

EMJ.NEXUS Data Processing Addendum

Subscriber Reading Edition SR1 | EMJ-NEXUS-DPA-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 DPA governs the processing of Enterprise Personal Data by EMJ LIFE HOLDINGS PTE. LTD. in connection with EMJ.NEXUS. This DPA 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;
- Security Schedule;
- Service Level Agreement;
- Data Rights & Exit Schedule;
- applicable written amendments.

This DPA applies to Personal Data processed by EMJ.LIFE on behalf of the Enterprise. This DPA does not transfer ownership of:

- Enterprise Input Data;
- Enterprise Personal Data;
- EMJ.NEXUS Metadata;
- platform schemas;
- governance models;
- system or technical Metadata;
- EMJ.LIFE intellectual property.

2. Definitions

2.1 Enterprise Personal Data

“Enterprise Personal Data” means Personal Data submitted, uploaded, linked, created, authorised or otherwise made available by or on behalf of the Enterprise for processing through EMJ.NEXUS.

2.2 Personal Data

“Personal Data” means information relating to an identified or identifiable natural person, or equivalent information protected under applicable data-protection law.

2.3 Data Subject

“Data Subject” means an identified or identifiable natural person to whom Personal Data relates.

2.4 Processing

“Processing” includes collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing, making available, aligning, combining, restricting, deleting, anonymising or otherwise handling Personal Data.

2.5 Personal Data Breach

“Personal Data Breach” means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Enterprise Personal Data.

2.6 Sub-processor

“Sub-processor” means a third party appointed by EMJ.LIFE to process Enterprise Personal Data on behalf of the Enterprise.

3. Roles of the Parties

3.1 Enterprise role

Except where the applicable Order Form or law expressly provides otherwise, the Enterprise acts as the:

- Controller;
- Organisation;
- Business;
- or equivalent decision-maker;

for Enterprise Personal Data. The Enterprise determines:

- purposes of Processing;
- categories of Personal Data;
- categories of Data Subjects;
- lawful basis or legal authority;
- retention and deletion requirements;
- permitted users and roles;
- geographic, sectoral and regulatory restrictions.

3.2 EMJ.LIFE processing role and separate administration

For Enterprise Personal Data processed on the Enterprise's documented instructions, EMJ.LIFE is the Processor, Data Intermediary or equivalent service provider and remains subject to this DPA. Creating Metadata, governing an Evidence Object, or holding a delivery record does not transfer ownership or remove Personal Data protection.

For its own applicant identity/KYB, contact authority, fraud-prevention, contract and billing administration, EMJ.LIFE independently determines the necessary purposes and means and acts in the corresponding controller/organisation role. Before collection, it shall provide purpose, legal basis where required, recipients, retention, transfers and rights information, use only necessary business contact/identity information and provide the privacy intake infrastructure@emj.life. A processor-only instruction does not authorise unrelated administrative or commercial use.

Unaccepted applicant contact/KYB records are deleted or irreversibly anonymised within ninety calendar days after rejection or withdrawal, unless a documented legal obligation or lawful dispute/fraud hold requires necessary limited retention. Accepted contract/billing records follow Annex B's lawful retention rules. Independent

administration is not a licence to retain the Enterprise's entire operational dataset or train unrelated AI models.

Independent administration includes controlled invitation email/LEI association, legal-name matching, the Stage One public-reference query, necessary payment/EGC ID records and Stage Two profile administration under MCT Sections 5.1 to 5.7. Query public GLEIF reference data by necessary identifier; do not disclose invitation emails, tax identifiers, operating-profile payload or evidence merely to retrieve an LEI. Public-source status does not remove Personal Data duties for identifiable sole traders or contacts.

Give the applicable collection notice for supplementary operating addresses, jurisdiction-dependent tax identifiers, SICs/role selection and optional D-U-N-S. Separate public identity-source values, private contact/tax data, enterprise-supplied supplements and platform decision records. Optional D-U-N-S refusal does not prevent core subscription/profile completion or Points. A recipient/matching service receives data only within its actual lawful, disclosed role and rights; GLEIF, an LEI issuer or D&B is not automatically a processor Sub-processor.

4. Document Priority

Mandatory applicable law and binding regulator directions prevail. An executed amendment prevails only for the provisions it expressly identifies and may not remove mandatory legal protections.

For each subject, the DPA governs Enterprise Personal Data processing; the Security Schedule governs security baselines; the SLA governs platform availability, support and Service Credits; the Data Rights & Exit Schedule governs ownership, retained-deliverable rights and exit; the E-IPP Policy governs Points and Score; and the Compendium Schedule governs Compendium eligibility, production and delivery.

The Order Form specifies transaction facts, selected plan, fees, term, approved scope, processing annex and enhanced commitments. An ordinary Order Form field does not override those subject-specific protections. A deviation must identify the affected document and clause, state replacement wording and be signed by both authorised representatives as an express amendment. Subject-specific schedules otherwise prevail over the Master Commercial Terms; task and product documentation ranks last and cannot change fixed contractual rights.

The eight documents identified in the Order Form and release register constitute the package. References to later website content do not incorporate later material terms automatically.

No ordinary pricing, purchase-order condition or technical setting reduces the applicable DPA. A lawful processing-specific amendment must be expressly identified and signed; mandatory Data Subject rights and regulator authority remain unaffected.

5. Processing Instructions

5.1 Documented instructions

EMJ.LIFE shall Process Enterprise Personal Data only:

- to provide EMJ.NEXUS;
- to perform the Agreement;
- according to the Enterprise's documented instructions;
- to provide support, security, backup, export and exit;

- to prepare an authorised Compendium;
- to comply with applicable law.

Documented instructions may be contained in:

- this DPA;
- the Enterprise Order Form;
- authorised platform settings;
- implementation instructions;
- support instructions;
- written export or deletion requests;
- other written instructions from an authorised Enterprise representative.

5.2 Instruction conflict

EMJ.LIFE shall inform the Enterprise if EMJ.LIFE reasonably believes that an instruction infringes applicable data-protection law. EMJ.LIFE may suspend the affected Processing while the instruction is clarified where continued Processing could create material legal, security or privacy risk.

5.3 No unauthorised commercial use

EMJ.LIFE shall not:

- sell Enterprise Personal Data;
- rent Enterprise Personal Data;
- disclose Enterprise Personal Data for unrelated advertising;
- create a separate data product from Enterprise Personal Data;
- use identifiable Enterprise Personal Data to train a general-purpose AI model without the Enterprise's prior written authorisation;
- combine identifiable Enterprise Personal Data with another customer's data for an unrelated purpose;
- disclose Enterprise Personal Data except as permitted by this DPA or applicable law.

6. Processing Details

6.1 Subject matter and processing configuration

The processor subject matter is Enterprise-authorized account/user administration, Node and Mission records, Evidence Objects, file handling, governance relationships and ledgers, operational logging, support, security monitoring, backup/recovery, lawful export/deletion and an accepted Compendium. Independent applicant/KYB and billing administration is separately governed by Section 3.2.

Processing Annex A states the actual purpose, operations, data types, Data Subjects, frequency, locations, Sub-processors, permitted recipients, transfer safeguards and approved retention deviations for each transaction. It must be completed and effective before the first processor data transfer or activation. No region, cloud supplier, public release, sensitive-data approval or transfer mechanism is presumed by a blank field.

6.2 Duration

Processor protections apply from the first authorised receipt of Enterprise Personal Data and throughout all Processing, including return/export, restricted exit storage, backups and any lawfully retained copies. Termination of the Subscription does not terminate this DPA while Processing continues.

Processing ends only when all applicable copies have been returned and deleted or irreversibly anonymised, except strictly necessary lawful retained copies protected by

this DPA until their permitted retention ends. DRE Section 14 and Annex B supply the default return/deletion schedule. No contractual exit window delays a legally required earlier deletion.

6.3 Categories of Data Subjects

Depending on the Enterprise's configuration, Data Subjects may include:

- Enterprise administrators;
- Enterprise users;
- employees;
- officers and directors;
- contractors;
- suppliers;
- customers;
- business partners;
- Node contacts;
- Mission participants;
- representatives of other organisations;
- persons identified in documents or evidence materials;
- other persons whose Personal Data is submitted by the Enterprise.

6.4 Categories of Personal Data

Depending on the Enterprise's configuration, Enterprise Personal Data may include:

- name;
- job title;
- business contact details;
- business email;
- business telephone number;
- organisation and role;
- user identifier;
- account and authentication information;
- access logs;
- activity records;
- documents and attachments;
- statements, declarations and approvals;
- Node and supplier information;
- Mission and participation records;
- Evidence Object content;
- timestamps;
- version and relationship information;
- support correspondence;
- billing and transaction information;
- security and audit logs.

Where identifiable, these categories also cover invitation verification, LEI reference snapshots/corrections, operating business addresses, tax identifier type/number/jurisdiction, declared supply-chain roles and optional D-U-N-S matching records. Ordinary business addresses are distinguished from individual/device precise-location tracking; no such tracking, personal tax-document upload or identity-document collection is newly authorised by the profile fields.

6.5 Special categories and regulated data

The Enterprise shall not submit the following unless EMJ.LIFE has expressly approved the Processing in writing and the required safeguards are documented:

- health data;
- biometric data;
- government-issued identity documents;
- financial-account credentials;
- payment-card data;
- criminal-record data;
- children's data;
- precise location data;
- political, religious or similarly sensitive information;
- national-security information;
- export-controlled information;
- other regulated or special-category data.

7. Enterprise Obligations

The Enterprise shall:

- comply with applicable data-protection law;
- provide lawful and documented instructions;
- establish and document the lawful basis;
- provide required notices;
- obtain required consents or authorisations;
- ensure submitted Personal Data is relevant and proportionate;
- avoid unnecessary Personal Data;
- maintain accuracy where accuracy is its responsibility;
- establish retention and deletion requirements;
- manage users and access;
- revoke access when no longer required;
- respond to Data Subject requests where required;
- assess cross-border Processing;
- ensure third-party and Node data may lawfully be submitted;
- not use EMJ.NEXUS as a substitute for legal, regulatory, medical, financial or professional advice.

8. EMJ.LIFE Obligations

EMJ.LIFE shall Process Enterprise Personal Data only on lawful documented instructions or a binding legal requirement; maintain the mandatory SEC safeguards; ensure personnel confidentiality and least-privilege access; keep required Processing and Sub-processor records; assist with Data Subject requests, breach assessment, legally required impact assessments and regulator consultation; notify under Section 11; and support lawful return, deletion and exit.

Where law requires processing beyond instructions, it shall notify the Enterprise before processing unless prohibited. It shall inform the Enterprise if an instruction appears to infringe applicable data-protection law. It shall not sell/rent Personal Data or use identifiable Enterprise data for unrelated marketing, a separate data product or general-purpose model training without the required lawful basis and expressly authorised scope. It remains responsible for appointed Sub-processor obligations under Section 13.

9. Confidentiality and Personnel

EMJ.LIFE shall ensure that personnel authorised to Process Enterprise Personal Data:

- are bound by confidentiality obligations;
- receive appropriate data-protection and security guidance;
- access data only as necessary;
- comply with EMJ.LIFE policies;
- lose access when authorisation ends.

Confidentiality obligations survive the end of employment, engagement, access or the Subscription.

10. Technical and Organisational Measures

The mandatory minimum measures are those in SEC Sections 3 to 10, including privileged MFA, role-based access and tenant isolation, encryption in transit and at rest, controlled keys, protected logs, vulnerability management, backup/recovery, incident response, secure changes, staff confidentiality and deletion/retention controls.

Annex A identifies any lawfully agreed enhancement or equivalent-control exception. No exception is implied by technology limitations. Before processor activation, EMJ.LIFE records verification that the applicable baseline and any agreed enhancements are operational. This is a contractual duty, not a claim that an audit, certification or technical assessment has already occurred.

11. Personal Data Breach

11.1 Breach notification trigger and progressive information

EMJ.LIFE shall notify the Enterprise without undue delay after becoming aware of a Personal Data Breach affecting Enterprise Personal Data. Where applicable law uses credible grounds to believe a breach occurred, notification starts from that threshold and shall not await final confirmation, root-cause completion or a materiality classification.

The initial notification may be preliminary. It shall provide available incident nature, affected data/system categories, approximate affected persons/records where known, likely consequences, containment/remediation, relevant times, contact and recommended actions. Missing details shall be supplied progressively without undue delay. The Enterprise's intake contact is in the Order Form; EMJ.LIFE's intake is infrastructure@emj.life.

This processor-to-Enterprise obligation is separate from any regulator or Data Subject notification deadline. The Agreement does not treat a controller's regulatory deadline as a permission for the processor to delay its own notice.

11.2 Cooperation

EMJ.LIFE shall reasonably cooperate with the Enterprise regarding:

- containment;
- investigation;
- risk assessment;
- regulatory notification;
- Data Subject notification;
- remediation;
- evidence preservation;

- post-incident review.

EMJ.LIFE is not required to disclose information that would:

- compromise security;
- disclose another customer's confidential information;
- waive legal privilege;
- violate law;
- materially increase the risk of further harm.

11.3 Enterprise notification responsibility

The Enterprise is responsible for determining whether it must notify:

- regulators;
- Data Subjects;
- customers;
- employees;
- suppliers;
- public authorities;
- other affected parties.

Unless instructed or legally required, EMJ.LIFE shall not contact Data Subjects or regulators on the Enterprise's behalf.

12. Data Subject Rights

12.1 Timely rights and compliance assistance

EMJ.LIFE shall assist access, correction, deletion, restriction, objection, portability and processing-information requests, and required impact assessment/regulator consultation, considering the nature of Processing and information available. It shall acknowledge a complete verified request within two Business Days and provide available relevant assistance within five Business Days, or sooner when the Enterprise identifies an applicable earlier legal deadline.

Verification and scope shall be proportionate. Unpaid disputed fees or an inactive account do not permit refusal of legally required assistance. Bespoke work may be separately priced only if lawful, disclosed and agreed, and shall not delay a mandatory response.

12.2 Direct requests

If a Data Subject contacts EMJ.LIFE directly concerning Enterprise Personal Data, EMJ.LIFE shall, where legally permitted:

- direct the Data Subject to the Enterprise;
- notify the Enterprise;
- avoid substantive response unless instructed or legally required;
- provide reasonable assistance.

12.3 Verification

EMJ.LIFE may require reasonable information to verify requests and protect:

- the Data Subject;
- the Enterprise;
- other Data Subjects;
- confidential information;
- security;
- legal rights;

- third-party data.

13. Sub-processors

13.1 Specific initial list and general change authorisation

The Enterprise authorises only the Sub-processors identified in the completed Annex A for their stated functions and locations. For later additions/replacements, the Enterprise gives general authorisation subject to prior information, the objection right and the safeguards in Sections 13.2 and 13.3. A category such as hosting or email is not itself an identification of a supplier.

The list shall distinguish a processor Sub-processor from an independent payment/KYB/publication recipient and identify its actual role. No AWS, payment provider, AI vendor or DOI agency is presumed to act as a Sub-processor merely because a commercial arrangement exists.

13.2 Sub-processor requirements and change notice

EMJ.LIFE shall contractually impose data-protection and security obligations no less protective for the delegated Processing, perform supplier assessment, limit access and remain responsible for performance of those obligations as required by law and this DPA.

It shall maintain and provide the current legal name, function and Processing locations for each Sub-processor. Additions or replacements require at least thirty calendar days' written notice before the new supplier receives Enterprise Personal Data. If urgent protective substitution is legally necessary, notify as early as practicable, explain why the normal period cannot be observed, and apply the same safeguards and objection/remedy process; no emergency exception creates an unlawful transfer.

13.3 Objection and affected-service remedy

The Enterprise may object on reasonable data-protection grounds within ten Business Days after receiving the supplier change notice. EMJ.LIFE shall address the objection before the proposed transfer, using an acceptable alternative, effective additional safeguards or exclusion of the affected Processing.

If no lawful reasonable solution is agreed, the Enterprise may terminate only the affected service before the change takes effect and receive its unused prepaid fees within thirty calendar days under MCT Section 14(c). The new supplier shall not receive the affected data while the objection remains unresolved unless the Enterprise expressly accepts a lawful alternative. Mandatory law and binding emergency directions prevail.

14. International and Cross-Border Transfers

14.1 Approved cross-border Processing

Enterprise Personal Data may be stored, accessed or transferred across borders only at the locations and to the recipients identified in Annex A, on documented instructions and with the actual safeguards required by applicable law. Remote support access is included in this assessment. A general global-service statement is not approval of every jurisdiction.

For Singapore-regulated transfers, EMJ.LIFE shall provide the legally required comparable protection. Where GDPR or another transfer regime applies, an applicable adequacy basis or valid transfer safeguard must be documented before transfer;

contractual clauses, assessments and supplementary controls are attached when required. No uncompleted annex or generic list of possible mechanisms substitutes for the actual arrangement.

14.2 Transfer safeguards

Where required, the parties shall implement appropriate safeguards, which may include:

- contractual transfer clauses;
- adequacy decisions;
- binding corporate rules;
- approved certifications;
- transfer-impact assessments;
- supplementary technical or organisational measures.

14.3 Transfer information and changes

Annex A identifies exporter/importer roles, approved countries, onward access, the selected legal transfer basis, required executed instrument and relevant supplementary safeguards. EMJ.LIFE provides updated information and material-risk changes promptly. A new material location/recipient requires the Section 13 notice/objection process and any required transfer amendment before the transfer. If safeguards cease to be lawful, suspend the affected transfer and promptly agree a lawful alternative or the affected-service exit remedy.

15. Government and Law-Enforcement Requests

If EMJ.LIFE receives a legally binding request for Enterprise Personal Data, EMJ.LIFE shall, unless prohibited by law:

- notify the Enterprise before disclosure;
- provide reasonable details;
- direct the requester to the Enterprise where appropriate;
- limit disclosure to the legally required scope;
- challenge or narrow the request where reasonably available;
- maintain confidentiality.

EMJ.LIFE need not notify the Enterprise where prohibited by law or where notification would create a material security or legal risk.

16. Audit and Compliance Assistance

16.1 Information

EMJ.LIFE shall make available information reasonably necessary to demonstrate compliance with this DPA, subject to:

- confidentiality;
- security;
- protection of other customers;
- privilege;
- trade secrets;
- availability of relevant information;
- reasonable frequency and scope.

16.2 Audit and inspection rights

EMJ.LIFE shall allow and contribute to a reasonable audit or inspection by the Enterprise or an independent auditor bound by confidentiality, including to verify compliance with this DPA. Ordinarily this is no more than once in twelve months with ten Business Days' notice during business hours, using relevant existing assurance information first where sufficient.

Additional or urgent review is permitted for a material breach, reasonable suspected non-compliance, regulator requirement or mandatory law. Frequency/notice limits do not obstruct statutory audit rights. Access shall protect other customers and security, but those protections do not justify withholding information necessary to demonstrate the applicable obligations. Each party bears its ordinary costs; EMJ.LIFE bears reasonable corrective verification costs if its material non-compliance is established.

16.3 Audit limitations

An audit shall not:

- disrupt EMJ.LIFE operations;
- access another customer's data;
- create a security vulnerability;
- expose unrelated confidential information;
- require source code or trade secrets;
- duplicate a recent independent audit without material reason.

The Enterprise is responsible for its audit costs unless applicable law provides otherwise.

17. Data Retention, Return and Deletion

17.1 During the Subscription

EMJ.LIFE shall retain Enterprise Personal Data only for as long as necessary to:

- provide the service;
- follow instructions;
- maintain security;
- support continuity;
- preserve required records;
- resolve disputes;
- comply with law.

17.2 Return and deletion

At termination the Enterprise chooses lawful return/export and deletion under DRE Sections 10 and 14. The default request window is 180 calendar days, but an earlier instruction or legal requirement prevails. Production copies are deleted or irreversibly anonymised within thirty calendar days after a verified deletion instruction or expiry of the Exit Period, whichever triggers the process first, subject only to permitted retention under Section 17.3. Isolated backups expire under the maximum ninety-calendar-day deletion cycle stated in DRE Section 14.

EMJ.LIFE provides a deletion confirmation within ten Business Days after completing the applicable production or backup deletion milestone, identifying any remaining lawful retained classes, basis, restriction and review/end date. Standard return/deletion is included; legally required rights are not conditioned on purchasing professional services.

17.3 Limited lawful retention

Retention of Enterprise Personal Data after the agreed Processing ends is permitted only as required or otherwise expressly permitted by applicable law and compatible with the parties' roles. An IP claim, evidence-integrity label or generic Historical Records duty is not an independent exception to a legal deletion duty.

Any retained copy must have a documented lawful basis, specific purpose, data minimisation, restricted access, retention/end or review date and deletion process. Where applicable law permits retention only because a law requires it, that stricter rule applies. Necessary independent contract/billing records under Section 3.2 are distinguished from processor evidence payloads. Expired holds are reviewed and removed without undue delay; retained data is not used for unrelated commercial Processing.

17.4 Historical Records and Personal Data protection

Valid record history may be preserved only within lawful retention and permitted purpose. Enterprise Personal Data in Metadata, identifiers, Score history or a delivery record remains Personal Data where identifiable, regardless of claimed IP ownership.

Where deletion is required, preserve only a lawful minimal non-identifying event marker or status/tombstone when appropriate. Temporary suspension, service exit and subsequent reactivation follow the DRE and E-IPP Policy and do not remove continuing DPA protection.

A LEI-state or profile restriction does not itself authorise permanent personal-record retention or erase correction/deletion rights. Preserve only lawful necessary source/query, invitation, completion, allocation and restriction history under this DPA and DRE. Correct inaccurate administrative supplements separately from immutable source snapshots and refresh the current value through a recorded process.

18. Data Rights and EMJ.NEXUS Metadata

18.1 Enterprise rights

The Enterprise retains its pre-existing rights in Enterprise Input Data and Enterprise Personal Data submitted by or on behalf of the Enterprise.

18.2 EMJ.LIFE rights

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 and delivery Metadata;
- technical and system Metadata;
- configuration and product information.

18.3 No implied transfer

Nothing in this DPA transfers to the Enterprise:

- EMJ.NEXUS software;

- EMJ.NEXUS Metadata;
- governance models;
- scoring or calculation models;
- platform architecture;
- technical implementation;
- trade secrets;
- product intellectual property.

19. De-Identified and Aggregated Information

EMJ.LIFE may create and use information that is:

- irreversibly anonymised;
- no longer reasonably capable of identifying a Data Subject or Enterprise;
- aggregated so that the Enterprise and Data Subjects are not reasonably identifiable.

Such information may be used for:

- security;
- reliability;
- product improvement;
- operational analysis;
- statistical reporting;
- capacity planning;
- benchmarking;
- research;
- fraud and abuse prevention.

EMJ.LIFE shall not use identifiable Enterprise Personal Data for these purposes unless authorised by the Enterprise or permitted by law.

20. Artificial Intelligence and Automated Processing

EMJ.LIFE shall not use identifiable Enterprise Personal Data to train a general-purpose AI model or unrelated commercial model without the Enterprise's prior written authorisation. EMJ.LIFE may use automated tools for:

- security detection;
- document classification;
- Metadata extraction;
- duplicate detection;
- workflow routing;
- quality control;
- service operations;
- support triage.

The Enterprise remains responsible for reviewing outputs used in:

- legal decisions;
- regulatory submissions;
- accounting;
- assurance;
- employment;
- credit;
- supplier;
- other material decisions.

EMJ.NEXUS outputs do not constitute legally binding automated decisions unless expressly agreed in writing and lawfully implemented.

21. Personal Data in Evidence Materials

The Enterprise shall ensure that evidence materials:

- contain only necessary Personal Data;
- do not include unnecessary sensitive data;
- are lawfully collected;
- may lawfully be provided to EMJ.LIFE;
- may be processed for the stated Mission or Evidence Object;
- may be included in an authorised Compendium;
- may be made available under the selected DOI access status.

The Enterprise shall identify materials requiring:

- redaction;
- masking;
- restricted access;
- additional approval;
- exclusion from public or controlled publication;
- separate retention;
- enhanced security.

22. Liability and Relationship with Other Documents

Liability for data-protection breaches is governed by the Master Commercial Terms, subject to mandatory law. Nothing in this DPA:

- limits mandatory Data Subject rights;
- removes regulator authority;
- permits unlawful Processing;
- transfers the Enterprise's responsibility for its data and instructions;
- makes EMJ.LIFE responsible for the Enterprise's independent compliance obligations.

The Security Schedule governs technical and organisational controls. The Data Rights & Exit Schedule governs export, Historical Records, termination and exit. The SLA governs availability and operational commitments.

23. Term and Survival

This DPA is incorporated when the Order Form becomes effective and applies from first authorised processor receipt through final return/deletion, restricted backup storage and all lawfully retained processor copies. Independent administrative Processing is governed by Section 3.2 and the applicable notice/law.

Confidentiality, security, purpose limitation, assistance, breach cooperation, audits, deletion, lawful retention and Data Subject/regulator rights continue for all retained Enterprise Personal Data. No earliest-of service end clause shortens this protection.

24. 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.

A Processing Disclosure Record Annex A

EMJ.LIFE populates and presents this Processing Disclosure Record and effective required transfer instruments before the first processor transfer or activation. The Enterprise reviews its actual instructions and accepts the DPA at Stage Two; the provider verifies its actual recipients and controls. The Subscriber is not required to fill the provider's infrastructure or transfer facts. Missing mandatory disclosure is resolved before the applicable processing is enabled.

Mandatory configuration	Completed transaction record
Enterprise legal name / Order reference	Populated from the verified Enterprise and accepted Order Summary.
Controller/processor roles and applicable jurisdictions	Disclosed by EMJ.LIFE for the contracted processing and confirmed by the Enterprise.
Purpose, service functions and Processing operations	Disclosed for the selected service scope; unrelated uses are excluded.
Data Subject categories and data types; exclusions	Presented for the actual processing scope and Enterprise instructions.
Frequency: ongoing/event-based; approved scope	Provider-supplied processing frequency and approved scope.
Hosting/storage country and actual region/system	Actual provider-supplied countries, regions and systems, disclosed before processing.
Backup country/region and retention cycle	Actual provider-supplied backup locations and retention cycle.
Remote support/access countries and roles	Actual support/access countries and roles disclosed by EMJ.LIFE.
Each Sub-processor: legal name, function, country	Actual named Sub-processors, their functions and relevant countries.
Independent recipients: role and necessary data	Actual independent recipients, roles and necessary data; distinguished from Sub-processors.
Permitted transfers; exporter/importer; legal basis	Applicable transfer parties, destinations and lawful mechanism.
Required executed transfer clauses/assessment/control references	Effective transfer clauses and required assessment/control references.
Sensitive/regulated data: not approved unless written scope	None unless expressly authorised
Retention: Annex B defaults; lawful deviations	Annex B baseline; each expressly accepted lawful departure identified separately.
Enterprise privacy/security contact	Confirmed contact from the authorised Enterprise account.
Provider verification reference / authoriser / date	Provider-generated verification record with authoriser and actual date.
Enterprise instruction approval / signatory / date	Authenticated instruction approval and actual acceptance record.

Annex changes follow DPA Sections 13 and 14 and MCT Section 24. This annex does not presume a third-party agreement, certification or API implementation.

B Retention Annex B: default schedule

The retention/deletion table in DRE Section 14 is incorporated as the operative default schedule. An earlier mandatory legal deadline or lawful controller instruction prevails. Any longer processor retention requires a lawful basis and the specific written amendment/instruction recorded in Annex A. Expired backup copies may not be restored into active use; if disaster recovery restores data marked for deletion, the deletion instruction is reapplied before ordinary access resumes.

Subscriber acknowledgement

☐ I have read and agree to the Data Processing Addendum within its stated scope and have reviewed the applicable Processing Disclosure Record provided at Stage Two. Processor workflows begin only after this acknowledgement and the required processing/transfer documents are effective.

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.