients;
- not require disclosure of information that would create a security risk; and
- where reasonably practicable, rely first on available documentation, reports, certifications and compliance information.

The Client will bear its own audit costs.

The Company may charge its reasonable costs for material assistance, personnel time, preparation, third-party support or bespoke compliance work unless prohibited by Applicable Data Protection Laws or where the audit identifies a material breach of this DPA by the Company.

Auditors must be subject to appropriate confidentiality obligations and must not be a direct competitor of the Company unless required by a Supervisory Authority or Applicable Data Protection Laws.

15. Return, Deletion and Retention

Return, deletion, retention and transition of Client Personal Data are governed by:

- the MSA;
- the applicable Proposal, Statement of Work or Infrastructure Schedule;
- this DPA; and
- Applicable Data Protection Laws.

At the end of the relevant Services, the Company will return or delete Client Personal Data in its possession or control where required by Applicable Data Protection Laws, subject to:

- legal retention obligations;
- provider limitations;

- operational requirements;
- security requirements; and
- normal backup-retention cycles.

The standard post-termination retention period under the MSA is **up to 30 days**.

At the Client's written request, retention may be extended for up to an additional **60 days**, for a maximum of **90 days**, provided that applicable hosting, infrastructure, storage, backup, Third-Party Service and related operational charges for the extended period are paid in advance.

Residual backup copies may remain until removed through the normal backup-retention cycle.

Additional export, migration, bespoke deletion, extended retention or transition assistance may be separately scoped and charged.

16. Sensitive and Special Category Data

The Client will not intentionally provide or instruct the Company to Process Special Category Data, sensitive Personal Data, criminal-offence data or equivalent protected data unless:

- such Processing is reasonably necessary for the Services;
- the Processing is expressly agreed in writing; and
- the Client has established an appropriate lawful basis and any required safeguards.

Where such data is expressly included in the Services, the Parties may agree additional technical, organisational or contractual controls.

17. Additional Client Requirements

This DPA reflects the Company's standard data-processing obligations.

Any additional Client-specific requirements, including:

- dedicated environments;
- specific data-residency commitments;
- enhanced audit rights;
- custom security controls;
- specialised monitoring;
- penetration testing;
- extended retention;
- bespoke reporting;
- additional certifications;
- additional regulatory requirements; or
- enhanced incident-response commitments

must be expressly agreed in the applicable Proposal, Statement of Work, Infrastructure Schedule or Service Order and may result in additional charges.

18. Liability

All liability arising out of or in connection with this DPA is subject to the exclusions, limitations and aggregate liability cap contained in the MSA, except to the extent such limitation is prohibited by Applicable Data Protection Laws.

Nothing in this DPA creates a separate or additional liability cap unless expressly agreed in writing.

19. Relationship with the MSA

This DPA governs matters relating specifically to the Processing of Client Personal Data.

Except where required by Applicable Data Protection Laws or expressly stated in this DPA, the MSA continues to govern all general and commercial matters, including:

- payment;
- confidentiality;
- intellectual property;
- warranties;
- acceptance;
- service levels;
- limitation of liability;
- notices;
- termination;
- dispute resolution;
- governing law; and
- jurisdiction.

If there is a conflict between this DPA and the MSA concerning the Processing of Client Personal Data, this DPA will prevail **only to the extent of that conflict and only in relation to that Processing**.

Where there is a conflict relating specifically to operational matters such as backup frequency, restore testing, disaster recovery, monitoring, availability or infrastructure architecture, the applicable **Infrastructure Schedule, Proposal or Statement of Work** will govern the relevant service commitment, subject to Applicable Data Protection Laws.

No separate signature is required where this DPA forms part of the executed MSA.

Annex 1 – Details of Processing

A. Subject Matter

Processing of Client Personal Data in connection with Software Development Services and, where contracted, Infrastructure and Hosting Services.

B. Duration

For the duration of the applicable Services and thereafter for as long as the Company lawfully retains Client Personal Data under the Agreement and Applicable Data Protection Laws.

C. Nature and Purpose – Software Development

Processing may include:

- access;
- review;
- development;
- configuration;
- testing;
- debugging;
- transmission;
- integration;

- migration;
- deployment;
- maintenance;
- troubleshooting;
- technical support; and
- other Processing reasonably necessary to provide the Software Development Services.

D. Nature and Purpose – Infrastructure and Hosting

Processing may include:

- hosting;
- storage;
- database operation;
- transmission;
- backup;
- restoration;
- monitoring;
- logging;
- security administration;
- access management;
- vulnerability management;
- incident response;
- production support; and
- other infrastructure operations reasonably necessary to operate, support and protect the relevant systems.

E. Categories of Data Subjects

Depending on the applicable Services, Data Subjects may include:

- Client employees;
- contractors;
- consultants;
- customers;
- users;
- suppliers;
- students;
- parents or guardians;
- administrators; and
- other individuals whose Personal Data is provided to or accessible by the Company in connection with the Services.

F. Categories of Personal Data

Depending on the Services, Personal Data may include:

- names;
- contact details;
- email addresses;
- telephone numbers;
- account information;
- authentication information;
- employment information;
- user-generated content;
- application data;
- transaction or operational data;

- logs and technical identifiers; and
- other Personal Data contained in systems made available to the Company.

G. Sensitive or Special Category Data

Only where expressly required for the Services, lawfully provided by the Client and subject to appropriate safeguards.

Annex 2 – Technical and Organisational Measures

The Company will maintain technical and organisational measures appropriate to the Services and the risk.

Access Control

- Role-based and least-privilege access.
- Access limited to personnel reasonably requiring it.
- Appropriate authentication controls.
- Periodic review of privileged access where appropriate.
- Administrative and privileged access to production systems will be logged where supported by the applicable systems and infrastructure.

Credential Security

- Appropriate credential-management practices.
- Administrative credentials restricted to authorised personnel.
- Secrets and production credentials stored using appropriate secure mechanisms.

Encryption

- Encryption in transit using appropriate industry-standard protocols.
- Encryption at rest where appropriate to the relevant service architecture.

Payment Card Data

- Full payment card numbers, CVV/CVC data, PIN data, and other sensitive authentication data will not be intentionally stored or processed on Company-controlled systems.
- Payment card transactions will, where reasonably practicable, be handled through approved third-party payment service providers using hosted payment pages, tokenisation, payment APIs, or equivalent secure mechanisms.
- Non-sensitive payment-related information, including transaction references, payment status, masked card details, billing information, and tokens, may be processed where reasonably necessary to provide the Services.

Software Development Security

- Secure development practices appropriate to the Services.
- Production-data access restricted where reasonably practicable.
- Use of non-production, anonymised, pseudonymised or synthetic data where reasonably practicable.
- Appropriate source-control and access controls.

Infrastructure Security

Where Infrastructure and Hosting Services are provided:

- cloud-security guardrails appropriate to the agreed architecture;
- access controls for infrastructure administration;
- controls intended to prevent unintended public exposure;
- monitoring and logging where included in the Services;
- vulnerability-management measures appropriate to the contracted service tier; and
- backup and recovery controls as specified in the Infrastructure Schedule.

Organisational Measures

- Confidentiality obligations.
- Appropriate security policies.
- Device-security measures.
- Data-protection and security awareness for personnel with access to Client Personal Data.

Business Continuity

Backup frequency, retention, restore testing, disaster-recovery exercises, recovery objectives and resiliency commitments are determined by the applicable Infrastructure Schedule, Proposal or Statement of Work.

Annex 3 – Subprocessors and Processing Locations

The Client gives general authorisation for the Company to use Subprocessors reasonably required to provide the Services.

The Company will maintain information identifying material Subprocessors, their purpose, and their primary Processing locations. This information may be set out in the applicable Proposal, Statement of Work, Infrastructure Schedule, Service Order, or a Subprocessor list maintained by the Company.

Any Client-specific hosting-region, data-residency, provider, approval, or advance-notice requirement must be expressly agreed in writing.

Typical categories may include:

Category	**Purpose**
Cloud infrastructure providers	Hosting, storage, databases, backup and related cloud services
Email and messaging providers	Transactional communications and notifications
Monitoring/security providers	Logging, monitoring, vulnerability and security services
Development platforms	Source control, deployment and development tooling
AI/API providers	AI-enabled functionality where included in the Services
Authorised Company personnel and contractors	Development, support, infrastructure and technical Services

The Company may use authorised personnel and contractors located in jurisdictions including the **United Arab Emirates, Nepal, India, Egypt and other locations reasonably required to provide the Services**, subject to Applicable Data Protection Laws and the international-transfer provisions of this DPA.

Annex 4 – Applicable Data Protection Frameworks

“Applicable Data Protection Laws” may include, where applicable to the relevant Client, Processing, Data Subjects or international transfer:

Jurisdiction / Region	**Framework**
European Union / EEA	GDPR and applicable national data-protection legislation
United Kingdom	UK GDPR, Data Protection Act 2018 and other applicable UK data-protection legislation
United Arab Emirates	UAE Federal Personal Data Protection Law and implementing requirements
DIFC	DIFC Data Protection Law and applicable regulations
Saudi Arabia	Saudi Personal Data Protection Law and applicable implementing and transfer requirements
Other jurisdictions	Any other applicable privacy, data-protection, cybersecurity or data-transfer law