Data Protection Impact Assessment (DPIA) Template

This template implements GDPR Art. 35 (Data Protection Impact Assessment) for any processing activity carried out by Mabble Helix that is "likely to result in a high risk to the rights and freedoms of natural persons." The template follows the structure recommended by the Article 29 Working Party Guidelines on DPIA (WP248 rev.01).

A DPIA is mandatory under Art. 35(3) where the processing involves:

1. Systematic and extensive evaluation of personal aspects (profiling) producing legal or similarly significant effects;
2. Processing on a large scale of special categories of data (Art. 9) or data relating to criminal convictions and offences (Art. 10);
3. Systematic monitoring of a publicly accessible area on a large scale.

A DPIA is also required where two or more of the WP29 nine criteria apply (evaluation or scoring, automated decision-making with legal effect, systematic monitoring, sensitive data, large scale, matching or combining datasets, vulnerable data subjects, innovative use or applying new technological or organisational solutions, prevents data subjects from exercising a right or using a service).

How to use this template

1. Open this file. Save a copy with a descriptive name to `internal/compliance/dpias/YYYY-MM-DD-<short-slug>.md` (create the directory on first use).
2. Fill each section in order. Do not skip §1 (description) before §3 (risk assessment) - the risk analysis depends on the description.
3. Where a section is "Not applicable," say so and state the reason; do not delete the section.
4. Cite primary controls by their identifier (R-Pn.nn) and link to the relevant source files in the Helix repository.
5. Submit the completed DPIA to the Compliance Office (sales@mabble.ai) for review. The DPO consultation evidence (§5) must be captured before the processing starts.
6. Re-run the DPIA when the processing materially changes or at least every two years.

---

§1. Description of the Processing

1.1 Identity and contact details of the Controller and Processor

Role	Entity	Contact

Controller	<fill in: customer organisation>	<fill in>
Processor	Mabble, Inc. (d/b/a "Helix")	sales@mabble.ai
Joint Controller (if any)	<fill in or N/A>	<fill in or N/A>
Sub-processor(s) involved	<list from `internal/compliance/vendor_risk_matrix.md`>	<fill in>

1.2 Nature, scope, context, and purposes of the processing

Field	Value
Activity name	<fill in>
Internal reference	<fill in: e.g., processing-2026-NN>
Purpose of processing (HIPAA TPO / GDPR lawful basis / CCPA business purpose)	<fill in>
Lawful basis (GDPR Art. 6(1))	<a / b / c / d / e / f - choose one>
Special category lawful basis (Art. 9(2)) if applicable	<a / b / c / d / e / f / g / h / i / j - choose one or N/A>
Categories of data subjects	<e.g., patients, customer end-users, employees>
Categories of personal data	<e.g., identifiers, health data, financial, biometric>
Special categories of data (Art. 9)	<yes / no - if yes, enumerate>
Children's data involved (Art. 8 GDPR, COPPA US)	<yes / no>
Volume (records)	<fill in>
Volume (data subjects)	<fill in>
Geography of data subjects	<fill in>
Geography of processing	<fill in: us-east-1 default; eu-west-1 for EU residency>
Retention period	<fill in: must align with `purge_after` field on records>
Anticipated start date	<fill in>
Anticipated end date or review date	<fill in>

1.3 Data flow

Describe how data enters Helix, how it is processed inside Helix, and how it leaves Helix. A diagram is recommended; if attached, reference the filename here.

Step	Source	Destination	Mechanism	Encryption	Audit
1. Ingest	<fill in>	Helix vault	<fill in: gRPC, REST, batch>	TLS 1.3 in transit; AES-256-GCM at rest	`internal/service/audit/...`
2. Storage	Helix vault	Helix vault	per-tenant DEK	AES-256-GCM	Merkle anchor
3. Access	Helix vault	Authorised principal	Capability token + RLS	TLS 1.3	`internal/service/capability/...`
4. Export (if any)	Helix vault	<fill in>	<fill in>	TLS 1.3 + AES-256-GCM	`internal/service/dsar/...`

5. Destruction	Helix vault	n/a	Crypto-shred (R-P1.13)	n/a	Audit event

1.4 Assets supporting the processing

Asset	Description	Owner
Helix API (gRPC + REST)	Customer-facing data plane	Mabble
Helix database (PostgreSQL)	Encrypted vault store, RLS-enforced	Mabble (on AWS RDS)
Helix audit pipeline	Outbox + NATS + Merkle chain + Sigstore Rekor anchor	Mabble
Customer identity provider	Federation source	Customer
Sub-processors	See `internal/compliance/vendor_risk_matrix.md`	Listed individually

---

§2. Necessity and Proportionality

2.1 Lawful basis (GDPR Art. 6)

Cite the specific lawful basis, the recital that supports it, and the evidence that the basis was assessed before processing started.

Lawful basis	Selected	Reasoning
(a) Consent	<yes / no>	<fill in. Note CMP consent receipt ID if (a).>
(b) Contract	<yes / no>	
(c) Legal obligation	<yes / no>	
(d) Vital interests	<yes / no>	
(e) Public task	<yes / no>	
(f) Legitimate interests	<yes / no>	If (f), include the balancing test.

2.2 Special-category lawful basis (Art. 9) - if applicable

Basis	Selected	Reasoning
(a) Explicit consent		
(b) Employment / social security / social protection		
(c) Vital interests where data subject incapable		
(d) Not-for-profit		
(e) Manifestly made public by data subject		

(f) Legal claims		
(g) Substantial public interest		
(h) Preventive / occupational medicine, diagnosis		
(i) Public health		
(j) Archiving, scientific or historical research, statistical purposes		

2.3 Data minimisation

State which categories of data are processed and justify why each is necessary. Identify any category that could be removed without defeating the purpose.

Category	Necessary?	Justification
<e.g., date of birth>	<yes / no>	<fill in>
<e.g., government-issued ID>	<yes / no>	<fill in>

2.4 Accuracy

State the mechanism for keeping data accurate and up to date (Art. 5(1)(d)). Helix supports correction via the DSAR rectification path (Phase 1-1.7).

2.5 Storage limitation

State the retention period (Art. 5(1)(e)) and the trigger for destruction. Default Helix retention: per-record `purge_after`; audit log 7 years (S3 Object Lock COMPLIANCE).

2.6 Transparency

State the Privacy Notice URL and the consent receipt mechanism (Phase 2 + Phase 3).

2.7 Rights of data subjects

Right	Supported?	Mechanism
Access (Art. 15)	Yes	DSAR workflow
Rectification (Art. 16)	Yes	DSAR workflow
Erasure (Art. 17)	Yes	Crypto-shred (R-P1.13)
Restriction (Art. 18)	Yes	DSAR workflow
Portability (Art. 20)	Yes	DSAR export
Objection (Art. 21)	Yes	DSAR workflow
Not subject to automated decision (Art. 22)	<yes / no>	

2.8 Schrems II - international transfers

If the processing involves a transfer of personal data out of the EEA / UK, complete the transfer impact assessment below. If the data stays within the EEA / UK throughout, mark "No transfer" and skip.

Field	Value
Recipient country	<fill in>
Recipient	<fill in>
Adequacy decision exists?	<yes / no - if yes, cite>
If no adequacy: transfer mechanism	<SCC Module 2 / UK IDTA / BCRs / Art. 49 derogation>
Supplementary measures (technical, organisational, contractual)	<fill in>
Government access risk assessment (Schrems II §§94-101)	<fill in>
Conclusion	<transfer is / is not permitted under Schrems II framework>

---

§3. Risk Assessment

3.1 Identification of risks to data subjects

Use the WP29 high-risk indicators (WP248 rev.01) and the harm typology below.

Risk ID	Threat	Affected data subjects	Likelihood (1-5)	Severity (1-5)	Inherent risk (LxS)
R1	Unauthorised access by a Helix sub-processor	<fill in>	<fill in>	<fill in>	<fill in>
R2	Insider threat (Helix engineer)	All	<fill in>	<fill in>	<fill in>
R3	Data exfiltration via compromised customer credential	Customer's data subjects	<fill in>	<fill in>	<fill in>
R4	Data loss (availability)	All	<fill in>	<fill in>	<fill in>
R5	Data corruption (integrity)	All	<fill in>	<fill in>	<fill in>
R6	Excessive retention beyond stated purpose	<fill in>	<fill in>	<fill in>	<fill in>
R7	Unauthorised secondary use	<fill in>	<fill in>	<fill in>	<fill in>

R8	Disclosure to a sub-processor in a country lacking adequacy	<fill in>	<fill in>	<fill in>	<fill in>
R9	Failure to honour a DSAR within timing	<fill in>	<fill in>	<fill in>	<fill in>
R10	Failure to detect a breach within Art. 33 timing	<fill in>	<fill in>	<fill in>	<fill in>

3.2 Likelihood x Severity scale

Value	Likelihood	Severity
1	Negligible - would require an extraordinary combination	Negligible - no foreseeable impact
2	Limited - possible but unlikely	Limited - minor inconvenience
3	Significant - could occur once during the lifetime of the processing	Significant - material consequences (financial loss, distress, reputational harm)
4	Maximum - could occur within a year	Maximum - serious consequences (identity theft, loss of livelihood, discrimination)
5	Certain - already documented or recurring	Certain - irreversible severe consequences (loss of life, permanent discrimination)

Inherent risk = Likelihood x Severity. Treat any risk scoring >=15 as a Tier 1 risk requiring escalation. Treat any risk where Severity = 5 as Tier 1 regardless of likelihood.

3.3 Risk owners

Risk ID	Risk owner
R1-R8	Compliance Office + Engineering Lead
R9-R10	Compliance Office

---

§4. Mitigation Measures

For each risk identified in §3, document the mitigations in place and their residual effect.

4.1 Risk treatment table

Risk ID	Inherent risk	Existing controls (citations)	Additional controls planned	Residual risk

R1	<LxS>	Capability tokens server-side only, RLS + FORCE RLS on every PII table, per-tenant DEK, audit log with Merkle anchor (R-P0.07).	<fill in if applicable>	<LxS>
R2	<LxS>	Helix admin role separated from runtime; second-engineer signoff for security-sensitive changes; immutable audit log.	Quarterly access review (roadmap); EDR rollout (roadmap).	<LxS>
R3	<LxS>	WebAuthn / TOTP MFA; capability tokens scoped per RPC; session revocation <=5s via CAEP propagation.	Customer admin enforcement of MFA (already supported); anomaly detection (roadmap).	<LxS>
R4	<LxS>	AWS Multi-AZ; RDS encrypted snapshots; WAL-G PITR; SLO/SLI + alerts (R-P1.20).	Logged restoration drill in clean account (roadmap).	<LxS>
R5	<LxS>	AES-GCM authenticated encryption; optimistic concurrency `version` column; CSA-aligned input validation.	Server-side `vault.config` JSONB validation (gap G-1.1).	<LxS>
R6	<LxS>	`purge_after` field per record; per-jurisdiction retention enforcement (R-P1.14).	<fill in>	<LxS>
R7	<LxS>	`purpose_of_use` enum tag on every record + capability token; BAA §3 contractually prohibits secondary use; DPA Art. 28(3)(a) instruction-only processing.	<fill in>	<LxS>
R8	<LxS>	Per-tenant Data Residency Registry (DRS, R-P1.22); SCC Module 2 + Schrems II TIA.	<fill in>	<LxS>

R9	<LxS>	DSAR workflow (Phase 1-1.7) with explicit timing fields; jurisdictional clock (e.g., GDPR 30 days, CCPA 45 days).	<fill in>	<LxS>
R10	<LxS>	Breach incident workflow (R-P1.19) with regulatory deadline timers; runbook at `internal/compliance/breach_notification_runbook.md`.	<fill in>	<LxS>

4.2 Compensating controls

If any mitigation cannot be deployed, document the compensating control and the time-bound plan to remediate.

Risk ID	Gap	Compensating control	Remediation owner	Remediation due
<fill in>	<fill in>	<fill in>	<fill in>	<fill in>

---

§5. Residual Risk and DPO Consultation

5.1 Residual risk summary

Tier	Count	Notes
Tier 1 (>=15 or Severity=5)	<fill in>	Each Tier 1 residual risk requires DPO sign-off and may require Art. 36 prior consultation with the supervisory authority.
Tier 2 (9-14)	<fill in>	Documented and accepted by the Controller in writing.
Tier 3 (<9)	<fill in>	Standard operational risk.

5.2 DPO consultation

Field	Value
DPO consulted (Art. 35(2))	<yes / no>
DPO name	<fill in>
DPO position	<fill in>
Consultation date	<fill in>

DPO recommendation	<fill in>
Controller's response to the DPO recommendation	<fill in: accepted / accepted with modifications / rejected with documented reasoning>

5.3 Art. 36 Prior Consultation

If any residual risk is Tier 1 and cannot be reduced, prior consultation with the supervisory authority is required under Art. 36. Document the submission.

Field	Value
Prior consultation required?	<yes / no>
Supervisory authority	<fill in>
Submission date	<fill in>
Reference number	<fill in>
Authority response	<fill in>

5.4 Stakeholder consultation (Art. 35(9))

The Controller is required to seek the views of data subjects (or their representatives) where appropriate. Document the consultation or document the reason it was not sought.

Field	Value
Data subject consultation performed?	<yes / no>
Method (survey, advocacy group, public consultation)	<fill in>
Summary of views	<fill in>
Adjustments made in response	<fill in>
If not sought: reasoning	<fill in>

---

§6. Approval

6.1 Sign-off

Role	Name	Signature	Date
Author (DPIA owner)	<fill in>	<fill in>	<fill in>
Data Protection Officer	<fill in>	<fill in>	<fill in>
Compliance Office	<fill in>	<fill in>	<fill in>
Controller representative	<fill in>	<fill in>	<fill in>
Engineering Lead	<fill in>	<fill in>	<fill in>
Mabble engineering (executive owner)	<fill in>	<fill in>	<fill in>

6.2 Review cadence

Field	Value
Next review due	<fill in: at material change OR within 24 months, whichever earlier>
Triggers for re-DPIA	New category of data; new sub-processor; new jurisdiction; new lawful basis; new automated decision-making; data-volume material change

6.3 Archive

Filled DPIA committed to `internal/compliance/dpias/<filename>.md` with a corresponding entry in the change log of this template.

Change log

Version	Date	Change
0.1.0	2026-05-14	Initial Track C publication.