

EMJ.NEXUS Data Rights & Exit Schedule

Subscriber Reading Edition SR1 | EMJ-NEXUS-DRE-001 | v1.0

Commercial baseline 12 October 2026 | v1.0 | Subscriber edition 14 October 2026

Legal provider EMJ LIFE HOLDINGS PTE. LTD. | Singapore UEN 202445078N

Contract Effective Date is determined by the executed Order Form. Template release does not activate service.

Reading and acceptance

This document is one of the seven required Stage Two acknowledgements. At Stage Two, read and download it while completing the Enterprise profile. OF has its separate reading-and-acceptance gate after KYB and before subscription plan selection.

Complete all fourteen required profile fields and separately acknowledge MCT, DPA, SEC, SLA, DRE, EIPP and CPS. Together with cleared payment and the correct Enterprise EGC ID, these are the conditions for the once-only first 200 E-IPP Points. A document checkbox alone does not confirm payment or activate service.

1. Purpose and Scope

This Schedule defines the rights, ownership, access, portability, retention, termination and exit treatment applicable to:

- Enterprise Input Data;
- Enterprise Personal Data;
- EMJ.NEXUS Metadata;
- Evidence Objects;
- Nodes;
- Missions;
- MCP records;
- EGC IDs;
- E-IPP Points;
- E-IPP Score history;
- Historical Records;
- Continuity Records;
- Association Records;
- Time-Integrity Records;
- Version Records;
- JSON evidence files;
- DOI landing pages;
- encrypted download archives;
- manifests;
- delivery records.

This Schedule forms part of the EMJ.NEXUS Enterprise Contract and Governance Pack and supplements:

- EMJ.NEXUS Enterprise Subscription Master Commercial Terms;
- the applicable Enterprise Order Form;
- Data Processing Addendum;
- Security Schedule;
- Service Level Agreement;
- E-IPP Points & Score Policy;
- Enterprise Digital Behaviour Evidence Compendium Schedule;
- applicable written amendments.

This Schedule governs data rights, Historical Records and exit. It does not replace:

- the DPA for Personal Data Processing;

- the Security Schedule for security controls;
- the SLA for availability and support;
- the E-IPP Policy for Points and Score rules;
- the Compendium Schedule for Compendium production and delivery.

2. Definitions

2.1 Enterprise Input Data

“Enterprise Input Data” means data, documents, files, statements, records, instructions, attachments, identifiers, evidence materials and other content lawfully submitted, uploaded, linked, created or authorised by or on behalf of the Enterprise for Processing through EMJ.NEXUS.

2.2 EMJ.NEXUS Metadata

“EMJ.NEXUS Metadata” means metadata, schemas, taxonomies, governance labels, control states, platform identifiers, relationship structures, version structures, publication metadata, delivery metadata, system metadata, technical metadata, configuration data and other structural or descriptive information generated, structured, maintained or governed by EMJ.LIFE in connection with EMJ.NEXUS.

2.3 Historical Records

“Historical Records” means records created, recorded or governed before the effective date of termination, expiry, suspension or non-renewal, including:

- Evidence Objects;
- Metadata;
- Node records;
- Mission records;
- Continuity Records;
- Association Records;
- Time-Integrity Records;
- Version Records;
- E-IPP Score history;
- DOI records;
- JSON records;
- delivery records;
- correction and supersession records.

2.4 Restricted EGC ID

“Restricted EGC ID” means an EGC ID whose historical identity and relationship records remain preserved, while active Mission, Node and evidence-creation functions are restricted.

2.5 Inactive EGC ID

“Inactive EGC ID” means an EGC ID that no longer provides active Subscription functions but remains associated with preserved Historical Records for traceability, continuity, version and governance purposes.

2.6 Exit Period

Exit Period means the 180 consecutive calendar days beginning on effective termination or expiry during which the Enterprise may request standard lawful export

and obtain restricted exit access. Temporary suspension does not itself start or shorten this window.

This is a request/access window, not the export turnaround time or permission to delay required deletion. A verified request submitted before its last day remains actionable after that day. An earlier deletion instruction or mandatory legal deadline prevails.

3. Enterprise Input Data Rights

3.1 Enterprise ownership

The Enterprise retains its pre-existing ownership and other rights in Enterprise Input Data, subject to:

- third-party rights;
- applicable law;
- the rights granted under the Agreement;
- the Enterprise's lawful authority to submit and use the data.

3.2 Processing licence

The Enterprise grants EMJ.LIFE a limited, non-exclusive, non-transferable and non-sublicensable right, except to authorised Sub-processors, to Process Enterprise Input Data as necessary to:

- provide EMJ.NEXUS;
- follow Enterprise instructions;
- maintain accounts;
- create and manage Evidence Objects;
- provide support;
- maintain security;
- perform backup and recovery;
- provide export and exit;
- prepare an authorised Compendium;
- comply with law;
- perform the Agreement.

3.3 No ownership transfer

Processing, storing, structuring, governing, recording, delivering or retaining Enterprise Input Data does not transfer ownership of the Enterprise Input Data to EMJ.LIFE.

4. EMJ.NEXUS Metadata Rights

4.1 EMJ.LIFE ownership and control

EMJ.LIFE or its licensors own or control EMJ.NEXUS Metadata, including:

- schemas;
- taxonomies;
- governance labels;
- control states;
- platform identifiers;
- relationship structures;
- version structures;
- publication Metadata;
- delivery Metadata;
- technical and system Metadata;

- configuration data;
- product information;
- governance logic.

Public LEI source data, registry facts and the Enterprise's underlying operating/contact/tax submissions do not become exclusive EMJ.LIFE intellectual property merely through storage or source matching. Applicable public-source and third-party rights remain distinct from proprietary platform schemas and governance logic. Keep source identity snapshots, enterprise supplements and internal completion/matching decisions distinguishable.

4.2 Platform access and surviving delivered-file licence

Active platform and Metadata access is limited to the Subscription Term and applicable restricted exit access. Separately, EMJ.LIFE grants the Enterprise a non-exclusive, perpetual, royalty-free right to retain, reproduce and use its lawfully delivered evidence files and embedded enterprise-specific descriptive Metadata for lawful internal and external evidence purposes after platform access ends.

Authorised disclosure to advisers, auditors, customers, regulators or other permitted recipients is allowed within applicable confidentiality, Data Subject and third-party restrictions. Clearly labelled working/derivative copies are allowed; altered files must not be represented as original issued evidence.

The licence does not transfer platform/schema ownership, grant a competing-service licence, permit bulk extraction/reconstruction of proprietary platform models, or expand actual licensed-content redistribution rights. Public DOI metadata retains its actual agency/public rights basis. A lawful restriction or required correction may affect use of the affected record, not arbitrarily cancel all previously delivered-file rights.

4.3 No reconstruction or commercialisation

The Enterprise shall not:

- reconstruct EMJ.NEXUS Metadata;
- reverse engineer the platform;
- extract the platform data model;
- commercialise the Metadata;
- provide schemas or governance logic to a competitor;
- use Metadata to create a competing product;
- claim ownership through access or delivery.

5. Evidence Objects, Nodes and Missions

5.1 Evidence Objects

The Enterprise retains rights in its original Enterprise Input Data and content incorporated into an Evidence Object.

EMJ.LIFE owns or controls:

- Evidence Object schemas;
- Evidence Object Metadata;
- platform structure;
- classification;
- control;
- version;
- relationship;
- status and governance logic.

The Enterprise may access and export Evidence Object content to which it is entitled.

5.2 Nodes

Node rights depend on:

- Enterprise Input Data;
- third-party rights;
- supplier agreements;
- applicable authorisations;
- the DPA;
- EMJ.NEXUS Metadata.

Creating or managing a Node does not represent that:

- the Node is approved;
- the Node is certified;
- the Node is assured;
- the Node is compliant;
- the Enterprise owns the Node;
- third-party data may be used without restriction.

5.3 Missions and MCP

The Enterprise retains rights in original Mission content it creates, subject to the Agreement.

EMJ.LIFE or its licensors own or control:

- Mission structure;
- Mission Metadata;
- MCP access permissions and disclosed task rules;
- participation logic;
- platform status;
- governance logic.

A Mission does not automatically establish:

- legal compliance;
- assurance;
- certification;
- performance;
- supplier approval;
- E-IPP Score;
- external acceptance.

6. EGC ID, Points and Score

6.1 EGC ID

An EGC ID is an internal enterprise-governance identifier.

It is not:

- a legal identity;
- a D-U-N-S Number;
- a company-registration number;
- an LEI;
- a tax identifier;
- an external certification;
- an external approval.

Issue or associate the EGC ID after cleared subscription payment under MCT Section 5.2, without waiting for Stage Two. Keep it associated with the verified LEI and Enterprise history. PROFILE_COMPLETE, current task permissions and initial Point allocation are independent; an incomplete profile or LEI restriction does not alone revoke the identifier or imply actual Subscription termination.

6.2 E-IPP Points

EIPP governs all Points. Temporary suspension freezes affected use without automatic forfeiture; eligibility and scheduled reset are handled under EIPP Section 14.1. On actual termination, expiry or non-renewal, unused Points expire with no cash value or refund; valid historical ledger outcomes remain attributable. Points are non-transferable between unrelated EGC IDs. A new active period does not revive expired operational balances except for the eligible annual allocation expressly governed by EIPP.

6.3 E-IPP Score

Historical E-IPP Score may be retained and displayed in accordance with the Agreement.

Termination does not automatically reset Historical E-IPP Score to zero.

Historical Score does not mean that the Enterprise continues to have:

- an active Subscription;
- active Mission rights;
- active Node rights;
- active Point rights;
- active evidence-creation rights.

7. Historical Records

7.1 No automatic deletion

Termination, expiry, suspension or non-renewal shall not automatically delete, erase, destroy or invalidate Historical Records.

Historical Records may include:

- Evidence Objects;
- Metadata;
- Node records;
- Mission records;
- EGC ID history;
- E-IPP Score history;
- Continuity Records;
- Association Records;
- Time-Integrity Records;
- Version Records;
- correction records;
- supersession records;
- DOI records;
- JSON records;
- delivery records;
- access records;
- export records.

7.2 Permitted historical retention

Preserve only records necessary for an authorised purpose within Section 14's schedule and applicable law. Personal Data in history remains subject to DPA protection, lawful instructions and deletion rights; an IP or evidence-integrity claim does not by itself authorise indefinite retention.

Necessary non-personal public publication identity and rights/version markers may remain for persistence. A legal hold must identify its basis, scope, access restriction and end/review date. Disputed, superseded or archived status is not a licence for unrelated commercial use.

7.3 Historical preservation is not active processing

Preserving Historical Records does not mean that EMJ.LIFE may continue active commercial Processing for unrelated purposes.

After termination, Historical Records may be:

- archived;
- access-restricted;
- marked Inactive;
- marked Superseded;
- subject to legal hold;
- subject to correction or dispute status.

8. Post-Termination EGC ID Status

8.1 Separate access and record states

Use account states Active, Suspended, Restricted and Inactive. Temporary suspension records its cause and scope; termination/expiry ends active rights and permits only authorised exit/historical access. Archived refers to a record-storage state, not automatic deletion of an EGC ID.

Publication/evidence, service activation, governance review and payload access use their separate SEC Section 16 domains. Every material transition records prior state, actor/authority, reason, source record and effective time. No unspecified new non-active state changes contractual rights without disclosure and an attributable rule.

8.2 Preserved identity and relationships

EMJ.LIFE shall preserve, subject to applicable law and retention rules:

- historical EGC ID identity;
- Enterprise association;
- Node relationships;
- Mission relationships;
- Evidence Object relationships;
- version relationships;
- time relationships;
- delivery relationships.

8.3 Prohibited post-termination activity

Unless the Enterprise reactivates an eligible Subscription, it shall not use a Restricted or Inactive EGC ID to:

- publish a new Mission;
- claim a new Mission;

- receive a new task;
- create a new governed participation record;
- add a governed Node;
- extend an evidence period;
- generate new E-IPP Points;
- generate new E-IPP Score activity;
- create a new Continuity Record;
- represent an inactive period as continuous.

9. Evidence Continuity

9.1 Actual cessation and technical interruptions

Actual termination, expiry or non-renewal stops new governed activity at its effective cessation time and creates an inactive gap. Temporary suspension or platform Downtime is evaluated from what activity and source/time/integrity records were actually preserved; it does not automatically prove that all evidence continuity was broken.

EMJ.LIFE shall document whether original timely source records remain verifiable and recoverable, what gap or limitation actually exists and which functions were affected. Provider-caused outage is not labelled an Enterprise compliance failure. Missing evidence, unlawful backdating or unsubstantiated periods cannot be invented to repair a real gap; retain any valid restricted/segmented record with its disclosed limitation.

A profile-completion hold, EntityStatus restriction or LAPSED renewal restriction is recorded for its actual affected new-task/evidence scope. It does not automatically invalidate evidence already lawfully recorded, erase historical Score or prove company closure. No new activity is invented during a blocked period; identify actual event, ingestion, source-status and permitted-function intervals before determining any continuity limitation.

9.2 No retroactive continuity

After actual cessation, reactivation starts Period B; it does not manufacture governed activity in the gap or merge it with Period A. Recovery of original timely records after a technical incident must preserve original event time, later ingestion/recovery time, reviewer and limitation; it is not permission to fabricate timestamps or unsupported participation.

9.3 Separate periods

Preserve attributable Period A records, the inactive gap and Period B records with their relationship. Do not present them as an uninterrupted period. An interrupted or shorter historical export may be delivered with an explicit limitation, but is not a 180-day eligible standard Compendium unless a separately substantiated uninterrupted qualifying period exists.

10. Data Export

10.1 Export right

During the Subscription Term and Exit Period, the Enterprise may request export of data to which it is entitled.

10.2 Standard exportable information

Provide the Enterprise's lawful Input Data and original attachments; entitled Evidence Object content; its source, time, continuity, version and correction records; its Node/Mission relationships; portable Score/ledger history and EGC ID association; issued JSON, entitled archive files, DOI landing metadata and relevant delivery records.

Include descriptive field names, record identifiers, status/rights boundaries and a minimal relationship description sufficient to interpret the exported enterprise records independently. Proprietary platform implementation, other-customer information and unauthorised third-party material are excluded; required personal-data access/portability and useful interpretation of the Enterprise's own records are not defeated by calling all descriptive fields proprietary Metadata.

Include entitled enterprise profile values and their source/supplement distinction, relevant LEI snapshots and query/update times, EGC ID association, completion/resolution and restriction history, and initial-allocation ledger history within lawful scope. Protect private invitation contacts and tax data and exclude other-entity/confidential supplier information. Optional D-U-N-S or third-party matching material is exported only within actual permissions; an export must not falsely label an unverified value as matched.

10.3 Restricted or non-exportable data

The Enterprise is not entitled to export:

- ownership of EMJ.LIFE Metadata;
- EMJ.NEXUS software;
- platform schemas;
- core data models;
- governance logic;
- Mission, MCP, Points or Score algorithms;
- internal risk models;
- another Enterprise's data;
- unauthorised third-party data;
- platform security secrets;
- vulnerability information;
- EMJ.LIFE trade secrets;
- unrelated confidential information.

10.4 Standard export format and integrity

Provide standard structured records in JSON and/or CSV, readable PDF where already issued, and entitled attachments in their existing format. Include a manifest, export date/version, basic field/relationship description and SHA-256 checksums or an agreed comparable integrity mechanism. A custom XBRL, XLSX or transformed format is not included unless expressly purchased and technically supported.

10.5 Export turnaround and lawful restrictions

Acknowledge a complete authorised export request within two Business Days and make one standard export available within ten Business Days after verified receipt, or sooner where mandatory law requires. Identify genuinely missing authorisation/scope information within two Business Days; do not restart the clock for information already held.

If unusual volume/format or a lawful third-party restriction prevents the standard time, give a specific reason, deliver the unaffected available portion on time and agree a

written schedule for the remainder. Provider technical inconvenience alone does not create indefinite delay. Disputed/unpaid fees do not block legally required Data Subject assistance or the included lawful standard exit export; custom paid migration work is separate.

10.6 Export fees

One standard exit export and ordinary return/deletion confirmation are included in the Subscription Fee. Standard rights assistance required by law is not conditioned on purchasing a service.

Additional repeated custom conversion, bespoke formats, extraordinary migration or professional transition work requires a separately disclosed and accepted scope/fee before work. The Enterprise's own data is not withheld solely to force acceptance of a custom migration charge.

11. JSON Evidence Files

The Enterprise may retain and use delivered JSON evidence files in accordance with:

- the Agreement;
- applicable access rights;
- confidentiality;
- third-party rights;
- limitation statements.

The Enterprise shall not:

- modify a file and represent it as the original;
- remove version information;
- remove DOI information;
- remove delivery information;
- remove integrity information;
- remove limitation statements;
- distribute it beyond authorised recipients;
- use it to imply audit, assurance or certification.

EMJ.LIFE retains ownership of the JSON schema, platform model and Metadata.

12. DOI Landing Pages

12.1 DOI metadata and payload states

A registered DOI has minimum publication/landing metadata separate from evidence-file access. That minimum may be public through the agency even if payload access is Private. Payload access is Private, Controlled Access or Public as expressly authorised under CPS Section 10.

Publication/version states ACTIVE, SUPERSEDED, HISTORICAL or WITHDRAWN and storage/archive indications are separate from account state and payload permissions. A restricted or expired account does not silently rewrite the public DOI identity or imply open access to its files.

12.2 Post-termination publication and download

After Subscription end, ordinary interactive/download access is limited to the Exit Period and permitted retention. The Enterprise keeps the surviving rights in already delivered files under Section 4.2.

For a registered DOI, EMJ.LIFE maintains the minimum resolving publication identity/status record while it remains the responsible publisher, without promising perpetual hosting of confidential payload. Where law requires withdrawal/redaction, preserve only the lawful minimal status record and version relationship. Reasonable successor/continuity arrangements follow Section 18. Third-party indexing is not guaranteed and metadata may remain public after payload deletion.

12.3 No implied public right

The existence of a DOI does not create:

- a public-access right;
- an unrestricted download right;
- an external assurance conclusion;
- a certification;
- regulatory acceptance;
- a government endorsement.

13. Encrypted Download Archives

The Enterprise may retain delivered encrypted archives.

The Enterprise is responsible for:

- key management;
- internal access;
- storage;
- backup;
- authorised distribution;
- protection against unauthorised decryption;
- protection against public disclosure.

EMJ.LIFE shall maintain reasonable delivery records, which may include:

- delivery date;
- recipient;
- download record;
- file version;
- integrity information;
- re-delivery record;
- withdrawal or supersession record.

14. Data Deletion, Anonymisation and Archiving

14.1 Default retention and deletion schedule

Record class	Default period / treatment
Operational Enterprise Input Data and Personal Data	During contracted Processing and the 180-day Exit Period, unless an earlier lawful instruction or legal deadline applies
Production copies after verified deletion trigger	Delete or irreversibly anonymise within 30 calendar days after the earlier trigger: verified deletion instruction or Exit Period end
Isolated backup copies of deleted data	Restricted from ordinary use; expire within 90 calendar days after production deletion, or earlier if legally required

Record class	Default period / treatment
Identifiable operational/security logs	Up to 180 calendar days rolling where necessary; after exit obey lawful deletion instructions unless specific permitted legal retention applies
Contract, invoice and payment administration records	Up to 7 years only to the extent necessary and lawful for legal/tax/claims purposes; retain only required fields, with annual review and earlier deletion when the purpose ends
Non-personal public DOI identity and minimal version/status markers	Persist while EMJ.LIFE is responsible publisher, subject to law and documented continuity arrangements
Personal history, Score/relationship records and evidence payload	No indefinite exception: apply the operational/deletion rules and specific lawful basis for any limited retained copy
Specific legal/regulator/dispute hold	Only necessary scope, restricted use, documented legal basis and end date or review at least every 90 days

The table is a contractual maximum/default framework, not a claim that every record is subject to a statutory seven-year minimum. A shorter mandatory deadline or lawful instruction takes priority. Where applicable law permits processor post-service retention only when required by law, that stricter rule applies. Any lawful agreed deviation must identify the class, purpose, basis, duration and approval in DPA Annex A.

14.2 Retained copies and confirmations

Retained copies remain access-restricted, confidential, secure and limited to their permitted purpose. Do not reintroduce deleted data from backups into active service; if needed for disaster recovery, reapply deletion/restriction before ordinary access. No general technical-recovery or Historical Records label authorises further retention.

Confirm production deletion within ten Business Days after its completion and confirm the backup deletion milestone within ten Business Days after completion. Identify any remaining lawful class, basis, restriction and expected deletion/review date. When a hold ends, delete or irreversibly anonymise the affected unnecessary data without undue delay.

14.3 Privacy-compatible history markers

Preserve an attributable minimal event/status marker where lawful to show correction, export, deletion, restriction or withdrawal. It may be non-identifying or irreversibly anonymised. No-silent-overwrite requirements do not compel retention of personal payload that must lawfully be erased, or continued disclosure of an unlawful prior version.

15. Correction and Version Governance

15.1 Correction request

The Enterprise may request correction of:

- Enterprise Input Data;
- Metadata relationships;
- version records;

- DOI Metadata;
- JSON delivery information;
- E-IPP Score history;
- EGC ID association;
- delivery records.

15.2 Correction procedure

EMJ.LIFE may:

- mark a record disputed;
- restrict use;
- create a corrected version;
- establish a supersession relationship;
- preserve the original;
- record the correction date;
- record the correction reason;
- update delivery or DOI status.

15.3 No silent overwrite

A correction shall not silently overwrite a prior record where the prior record is relevant to:

- Historical Records;
- evidence integrity;
- dispute resolution;
- legal retention;
- delivery history;
- continuity.

16. Enterprise Exit Obligations

Upon termination or expiry, the Enterprise shall:

- request required export within the Exit Period;
- protect exported files;
- maintain encryption keys;
- revoke former user access;
- delete or return EMJ.LIFE credentials;
- stop using Restricted or Inactive EGC IDs for new activity;
- stop representing inactive periods as continuous;
- comply with third-party confidentiality and data rights;
- pay applicable export or transition fees;
- provide reasonable cooperation for secure exit.

17. EMJ.LIFE Exit Obligations

Upon termination or expiry, EMJ.LIFE shall:

- restrict former user access;
- restrict or deactivate credentials;
- preserve authorised Historical Records;
- provide standard export;
- protect export files;
- apply deletion, anonymisation or archiving rules;
- maintain required legal-retention controls;
- prevent unauthorised post-termination access;

- maintain material delivery and version records;
- provide reasonable transition assistance where included or separately agreed.

18. Provider Discontinuation and Business Continuity Event

For planned discontinuation, give the MCT sixty-calendar-day notice where legally and practically possible; for an unforeseen inability, notify promptly with impact, available access and transition plan. Protect data, facilitate the included standard export, honour the 180-day exit window to the extent legally/technically available, and address registry/DOI continuity.

Unused prepaid service and paid undelivered Compendium remedies follow MCT Section 14 and CPS Section 18, with thirty-calendar-day refund/credit settlement where applicable. No unilateral credit substitutes for a required refund without Enterprise acceptance.

Any successor receives data only on lawful instructions/transfer safeguards and compatible obligations. Do not arbitrarily sell, publicly disclose or transfer confidential Enterprise history. Delivered-file licences survive; where original hosting cannot continue, preserve/export lawful minimal identity and version records and communicate the available successor or resolution arrangements.

19. Relationship with Other Documents

This Schedule governs:

- Enterprise Input Data rights;
- EMJ.NEXUS Metadata rights;
- export;
- Historical Records;
- EGC ID post-termination status;
- evidence continuity;
- deletion;
- anonymisation;
- archiving;
- DOI and delivery-record treatment;
- exit.

The DPA governs Personal Data Processing.

The Security Schedule governs security controls.

The SLA governs availability and support.

The E-IPP Policy governs Points and Score.

The Compendium Schedule governs Compendium-specific production and delivery.

The Master Commercial Terms governs general commercial terms, liability, confidentiality, intellectual property and dispute resolution.

20. Term and Survival

This Schedule begins when the applicable Enterprise Contract and Governance Pack becomes effective and continues while EMJ.LIFE provides EMJ.NEXUS or retains Enterprise Data or Historical Records.

The following obligations survive termination for as long as relevant:

- ownership;

- confidentiality;
- data protection;
- security;
- export;
- deletion;
- anonymisation;
- archiving;
- Historical Records;
- version governance;
- DOI status;
- delivery records;
- correction and supersession;
- legal retention;
- limitation of use;
- exit assistance.

21. Incorporation and Execution

This document is incorporated into the Agreement by the executed Enterprise Order Form identifying its controlled document ID, v1.0, issue date 12 October 2026 and subscriber release SR-20261014-01 based on CP-20261012-R03. The supplied release register identifies the applicable file fingerprints. Separate signatures on this document are not required, except the parties execute the Order Form by signature or recorded electronic acceptance under MCT Section 25.7. Party identity, both parties' authorised acceptance and the Contract Effective Date are recorded in the Order acceptance receipt. Annexes and express amendments are effective only under MCT Section 24; this template revision does not automatically amend an earlier executed Agreement.

Subscriber acknowledgement

☐ I have read and agree to the Data Rights & Exit Schedule, including ownership, delivered-file rights, lawful retention, export, deletion and exit rules.

This acknowledgement is recorded during Stage Two, separately from OF. Its document ID, version, Subscriber account, exact accepted version and actual time are linked to the Enterprise and EGC ID. All seven document acknowledgements and all fourteen required fields must be complete before the first 200 E-IPP Points are allocated. No separate signature or repeated corporate questionnaire is required for this document.

Stage Two completion and initial Points

All fourteen required fields in MCT Section 5.5 must be complete. D-U-N-S is the fifteenth, optional field. A permitted source-gap or tax-not-applicable resolution must be documented; unresolved or fabricated values do not satisfy a required field.

The first 200 E-IPP Points are allocated once only when cleared subscription payment, the correct Enterprise EGC ID, completion of all fourteen required profile fields, and the seven separate Stage Two document acknowledgements are recorded for the same Enterprise. The seven documents are MCT, DPA, SEC, SLA, DRE, EIPP and CPS.

Acceptance of OF alone does not satisfy this gate. D-U-N-S is optional and is excluded from the required-field and document checks.

The fourteen-field completion result and each of the seven document acknowledgements are recorded separately and linked to the same Enterprise. All must be complete, with cleared payment and EGC ID, before the once-only initial allocation. OF acceptance does not substitute for the seven acknowledgements. Point usability and service/task activation remain governed by their separate conditions.