WiBiz Client Terms

One document for the terms of every WiBiz engagement: a one-page summary, then the Master Services Agreement and its schedules. Your Order Form states your services, fees and dates.

Version: v1.0

Date: 1 November 2026

Author: WiBiz (wibiz.ai)

Owner: Nick (Nicklaus D'Cruz, founder and CEO)

Provider: Digital Benefits Pte. Ltd. trading as WiBiz, UEN 201735371H, 60 Paya Lebar Road, #06-28, Paya Lebar Square, Singapore 409051

Currency: USD only

Your terms on one page

This page is a plain-English summary. The numbered terms that follow govern, and your Order Form states your services, fees and dates.

What you get. The services, scope and acceptance criteria in your Order Form. WiBiz builds them, tests them, and declares Signal Launch in writing when its own delivery work is complete. From the Signal Launch date you have 10 business days to report any defect against the agreed scope; a confirmed defect is fixed at no charge. Services carry a 90-day warranty from delivery. If WiBiz misses its build clock for a reason within its control, you may choose a pro-rated refund of the undelivered implementation work or end the Order Form without further charge.

What you pay. The fees in USD stated in your Order Form. The implementation fee is paid before the build starts. Your subscription starts on the Signal Launch date. Invoices are due 14 days from the invoice date, and fees exclude applicable taxes. A Change Order confirms scope, fee and timing before any new work starts.

How to cancel. Unless your Order Form says otherwise, it runs for 12 months and renews for 12 months unless either party gives 30 days' written notice before the term ends. Either party may end it for a material breach not fixed within 30 days of notice (14 days for a payment breach). If your account is recorded as dormant, you may end the Order Form by written notice with no further subscription charges. Your data is available for export for 30 days after termination.

How we protect your data. You keep ownership of your data. WiBiz processes personal data only on your documented instructions, under Schedule 2 and the security measures in Schedule 3. WiBiz aims to notify you within 72 hours of becoming aware of a confirmed data breach, gives 30 days' notice before adding or replacing a subprocessor, and deletes your data after the export period. Singapore law governs these terms.

Public policies. These apply by link and are not part of what you sign: the WiBiz Privacy Policy, which also covers cookies (https://start.wibiz.ai/privacy-policy/), the Website Terms and Conditions (https://start.wibiz.ai/terms-and-conditions/), and the WiBiz Trust Center (https://trust.wibiz.ai/).

How these terms fit together

Part	What it covers
Part A: Master Services Agreement	The main contract: orders, Signal Launch and acceptance, fees, data, confidentiality, IP, warranties, liability, term and termination

Schedule 1: Service Levels	Availability, maintenance, support and response targets, service credits where stated
Schedule 2: Data Processing	How WiBiz processes personal data for you, subprocessors, breaches, return and deletion
Schedule 3: Information Security	The security controls WiBiz maintains
Schedule 4: Acceptable Use	What the services may and may not be used for
Schedule 5: Refunds and Cancellation	Refunds, exclusions and chargebacks
Annex: International Transfers	Applies only where personal data is transferred across borders in a way that requires an approved transfer mechanism, such as EEA, UK or Swiss Standard Contractual Clauses

Numbering: Part A clauses are A.1 to A.23; Schedule clauses carry the schedule number (for example 2.8 is Schedule 2, clause 8); Annex clauses are T.1 to T.13. Where a clause is not used it is omitted, so some numbers are skipped.

Part A: Master Services Agreement

This Part A is the Master Services Agreement between the legal entity identified as the provider in the Order Form ("WiBiz") and the customer identified in that Order Form ("Customer"). It begins on the date stated in the first executed Order Form. The provider is Digital Benefits Pte. Ltd. trading as WiBiz, UEN 201735371H, 60 Paya Lebar Road, #06-28, Paya Lebar Square, Singapore 409051. Governing law: the laws of Singapore, without regard to conflict-of-laws principles.

A.1 Contract documents and priority

The agreement consists of the executed Order Form (including its Statement of Work), signed electronically or accepted by one-click acceptance, and these WiBiz Client Terms: Part A (this Master Services Agreement), Schedule 1 (Service Levels), Schedule 2 (Data Processing), Schedule 3 (Information Security), Schedule 4 (Acceptable Use), Schedule 5 (Refunds and Cancellation), the International Transfers Annex where it applies, and any other signed schedule.

Unless an executed document expressly states otherwise, conflicts are resolved in this order:

1. mandatory law and applicable approved international transfer clauses;
2. Schedule 2 for personal-data matters;
3. Order Form for customer, service, fees, quantity, and term;
4. Statement of Work for implementation, dependencies, deliverables, and acceptance;
5. Schedule 3 (Information Security) and Schedule 1 (Service Levels) for their subject matter;
6. Part A;
7. Schedule 4 (Acceptable Use) and Schedule 5 (Refunds and Cancellation).

Marketing, demonstrations, proposals, questionnaires, Trust Center content, and email do not amend the agreement unless expressly incorporated into an executed document.

A.2 Services and orders

WiBiz will provide the services and deliverables described in an executed Order Form or Statement of Work. No commitment is binding until authorised representatives execute the relevant document. Affiliates may order only if the Order Form identifies them and allocates responsibility.

A.3 Commencement, implementation, Signal Launch, and acceptance

Implementation milestones, dependencies, delivery criteria, acceptance tests, review periods, and launch contacts must be stated in the Statement of Work.

Signal Launch declaration. WiBiz declares Signal Launch by issuing a written Signal Launch Notice, with its Delivery Certificate, once WiBiz's own delivery obligations for the release are complete: quality assurance passed, the launch security gate passed, internal approval recorded where the service tier requires it, and delivery reported to Customer. WiBiz must not declare Signal Launch while a WiBiz-owned launch blocker remains open, and must not describe an item blocked by Customer as delivered.

Effective date. Signal Launch is effective on the date of the Signal Launch Notice (the "Signal Launch Date"). The Signal Launch Date is recorded once and does not change.

Subscription commencement. Unless the Order Form expressly states otherwise, the subscription commences on the Signal Launch Date and, for an annual plan, the twelve-month term starts on that date. Any final implementation-fee milestone falls due on the Signal Launch Date.

Review period and deemed acceptance. Deemed acceptance is permitted, with a 10-business-day review period from WiBiz's written delivery notice, which is the Signal Launch Notice. A defect against the agreed scope reported in writing within that period, with reasonable detail, prevents deemed acceptance of the affected deliverable until resolved. It does not change the Signal Launch Date, subscription commencement, or billing, and WiBiz corrects a confirmed defect at no additional charge. At the end of the review period, the delivered scope that is not subject to an open valid defect notice is deemed accepted with effect from the Signal Launch Date, and a deliverable held by a valid defect notice is accepted, with the same effect, when WiBiz delivers the correction. A latent defect or a security defect discovered after the review period is not barred by deemed acceptance and is handled under the delivery-guarantee remedy in clause A.6.

Matters that do not delay Signal Launch. None of the following delays, suspends, or reverses Signal Launch, subscription commencement, or billing: silence; the absence of a signature; questions, comments, or acknowledgements; a request for new or changed functionality, which is handled as a Change Order under clause A.5; or an action that only Customer can take, such as connecting Customer's own messaging number, granting access to Customer's payment-provider account, or supplying a third-party credential. WiBiz will list each outstanding Customer action in the Signal Launch Record with its owner, due date, and operational effect, and clause A.4 applies to it.

Acknowledgement. Customer's signature on a Signal Launch Record acknowledges receipt. It is not a condition of Signal Launch, acceptance, subscription commencement, or payment, and WiBiz will not record a signature that was not given.

Customer rights preserved. Nothing in this clause limits Customer's warranty rights under clause A.13, any delivery guarantee, refund, or exit right stated in the Order Form or Statement of Work, or any right that cannot lawfully be excluded.

Minor defects that do not materially impair agreed use may be recorded for correction without preventing acceptance only if the Statement of Work expressly says so.

A.4 Customer responsibilities

Customer will provide timely access, content, decisions, approvals, credentials, lawful instructions, technical contacts, and other dependencies stated in the Statement of Work. Customer is responsible for the accuracy, legality, and rights associated with Customer Data and for its users' compliance with the agreement.

WiBiz will notify Customer when a dependency is missing and describe the likely effect. Schedule, fees during delay, suspension, dormancy, reactivation, and termination consequences apply only as expressly stated in the Order Form or Statement of Work.

A.5 Change control

Either party may request a change. WiBiz will assess the effect on scope, timing, fees, security, data protection, and dependencies. A change is effective only when authorised representatives approve a written Change Order, except an emergency security measure reasonably necessary to protect the services or data.

A.6 Fees, invoicing, and taxes

Fees, currency, billing milestones, subscription commencement (which defaults to the Signal Launch Date under clause A.3), usage measurement, invoice dates, payment due dates, deposits, expenses, taxes, and renewal pricing must be stated in the Order Form. WiBiz commercial documents use USD only.

Delivery guarantee. WiBiz gives two delivery commitments, which clauses A.3 and A.13 refer to together as the delivery-guarantee remedy:

(a) Build clock. If WiBiz exceeds the WiBiz build clock stated in the Order Form for a reason within WiBiz's control, Customer may elect either a pro-rated refund of the undelivered portion of the implementation fee or termination of the Order Form without further charge. A delay caused by a Customer hold, an unresolved Customer dependency, or a Customer-requested change does not trigger this guarantee. WiBiz's record of when a Customer-caused delay paused the build clock is the evidence for whether it applies. WiBiz honours this guarantee as a standing term once its condition is met.

(b) Uncured defect. WiBiz's primary remedy for a confirmed delivery failure is re-performance within a reasonable time. Where re-performance is not achieved within 30 days of Customer's written notice of a material, reproducible defect, including a warranty non-conformance under clause A.13 or a latent or security defect under clause A.3, Customer's remedy is a pro-rata refund of fees paid for the specific non-conforming deliverable, as Customer's sole and exclusive remedy for that defect, without limiting rights that cannot lawfully be excluded.

Invoices are due 14 days from the invoice date. WiBiz may charge interest on overdue amounts at 1.5% per month or the maximum permitted by law, whichever is lower, and may suspend non-essential services for accounts more than 30 days overdue after written notice. Fees are exclusive of applicable taxes, which Customer bears except taxes on WiBiz's net income. WiBiz may adjust fees for a renewal term on 60 days' written notice before the renewal date. Fees continue during a customer-caused hold under clause A.17.

Customer must notify WiBiz of a good-faith invoice dispute within the approved period and pay undisputed amounts. WiBiz must provide reasonable supporting detail.

A.7 Customer Data and privacy roles

As between the parties, Customer retains rights in data, content, and materials supplied by or for Customer ("Customer Data"). Customer instructs WiBiz to process Customer Data only to provide and secure the services, comply with law, and perform the agreement.

For personal data processed on Customer's behalf, Customer is normally controller or organisation and WiBiz is processor or data intermediary, as detailed in Schedule 2. WiBiz may act as an independent controller for business contact, billing, contract, security-contact, and account-administration data where it independently determines purposes and means.

A.8 Security

WiBiz will maintain the approved measures in Schedule 3 (Information Security). The schedule must contain only controls supported by current evidence and must identify any shared customer responsibilities.

Security certifications, audit reports, testing frequency, data residency, recovery targets, and incident-notification times are commitments only if expressly stated in a signed schedule. Policy objectives or public summaries are not warranties of universal implementation.

A.9 Confidentiality

"Confidential Information" means non-public information disclosed in connection with the agreement that is marked confidential or should reasonably be understood as confidential, including Customer Data, security information, pricing, business plans, and technical information.

The recipient will use Confidential Information only to perform or receive the services, protect it with at least reasonable care, and disclose it only to personnel, advisers, and approved subcontractors who need it and are bound by confidentiality obligations. These duties do not apply to information the recipient can show was lawfully known without restriction, becomes public without breach, is received lawfully from another source, or is independently developed.

If disclosure is legally required, the recipient will give advance notice where lawful and disclose only what is required. Confidentiality obligations survive for 3 years after termination, except trade secrets, which remain protected for as long as they qualify as trade secrets under applicable law, and personal data, which is governed by Schedule 2's own retention and deletion terms.

A.10 Intellectual property

Each party retains its pre-existing materials, technology, methods, data, branding, and intellectual property. WiBiz retains its platform, reusable components, configurations, methods, documentation, tools, and improvements. Customer retains Customer Data and Customer Materials.

For bespoke deliverables built specifically for Customer, on payment in full for the applicable deliverable, WiBiz grants Customer a perpetual, non-exclusive, worldwide licence to use it for Customer's own internal business purposes. This is a licence, not an assignment: WiBiz may reuse the underlying methods, patterns, and non-Customer-identifying components in other engagements. Third-party components and open-source software are governed by their own licence terms, disclosed on reasonable request. Domains, accounts, and credentials follow the ownership model selected on the Order Form. Customer may export Customer Data under Schedule 2's return-and-deletion terms. The bespoke-deliverable licence survives termination; WiBiz-hosted service access ends per clause A.17 and Schedule 2.

No customer name, logo, testimonial, case study, or project disclosure may be used without prior written approval.

A.11 Third-party services and subprocessors

The services may depend on approved third-party services. Applicable providers, functions, and locations must be stated in Schedule 2 schedules or service documentation. WiBiz remains responsible for subcontracted performance to the extent required by the agreement and law.

Customer-directed third-party services are governed by their provider terms. The agreement must identify responsibility for accounts, fees, configuration, availability, data export, and termination.

A.12 Acceptable use and compliance

Customer and its users must comply with the Schedule 4 (Acceptable Use) and applicable law. Each party is responsible for licences, permissions, notices, and consents allocated to it. WiBiz may suspend affected use only as provided in Schedule 4, Schedule 2, or Part A and must minimise scope and duration where reasonably practicable.

A.13 Warranties

Each party warrants that it has authority to enter the agreement. WiBiz warrants that it will perform professional services with reasonable skill and care and that the services will materially conform to the signed specifications during the 90-day warranty period beginning on delivery of the applicable deliverable.

WiBiz's sole remedy obligation is re-performance of the non-conforming element at no additional charge; if not cured within 30 days of Customer's written notice, the delivery-guarantee remedy in clause A.6 applies instead. Excluded: non-conformance caused by unauthorised modification, misuse, third-party integrations not provided by WiBiz, or Customer-

supplied content or instructions. WiBiz warrants it will use commercially reasonable efforts, consistent with Schedule 3 (Information Security), to prevent introduction of malware through WiBiz-controlled code; this is not a warranty against malware from any source. Each party is responsible for its own compliance with law applicable to its own business; WiBiz does not warrant compliance with laws specific to Customer's industry or jurisdiction beyond what is expressly scoped in the Statement of Work.

Nothing excludes a warranty or guarantee that cannot lawfully be excluded.

A.14 Indemnities

WiBiz indemnifies Customer against a third-party claim that a WiBiz-owned deliverable, as delivered and used as intended, infringes that third party's intellectual property rights, and against a third-party claim arising from WiBiz's confirmed failure to implement the security measures expressly agreed in a signed Schedule 3 (Information Security), resulting in unauthorised access to Customer Data. Excluded: claims arising from Customer's own instructions, Customer-supplied materials, unauthorised modification, or combination with something not provided by WiBiz.

Customer indemnifies WiBiz against a third-party claim arising from Customer Data, Customer's instructions, or Customer's or its authorised users' unlawful or unauthorised use of the services, including a claim that Customer Data or Customer's use violates a third party's rights or applicable law.

For both indemnities: the indemnified party must give prompt written notice, the indemnifying party controls the defence and any settlement, which may not admit fault by the indemnified party without its consent, and the indemnified party will reasonably cooperate at the indemnifying party's expense. These indemnities are governed by the increased cap in clause A.15, not the general cap.

A.15 Limitation of liability

Except as stated below, each party's total aggregate liability arising out of or relating to the agreement is capped at the total fees paid or payable by Customer in the 12 months immediately preceding the event giving rise to the claim. For the intellectual-property and confirmed-security-breach indemnities in clause A.14, the cap is instead two times that 12-month fee figure.

Excluded loss categories, both directions, to the extent permitted by law: indirect, consequential, special, or punitive damages, and loss of profits, revenue, goodwill, or anticipated savings.

Carve-outs from any cap or exclusion, both directions: fraud, wilful misconduct, death or personal injury caused by negligence, breach of confidentiality obligations, and any liability that cannot lawfully be excluded or limited.

Service credits under a Schedule 1 (Service Levels), where they exist, are Customer's exclusive remedy for the specific availability shortfall they address, without limiting other liability for a separate cause.

A.16 Insurance

WiBiz will maintain commercially reasonable insurance appropriate to its business, including public liability and, once obtained, technology errors and omissions and cyber liability cover, and will provide evidence of cover on reasonable request. Specific policy types, limits, and insurer standards require an actual insurance certificate from Finance and are the one item under this clause not yet resolved.

Insurance does not limit a party's liability unless the agreement expressly says so.

A.17 Term, renewal, and termination

Part A continues while an Order Form remains active. Absent a stated term, an Order Form runs for twelve months from the effective date, renewing for successive twelve-month periods unless either party gives 30 days' written notice of non-renewal before the then-current term ends.

Either party may terminate for the other's material breach that remains uncured 30 days after written notice, except a payment breach, which may be cured within 14 days of notice before termination rights arise. Either party may terminate

immediately, without a cure period, for the other party's insolvency, cessation of business, or equivalent event, or for unlawful use materially affecting the terminating party; WiBiz may terminate immediately where Customer's non-payment continues 30 days past the cure period above. Either party may terminate an affected Order Form if a force-majeure event under clause A.20 continues for 60 consecutive days.

Termination for convenience is not available by default, consistent with WiBiz's upfront-payment commercial model. A negotiated early-termination right may be added per Order Form, carrying an early-termination charge equal to the fees for the remaining committed term unless the Order Form states otherwise. If Customer stops using a subscribed service without terminating, WiBiz will notify Customer in writing; after 60 days without response, WiBiz may treat the account as dormant, suspend non-essential processing, and continue billing until the Order Form is terminated under this clause or under the dormancy exit right in the Order Form.

On termination, each party will pay accrued amounts and perform the approved transition, export, return, deletion, and cooperation obligations. Provisions concerning confidentiality, ownership, payment, liability, dispute resolution, and data handling survive as appropriate.

A.18 Data return, deletion, and transition

The Order Form and Schedule 2 must state export format, availability period, assistance fees, retention exceptions, backup treatment, deletion evidence, and the party responsible for transition. No deletion period is promised unless operationally verified.

A.19 Records, assurance, and audit

WiBiz will provide the assurance information stated in Schedule 2 or Schedule 3 (Information Security), within applicable confidentiality and security restrictions. Audit rights must avoid exposing another customer's data, creating security risk, or unreasonably disrupting operations.

WiBiz will provide current independent reports, certifications, and completed questionnaires where sufficient. A further audit requires 30 days' written notice, a defined scope, a confidentiality undertaking from the auditor, and is limited to once per 12 months absent a substantiated security incident; Customer bears its own audit costs, and WiBiz bears the reasonable cost of its own personnel's time.

A.20 Force majeure

Neither party is liable for delay caused by events beyond its reasonable control, excluding payment obligations for services already provided. Qualifying events include natural disaster, war, civil unrest, government action, utility or internet infrastructure failure, and pandemic, but not a party's own financial difficulty or ordinary staffing shortfall. The affected party must notify the other, mitigate impact, and resume performance as soon as reasonably practicable. Either party may terminate the affected Order Form under clause A.17 if the event continues 60 consecutive days.

A.21 Governing law and disputes

This agreement is governed by the laws of Singapore, without regard to conflict-of-laws principles. The courts of Singapore have exclusive jurisdiction, except that either party may seek interim or emergency injunctive relief in any court of competent jurisdiction to protect its intellectual property or confidential information. For an enterprise counterparty that requests arbitration in place of litigation, WiBiz may agree to Singapore International Arbitration Centre arbitration, seated in Singapore, conducted in English, under the SIAC Rules then in force, as a negotiated variation recorded in the Order Form. Where a specific engagement is found to trigger a foreign jurisdiction's mandatory local protections, that regime's own specialist counsel review applies in addition to this clause.

Before formal proceedings, authorised commercial representatives should attempt good-faith resolution for 15 business days from written notice of a dispute, except where urgent relief is required.

A.22 Notices

Contract notices must be sent to the addresses in the Order Form. Email to the contract contact stated in the Order Form is effective when sent, unless the sender receives an automated failure notice, in which case notice must be given by another method in this clause; deemed received the next business day in Singapore. Legal notices to WiBiz: legal@wibiz.ai, and by post to the registered office stated in the opening paragraph of Part A.

A.23 General

The agreement contains the entire agreement for its subject matter. Amendments must be written and authorised. Neither party may assign without the other's written consent, except either party may assign to an affiliate or in connection with a merger, acquisition, or sale of substantially all its business, provided the assignee agrees in writing to assume the assigning party's obligations. Neither party creates a partnership, employment, fiduciary, or agency relationship. Invalid provisions are adjusted only to the minimum extent necessary. Failure to enforce is not a waiver. Counterparts and approved electronic signatures may be used.

Schedule 1: Service Levels

This Schedule applies only to the production services identified in an executed Order Form. It does not apply to public websites, demonstrations, implementation environments, beta features, customer-owned systems, or third-party services unless expressly listed.

1.1 Covered services

Production service	Measurement boundary	Region	Service owner	Effective date
No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	As stated in the Order Form	As stated in the Order Form	As stated in the Order Form

1.2 Definitions

"Available Minutes" means total minutes in the measurement month, excluding approved exclusions. "Downtime" means minutes when the covered service is unavailable to substantially all authorised users at the agreed measurement point. "Monthly Uptime Percentage" means `(Available Minutes - Downtime) / Available Minutes x 100`.

1.3 Availability commitment

Covered service	Monthly uptime target	Measurement source	Reporting method
No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	As stated in the Order Form	No commitment unless stated in the Order Form

No uptime percentage applies unless stated in the Order Form.

1.4 Exclusions

Exclusions are stated in the Order Form, supported by objective evidence, and may include:

- announced maintenance within the approved window;
- customer systems, actions, credentials, configurations, or instructions outside WiBiz control;
- third-party systems expressly excluded in the Order Form;
- customer-requested suspension;
- unlawful or prohibited use;

- force majeure under Part A; and
- emergency protective action reasonably necessary to prevent material harm.

1.5 Maintenance

Term	Commitment
Standard maintenance window	No commitment unless stated in the Order Form
Advance notice	No commitment unless stated in the Order Form
Emergency maintenance notice	As soon as reasonably practicable
Maximum excluded maintenance	No commitment unless stated in the Order Form

WiBiz will minimise maintenance impact and use reasonable efforts to avoid the customer's stated critical periods.

1.6 Incident priority

Priority	Objective definition	Customer impact examples
P1 Critical	Covered production service unavailable or confirmed severe security impact with no reasonable workaround	As stated in the Order Form
P2 High	Material production function impaired, significant users affected, workaround limited	As stated in the Order Form
P3 Medium	Non-critical function impaired, workaround available	As stated in the Order Form
P4 Low	General question, cosmetic issue, or low-impact request	As stated in the Order Form

Final classification considers actual impact, scope, urgency, security, and available workaround. WiBiz may reclassify with reasons and evidence.

1.7 Support and response targets

Priority	Coverage window	Initial response	Update cadence	Target restoration or workaround	Target resolution
P1	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form
P2	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form
P3	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form
P4	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	No commitment unless stated in the Order Form

"Initial response" means acknowledgement and assignment, not resolution. Resolution targets must not be presented as guarantees unless expressly approved.

1.8 Support submission and customer cooperation

Approved support channel: the support address stated in the Order Form Emergency channel: security@wibiz.ai for a security-impacting incident Support timezone and holidays: Singapore time, aligned to Singapore public holidays, per the published WiBiz pricing tiers (same-day business-hours support for Standard and Pro, named-contact priority support for Pro, email-only support for Lite)

Customer must provide reasonable diagnostic information, an authorised contact, safe access where required, and timely decisions. WiBiz must not request production credentials through an unapproved channel.

1.9 Security incidents and personal data breaches

Security-incident and personal-data-breach notification is governed by Schedule 2 and Schedule 3 (Information Security), not by ordinary support targets. No contractual incident-notification hour is approved in this draft.

1.10 Continuity, backup, and recovery

1.11 Service credits and remedies

Monthly uptime band	Proposed credit	Status
No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	Not applicable

No service credit applies unless stated in the Order Form.

1.12 Reporting and review

WiBiz will provide the approved service report or incident report stated in the Order Form. Material incidents should have a documented cause, containment, recovery, corrective actions, owners, and target dates, within applicable security and legal restrictions.

1.13 Changes

This Schedule may change only through the contract change mechanism. Public status pages or policy updates do not reduce a signed service level.

Schedule 2: Data Processing

This Schedule 2 (Data Processing) forms part of the agreement between the customer identified in the applicable Order Form ("Customer") and the verified WiBiz contracting entity ("WiBiz"). It applies only to processing of personal data by WiBiz on behalf of Customer.

2.1 Definitions and interpretation

"Applicable Data Protection Law" means the personal-data law applicable to the processing described in Appendix 2A, including the Singapore Personal Data Protection Act 2012 ("PDPA") and, only where in scope, the EU General Data Protection Regulation 2016/679 ("GDPR"), UK data protection law, or other identified law.

"Customer Personal Data" means personal data processed by WiBiz on behalf of Customer under the agreement. "Data Breach" means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Data. "Subprocessor" means a third party engaged by WiBiz to process Customer Personal Data on Customer's behalf.

Controller, processor, organisation, data intermediary, data subject, processing, and supervisory authority have the meanings given by applicable law.

If this Schedule 2 conflicts with Part A on personal-data processing, this Schedule 2 controls. Applicable approved transfer clauses control to the extent of a conflict concerning a restricted transfer.

2.2 Roles and scope

Customer is the controller or organisation and WiBiz is the processor or data intermediary for the processing in Appendix 2A, unless the parties document another lawful role.

WiBiz may act as an independent controller for business contact, contract, billing, fraud-prevention, account-security, and legal-compliance data where it independently determines purposes and means. That processing is governed by the applicable external Privacy Notice and is outside this Schedule 2.

For a client-owned or white-label service, Customer is responsible for its end-user privacy notice, lawful basis, consent, rights process, and instructions unless the agreement expressly allocates a responsibility to WiBiz.

By default, Customer is controller or organisation and WiBiz is processor or data intermediary for the processing in Appendix 2A, and WiBiz is independent controller for its own business-contact, billing, contract-administration, security-contact, and account-administration data, governed by the External Privacy Notice rather than this Schedule 2. A product-specific role matrix confirming this default, or documenting an exception, is completed per Order Form as an operational verification step.

2.3 Customer instructions

WiBiz will process Customer Personal Data only:

- on Customer's documented instructions in the agreement, Appendix 2A, approved configurations, or authorised written directions;
- to provide, secure, support, and maintain the contracted services; or
- as required by law, in which case WiBiz will notify Customer before processing unless prohibited.

Instructions include approved international transfers. WiBiz will promptly inform Customer if it reasonably believes an instruction infringes Applicable Data Protection Law and may suspend the affected processing while the parties resolve the issue.

Customer is responsible for ensuring its instructions, collection, disclosures, and use are lawful and for providing required information to data subjects.

2.4 Confidentiality and personnel

WiBiz will limit access to personnel who need Customer Personal Data for authorised duties. Those personnel must be bound by confidentiality and receive appropriate privacy and security instruction.

2.5 Security

WiBiz will implement and maintain appropriate technical and organisational measures proportionate to risk. The binding measures for the service must be completed in Schedule 3 (Information Security) and Appendix 2C of this Schedule 2.

The parties will consider the state of the art, implementation costs, nature, scope, context, purposes, and risks to individuals. Customer is responsible for the security responsibilities expressly allocated to it.

No unverified certification, universal encryption, residency, recovery, or testing claim is incorporated by this clause.

2.6 Subprocessing

General written authorisation applies: WiBiz will give 30 days' advance notice of a new or replaced Subprocessor and Customer may object on reasonable data-protection grounds within that period; if the parties cannot resolve the objection, Customer may terminate the affected service without penalty as its remedy.

WiBiz will:

- maintain a current Subprocessor Schedule identifying function and relevant processing location;
- conduct proportionate due diligence before appointment;
- impose written data-protection obligations providing no less protection than this Schedule 2 for the delegated processing;
- remain responsible for Subprocessor performance to the extent required by applicable law; and
- notify Customer of approved changes using the agreed mechanism.

The notice period is 30 days, per the clause above; the Subprocessor list itself is Appendix 2B, completed per engagement with a verified inventory.

2.7 Assistance with individual rights

Taking into account the nature of processing, WiBiz will provide reasonable assistance through appropriate technical and organisational measures so Customer can respond to requests concerning access, correction, deletion, restriction, objection, portability, or other applicable rights.

If WiBiz receives a request relating to Customer Personal Data, it will not respond on Customer's behalf unless authorised or legally required. It will forward the request to Customer without undue delay, using lawful identity and security controls.

Requests: the privacy request channel stated in Appendix 2D. Included assistance covers reasonable technical and organisational support to respond to a rights request using the service's existing functionality; assistance requiring material additional engineering work outside ordinary service delivery is chargeable at WiBiz's standard rates, agreed in advance.

2.8 Data Breaches

WiBiz will notify Customer without undue delay after becoming aware of a Data Breach affecting Customer Personal Data. The initial notice will include available information concerning:

- the nature and scope of the incident;
- affected data, systems, and individuals where known;
- likely consequences;
- containment and remediation measures;
- the incident contact; and
- information reasonably required for Customer's assessment and notifications.

WiBiz may provide information in phases and will give material updates. Notification is not an admission of fault.

WiBiz's operational target is notification within 72 hours of becoming aware of a confirmed Data Breach, using the incident channel stated in Appendix 2D, with material updates as they become available. This is a target, not an admission that every incident is assessable within that window, and does not change the "without undue delay" obligation above. Forensic cooperation, regulator and individual communications, evidence preservation, and cost allocation follow Schedule 3 (Information Security)'s incident-response terms once completed for the relevant engagement.

Customer determines whether and how to notify regulators and individuals unless law directly requires WiBiz to notify. The parties will coordinate public statements where lawful.

2.9 Compliance assistance

Taking into account the nature of processing and information available, WiBiz will reasonably assist Customer with security obligations, breach assessment, data protection impact assessments, and prior consultation with regulators where required.

Included assistance covers reasonable support using existing service documentation and functionality; material work outside ordinary service delivery, such as a bespoke data protection impact assessment, is chargeable at WiBiz's standard rates, agreed in advance.

2.10 Government and legal requests

Unless prohibited, WiBiz will notify Customer of a legally binding request for Customer Personal Data and will assess the request for validity, seek clarification or limitation where appropriate, and disclose only what is legally required.

Additional obligations for restricted transfers are governed by the approved Standard Contractual Clauses or other transfer addendum.

2.11 Return and deletion

At Customer's choice after service termination, WiBiz will return or delete Customer Personal Data and existing copies unless law requires retention.

On Customer's request after termination, WiBiz will make Customer Data available for export in a standard machine-readable format for 30 days, then delete it, including from routine backups within their normal rotation cycle rather than by special extraction, except where law requires longer retention. Transition assistance beyond standard export is chargeable at WiBiz's standard rates, agreed in advance.

2.12 Records and audits

WiBiz will make available information reasonably necessary to demonstrate compliance with this Schedule 2 and will permit audits required by applicable law under approved safeguards.

The parties should first use current independent reports, certifications, questionnaires, and remote evidence where sufficient. Any further audit must have reasonable notice, defined scope, qualified and confidential auditors, security safeguards, minimal operational disruption, and protection for other customers.

A further audit requires 30 days' written notice, a defined scope, a confidentiality undertaking from the auditor, and is limited to once per 12 months absent a substantiated security incident, in which case additional audit rights apply without the frequency limit; Customer bears its own audit costs, WiBiz bears the reasonable cost of its own personnel's time, and regulator access is provided as required by applicable law.

2.13 International transfers

WiBiz will not transfer Customer Personal Data to another country or permit remote access from another country except on documented instructions and with safeguards required by Applicable Data Protection Law.

For Singapore PDPA scope, relevant contracts and practices must provide a standard of protection comparable to the PDPA. Countries and territories must be identified where required.

For an EEA restricted transfer, the parties will execute the approved International Transfers Annex with the correct module, completed annexes, and transfer assessment. Separate UK or Swiss mechanisms must be completed where applicable.

2.14 Liability

Liability arising from this Schedule 2 is governed by the approved Part A liability framework, except where applicable law or transfer clauses require otherwise.

This Schedule 2's liability is governed by the Part A clause A.15 cap, including the increased cap for the confirmed-security-breach indemnity in Part A clause A.14, except where the approved International Transfers Annex's own liability terms apply to a specific restricted transfer.

2.15 Term and changes

This Schedule 2 continues while WiBiz processes Customer Personal Data. Material changes require written agreement, except an update expressly permitted by an approved subprocessor process or required to comply with law without reducing protection.

Appendix 2A: Processing details

Required detail	Completed description
Subject matter	As stated in the Order Form
Duration	As stated in the Order Form
Nature and purpose	As stated in the Order Form
Processing operations	As stated in the Order Form
Data subject categories	As stated in the Order Form
Personal data categories	As stated in the Order Form
Restricted or special data	Prohibited by default unless expressly permitted per engagement with verified safeguards in Schedule 3 (Information Security)
Processing frequency and volume	As stated in the Order Form
Customer instructions	As stated in the Order Form
Retention and deletion	30-day export window after termination, then deletion including from routine backups; see clause 2.11
Controller or organisation	As stated in the Order Form
Processor or data intermediary	As stated in the Order Form
Independent controller activities	As stated in the Order Form

Appendix 2B: Subprocessors and locations

Subprocessor legal name	Function	Service or product	Data categories	Primary location	Backup or log location	Support-access location	Transfer mechanism	Approval date
As stated in the Order Form								

Appendix 2C: Technical and organisational measures

The technical and organisational measures in Schedule 3 (Information Security) apply, with any service-specific variations stated in the Order Form.

Appendix 2D: Contacts and decisions

Field	Details
Customer privacy contact	As stated in the Order Form
WiBiz privacy contact	privacy@wibiz.ai
Incident channel	security@wibiz.ai
Rights-request channel	privacy@wibiz.ai
Contractual incident target	72 hours from WiBiz becoming aware of a confirmed Data Breach, as an operational target
Subprocessor authorisation model	General written authorisation with 30 days' advance notice and objection rights
Subprocessor notice period	30 days
Audit model	Independent reports and questionnaires first; further audit on 30 days' notice, once per 12 months absent a substantiated incident
Applicable laws	As stated in the Order Form
International transfer addendum	As stated in the Order Form

Schedule 3: Information Security

This Schedule describes the security commitments that apply only when completed, approved, and incorporated into an executed agreement. Internal policy objectives, planned controls, public summaries, and certification roadmaps are not binding service commitments unless stated here.

3.1 Scope and responsibility

Field	Completed scope
Covered services	No commitment unless stated in the Order Form
Covered environments	No commitment unless stated in the Order Form
Covered Customer Data	As stated in the Order Form
Excluded systems	As stated in the Order Form
WiBiz security owner	No commitment unless stated in the Order Form
Customer security owner	As stated in the Order Form
Effective date	As stated in the Order Form

Customer remains responsible for controls allocated to it, including authorised users, lawful instructions, customer-managed devices, customer-owned systems, credentials, configurations, and timely removal of access.

3.2 Security governance

WiBiz will maintain a documented information-security programme proportionate to the covered services and risks. The programme will assign responsibilities, review risks, manage approved policies, track remediation, and retain evidence.

3.3 Asset and data management

WiBiz will maintain inventories reasonably sufficient to identify covered systems, service owners, data categories, processing purposes, and applicable locations. Customer Data will be classified and handled according to approved sensitivity requirements.

Production Customer Data must not be used in development or testing unless expressly authorised, minimised, and protected under equivalent controls.

Control decision	Approved value
Permitted data categories	No commitment unless stated in the Order Form
Prohibited or restricted data	No commitment unless stated in the Order Form
Primary data locations	As stated in the Order Form
Backup and log locations	As stated in the Order Form
Support-access locations	As stated in the Order Form
Retention and deletion	No commitment unless stated in the Order Form

3.4 Identity and access management

WiBiz will use individual accounts, least-privilege access, role-appropriate approval, timely access removal, and periodic review for covered systems.

Control	Binding service commitment
Multi-factor authentication scope	No commitment unless stated in the Order Form
Privileged-access approval	No commitment unless stated in the Order Form
Access review frequency	No commitment unless stated in the Order Form
Leaver removal target	No commitment unless stated in the Order Form
Emergency-access controls	No commitment unless stated in the Order Form
Customer access responsibilities	As stated in the Order Form

No statement that all systems use multi-factor authentication or quarterly review applies unless stated in the Order Form.

3.5 Encryption and key management

WiBiz will use service-appropriate protections for Customer Data in transit and at rest, as verified below.

Data or service	In-transit protection	At-rest protection	Key owner and service	Exceptions	Evidence date
As stated in the Order Form					

3.6 Secure configuration and change management

WiBiz will maintain approved configurations, separate production access where appropriate, review material changes, record deployments, and provide rollback or recovery measures proportionate to risk.

Emergency changes must be documented and retrospectively reviewed.

3.7 Secure development and release

For WiBiz-controlled code in scope, the approved process will address:

- security requirements and threat considerations;
- peer review or independent review;
- dependency and secret checks;
- automated and manual testing proportionate to risk;
- environment separation and controlled deployment;
- remediation of release-blocking findings; and
- retained release evidence.

3.8 Logging, monitoring, and detection

Covered services will generate and protect logs sufficient for approved operational and security purposes, consistent with data minimisation and retention limits.

Control	Approved commitment
Logged events	No commitment unless stated in the Order Form
Log retention	No commitment unless stated in the Order Form
Monitoring coverage	No commitment unless stated in the Order Form
Alert triage coverage	No commitment unless stated in the Order Form
Time synchronisation	No commitment unless stated in the Order Form
Customer log access	No commitment unless stated in the Order Form

3.9 Vulnerability management and security testing

WiBiz will maintain a risk-based process to identify, assess, remediate, and verify vulnerabilities in covered systems.

Item	Approved commitment
Vulnerability scanning scope and frequency	No commitment unless stated in the Order Form
Critical remediation target	No commitment unless stated in the Order Form
High remediation target	No commitment unless stated in the Order Form
Medium and low treatment	No commitment unless stated in the Order Form
Independent penetration-test scope and cadence	No commitment unless stated in the Order Form
Retest requirement	No commitment unless stated in the Order Form
Client evidence	No commitment unless stated in the Order Form

Testing must be authorised by written Rules of Engagement defining scope, exclusions, test window, safety controls, data handling, emergency stop, reporting, remediation, retest, and disclosure.

No annual penetration-test or remediation-day commitment applies unless stated in the Order Form.

3.10 Incident response

WiBiz will maintain an incident process covering reporting, triage, containment, investigation, recovery, evidence, communication, corrective action, and lessons learned.

Data Breach obligations are governed by Schedule 2.

3.11 Business continuity, backup, and recovery

Service	Backup scope	Frequency	Location	Retention	RPO	RTO	Restore-test evidence
As stated in the Order Form					No commitment unless stated in the Order Form	No commitment unless stated in the Order Form	As stated in the Order Form

No universal backup, disaster-recovery, RPO, or RTO claim is approved. Customer responsibilities for exports, local copies, continuity, and customer-owned systems must be stated in the Order Form.

3.12 Vendor and subprocessor security

WiBiz will perform proportionate due diligence before using a material vendor or Subprocessor for the covered services, impose appropriate written obligations, track material risks, and review changes according to the approved vendor process.

The binding Subprocessor list is the completed Schedule 2 schedule, not a generic policy statement.

3.13 Personnel security

WiBiz will require confidentiality, role-appropriate security instruction, acceptable-use compliance, and access controls for personnel with covered access.

3.14 Physical security

Physical controls for provider-operated facilities and cloud data centres must be described according to verified responsibility. WiBiz must not claim to operate physical controls belonging to a cloud provider.

3.15 Data separation, export, and deletion

WiBiz will use service-appropriate logical separation and authorisation controls. Export and deletion will follow Schedule 2 and Order Form.

3.16 Assurance and customer review

WiBiz may provide approved questionnaires, policy summaries, test summaries, independent reports, or certifications within applicable confidentiality and security restrictions. Certifications must be described by exact scope, issuer, status, and validity date.

WiBiz must not describe SOC 2 as a certification or claim Cyber Essentials, ISO 27001, DPTM, CSA STAR, or another status without current evidence and approval.

Audit rights are governed by Schedule 2 and Part A.

3.17 Material changes

WiBiz will not materially reduce the agreed protection of Customer Data during an active Order Form without the approved notice and contract process. Changes required to address an urgent risk may be implemented promptly, with notice where reasonably practicable.

3.18 Exceptions and residual risks

Exception or open control	Affected service or data	Risk	Compensating control	Owner	Target date	Customer disclosure required
As stated in the Order Form						

Schedule 4: Acceptable Use

4.1 Application

This Schedule 4 (Acceptable Use) applies to customers, authorised users, and anyone using a WiBiz-owned service under a customer account. It is separate from the internal workforce acceptable-use policy.

For a client-owned or white-label service, the client remains responsible for acceptable-use terms presented to its end users unless the signed agreement states otherwise. This Schedule still governs the client's use of WiBiz services where incorporated into the client agreement.

4.2 General rule

Users must use the services lawfully, safely, and in accordance with the signed agreement, documented instructions, and rights of other people. A customer is responsible for its authorised users, content, instructions, configured workflows, contact lists, permissions, and legally required notices and consents.

4.3 Prohibited conduct

Users must not use a service to:

- violate law, regulation, court order, sanctions, or another person's rights;
- commit fraud, impersonation, deception, harassment, stalking, threats, exploitation, or discrimination;
- send unlawful or unsolicited messages, calls, or marketing;
- process contact data without a lawful basis, required notice, and applicable consent;
- upload malware, harmful code, credential-stealing material, or destructive instructions;
- probe, scan, test, bypass, or compromise security without written authorisation;
- gain unauthorised access to accounts, networks, data, or devices;
- interfere with availability, impose unreasonable load, or evade usage controls;
- scrape, harvest, or enrich personal data unlawfully;
- infringe intellectual property, privacy, publicity, confidentiality, or contractual rights;
- generate or distribute unlawful sexual content, child sexual abuse material, extremist content, or content facilitating serious harm;
- provide regulated professional advice or make legally significant decisions without qualified human oversight where law or the agreement requires it;
- submit payment-card data, government identifiers, health data, biometric data, children's data, credentials, or other restricted data unless the applicable Order Form and security schedule expressly permit it;

- conceal message origin, manipulate consent records, or disable required opt-out mechanisms; or
- resell, sublicense, benchmark publicly, reverse engineer, or build a competing service except as expressly permitted in writing.

4.4 Communications and consent

Customers must maintain accurate source, consent, suppression, and opt-out records for communications they direct. They must honour opt-outs promptly and comply with applicable calling, messaging, marketing, recording, and do-not-contact laws.

Supported messaging and calling channels, and their channel-specific compliance schedules, are identified per product in the Order Form; this Schedule's general communications-and-consent obligations above apply regardless of which channels a given engagement uses.

4.5 Data and account security

Customers must:

- restrict access to authorised users;
- use available authentication and security controls;
- protect credentials and devices;
- promptly remove access that is no longer required;
- use minimum necessary data;
- follow documented export and deletion procedures; and
- notify WiBiz promptly of suspected unauthorised access or prohibited use.

4.6 Monitoring and investigation

WiBiz may use proportionate technical and organisational measures to prevent, detect, and investigate misuse as permitted by applicable law and the agreement. WiBiz may preserve relevant records where reasonably necessary for security, legal compliance, or claims.

4.7 Enforcement

Where reasonably practicable, WiBiz will notify the customer and allow remediation. WiBiz may restrict or suspend affected use immediately where necessary to prevent material harm, protect systems or third parties, comply with law, or respond to an urgent security risk.

Termination, data export, fees during suspension, reactivation, and appeal rights are governed by the signed agreement. This Schedule does not create an unapproved right to suspend all services or retain customer data indefinitely.

4.8 Reporting

Report suspected abuse or security concerns to abuse@wibiz.ai or security@wibiz.ai. Good-faith vulnerability reports are governed by the Responsible Disclosure Policy.

4.9 Changes

Material changes require a new version and notice under the signed agreement. A change must not retroactively expand restrictions or reduce a customer's material contractual rights.

Schedule 5: Refunds and Cancellation

5.2 Contracting entity and merchant

Contracting entity and merchant of record: Digital Benefits Pte. Ltd. trading as WiBiz, UEN 201735371H. Payment providers: Stripe, and Razorpay where used, as payment processors, not a separate merchant of record. Support contact: the support contact stated in the Order Form.

5.6 Service failure, delivery guarantee, and credits

Any delivery guarantee, dormancy exit, service credit, remediation right, or refund for service failure must be stated consistently in the signed agreement and Schedule 1 (Service Levels). This Schedule does not create a broader or conflicting remedy.

Under these terms, the delivery-guarantee remedy (re-performance, then pro-rata refund of fees for the specific non-conforming deliverable if uncured) is the exclusive remedy for a delivery failure; service credits under Schedule 1 (Service Levels), where they exist, are the exclusive remedy for the specific availability shortfall they address; termination rights follow Part A clause A.17.

5.7 Exclusions

Completed work and consumed usage are non-refundable once commenced.

No exclusion applies where prohibited by law.

5.8 Consumer and mandatory rights

Nothing in these terms excludes a mandatory consumer guarantee, cooling-off right, unfair-contract-term protection, or other non-excludable remedy.

5.9 Chargebacks

Customers should contact the approved support channel before initiating a chargeback where lawful. WiBiz may provide transaction and delivery records to payment providers and financial institutions in response to a chargeback as permitted by privacy law.

5.10 Changes

Changes apply prospectively from the stated effective date. Existing purchases remain governed by the version incorporated when the purchase was made, except where law requires otherwise.

Annex: International Transfers and Standard Contractual Clauses

T.1 Purpose and conditional application

This Annex applies only where the services involve a transfer of personal data that requires an approved international transfer mechanism. It does not establish that every WiBiz engagement falls within GDPR or requires Standard Contractual Clauses ("SCCs").

The parties must first determine:

- the exporter and importer legal entities;
- the role of each party for each processing activity;
- whether the transfer is restricted;

- whether the importer and processing already fall directly within GDPR;
- the countries and remote-access locations involved;
- the appropriate transfer mechanism; and
- whether EEA, UK, Swiss, Singapore, or other law applies.

T.2 EEA Standard Contractual Clauses incorporation

Where this Annex applies, the parties incorporate the European Commission SCCs in the Annex to Commission Implementing Decision (EU) 2021/914, available from the official European Commission or EUR-Lex source, as completed by this Annex.

The Standard Contractual Clauses text must not be altered except for permitted module selection, options, party details, Appendix completion, and additional safeguards that do not contradict the clauses or prejudice data-subject rights.

The SCCs prevail over conflicting agreement terms for the covered transfer.

T.3 Module and options

The selections for each transfer are stated in the Order Form:

Standard Contractual Clauses item	Selection
Module 1, controller to controller	No commitment unless stated in the Order Form
Module 2, controller to processor	No commitment unless stated in the Order Form
Module 3, processor to processor	No commitment unless stated in the Order Form
Module 4, processor to controller	No commitment unless stated in the Order Form
Clause 7 docking clause	No commitment unless stated in the Order Form
Clause 9 subprocessor authorisation	No commitment unless stated in the Order Form
Clause 9 notice period	No commitment unless stated in the Order Form
Clause 11 independent dispute resolution	No commitment unless stated in the Order Form
Clause 17 governing Member State law	No commitment unless stated in the Order Form
Clause 18 courts	No commitment unless stated in the Order Form

Module 2 is commonly relevant to an EEA controller engaging a Singapore processor. Module 3 may be relevant when the exporter is a processor and WiBiz is a subprocessor. These are examples, not completed selections.

T.4 Annex I.A: Parties

Data exporter

Field	Details
Legal name and registration	As stated in the Order Form
Address	As stated in the Order Form
Contact person and details	As stated in the Order Form
Activities relevant to transfer	As stated in the Order Form
Role	No commitment unless stated in the Order Form

Signature and date	As stated in the Order Form

Data importer

Field	Details
Legal name and UEN	Digital Benefits Pte. Ltd., UEN 201735371H
Address	60 Paya Lebar Road, #06-28, Paya Lebar Square, Singapore 409051
Contact person and details	privacy@wibiz.ai
Activities relevant to transfer	As stated in the Order Form
Role	No commitment unless stated in the Order Form
Signature and date	As stated in the Order Form

T.5 Annex I.B: Transfer description

Required detail	Completed description
Data subject categories	As stated in the Order Form
Personal data categories	As stated in the Order Form
Sensitive data and restrictions	No commitment unless stated in the Order Form
Transfer frequency	As stated in the Order Form
Nature of processing	As stated in the Order Form
Processing purpose	As stated in the Order Form
Retention period or criteria	No commitment unless stated in the Order Form
Subprocessor processing	As stated in the Order Form
Primary storage country	As stated in the Order Form
Backup and log countries	As stated in the Order Form
Remote support-access countries	As stated in the Order Form

T.6 Annex I.C: Supervisory authority

T.7 Annex II: Technical and organisational measures

Attach Schedule 3 (Information Security) and provide specific measures for the covered transfer, including as applicable:

- pseudonymisation and encryption;
- confidentiality, integrity, availability, and resilience;
- restoration of availability and access;
- security testing and evaluation;
- identity, authentication, authorisation, and access review;
- logging and monitoring;
- secure transmission and storage;
- physical security;

- event detection, response, and breach notification;
- business continuity and backups;
- deletion, retention, and data minimisation;
- subprocessor governance;
- data-subject rights assistance; and
- transfer-specific supplementary measures.

Generic policy statements are not enough. Measures must identify actual service scope, responsible party, current implementation, and evidence.

T.8 Annex III: Subprocessors

Complete if the selected module and authorisation option require it.

Subprocessor	Address and contact	Processing description	Location	Safeguard	Authorisation date
As stated in the Order Form					

T.9 Transfer impact assessment

Before transfer, the parties must document the Clause 14 assessment, including:

- transfer circumstances, categories, format, frequency, and chain;
- destination and remote-access countries;
- relevant laws and practices concerning access by public authorities;
- available practical experience where relevant;
- contractual, technical, and organisational safeguards;
- likelihood and severity of harm;
- necessity of supplementary measures; and
- approval, review trigger, and evidence sources.

T.10 Government access and supplementary measures

WiBiz will follow the selected Standard Contractual Clauses obligations concerning government requests, including validity review, challenge where reasonable grounds exist, data minimisation, exporter notice where permitted, and transparency records.

T.11 Onward transfers and changes

Onward transfers require a lawful basis and the safeguards required by the selected Standard Contractual Clauses module. A new country, access location, subprocessor, or material processing change must trigger review of the transfer record and assessment.

T.12 UK and Swiss transfers

The EU SCCs alone may not complete UK or Swiss transfer requirements.

- UK transfers require the approved UK International Data Transfer Agreement or UK Addendum, completed for the actual transfer.
- Swiss transfers require the necessary adaptations and authority details where applicable.

T.13 Singapore transfers

For PDPA scope, the parties must ensure legally enforceable obligations and practices providing protection comparable to the PDPA. Contracts should identify relevant countries and territories and bind recipients to appropriate protection, retention, breach, and onward-transfer controls.

Version history and source record

Version	Date	Change
v1.0	1 November 2026	First issue. Consolidates the client-facing contract instruments into one document, signed or accepted once through the Order Form.

Source instruments consolidated, with substantive terms unchanged except as listed below: Master Services Agreement v1.3 (Part A), Service Level Schedule v1.2 (Schedule 1), Data Processing Addendum v1.2 (Schedule 2), Information Security Schedule v1.2 (Schedule 3), Customer Acceptable Use Policy v1.2 (Schedule 4), Refund and Cancellation Policy v1.2 (Schedule 5), International Transfer and Standard Contractual Clauses Addendum v1.2 (Annex). Agreements already signed on those instruments continue on them until migrated.

Consolidation changes:

1. Clauses renumbered with a part prefix (A., 1. to 5., T.); internal cross-references renumbered to match. References to Standard Contractual Clauses clause numbers are unchanged.
2. References between instruments unified: the MSA becomes Part A, the Data Processing Addendum becomes Schedule 2, and so on; "this Addendum", "this Schedule" and "this Policy" read "this Schedule" or "this Annex". The Data Processing Addendum's own Schedules 1 to 4 become Appendices 2A to 2D.
3. Part A clause A.1 lists the consolidated document and adds one-click acceptance of the Order Form as a form of execution; priority item 7 names Schedules 4 and 5.
4. Per-engagement blank fields now read "As stated in the Order Form"; fields that held no approved value read "No commitment unless stated in the Order Form", so no undecided figure is presented as a commitment.
5. Internal drafting notes, issuance checklists, approval registers, signature blocks and internal decision-record references removed; separate signatures are replaced by the single Order Form signature or acceptance.
6. Schedule 5 carries the clauses of the Refund and Cancellation Policy that apply to invoiced engagements (contracting entity, service-failure remedies, exclusions, mandatory rights, chargebacks, changes); the self-service drafting framework (scope note, purchase-category table, cancellation and refund drafting instructions) is not carried because it applies to no current engagement.
7. Drafting phrases reworded without changing the commitment: "approved by this draft" becomes "applies unless stated in the Order Form"; "if approved by counsel" in the Annex becomes "where this Annex applies"; exclusions in Schedule 1 are those stated in the Order Form.
8. Public notices (Privacy Policy, cookies, Website Terms) are linked by public URL and not included.