

GOVERNED TEMPLATE RENDERING REFERENCE: DATA CLASSIFICATION DEFAULT V2 (DRAFT)

definition f4f5c0be...66f8

DATA CLASSIFICATION · PROJECT ARTIFACT

SPECIRA

Data Classification: Dispatch Modernization

Meridian Field Services: instructional example, not project evidence

DRAFT · WATERMARK POLICY: DRAFT_ONLY

template data_classification v2 · pack: specira_default_delivery

the cluster's anchors resolve here: labels, fields, retention, bases

§1 Classification Labels & Handling Rules

mandatory

1 decision

1 evidence rule

validators: label_set_closed_three_to_four_tiers · handling_rules_defined_once_per_level · scheme_owner_and_change_rule_stated

A closed set with anchored definitions (what qualifies is decided by content, not by vibes) and the handling matrix defined ONCE per level. Rows everywhere else cite a level and inherit its rules; per-row handling prose is the drift this matrix kills.

Level	Anchor (what qualifies)	Example, this project
PUBLIC	Published service information	The customer-facing service catalog
INTERNAL	Operational data whose exposure inconveniences but does not harm	Reason-code meanings
CONFIDENTIAL	Business data whose exposure harms Meridian or a customer	Assignment history, job addresses
RESTRICTED	Personal data whose exposure harms a person	Technician location tracks

Level	Storage	Transit	Sharing	Display
PUBLIC	n/a	TLS	Open	n/a
INTERNAL	n/a	TLS	Staff	n/a

Level	Storage	Transit	Sharing	Display
CONFIDENTIAL	Encrypted at rest	TLS	Role need	n/a
RESTRICTED	Encrypted at rest	TLS; never leaves the residency region (data flow & privacy ^[1])	Named-role need only	Masked outside dispatch surfaces: positions render as bands, not coordinates, off the board

Owner & change rule: N. Duval; additions or redefinitions by governance decision only; the set stays closed so every citation elsewhere stays resolvable. Contested classifications escalate to N. Duval.

§2 PII Register

mandatory

1 decision

1 evidence rule

validators: every_pii_row_cites_data_model_field_id · special_category_column_present_with_explicit_values · register_and_schema_resolve_both_directions

Rows cite the data model's field ids; bare entity-and-field text is how registers rot. The data model's sensitivity-tag validator resolves against this register, both directions; a migration adding a personal field without a row here is a generation defect.

Field (cites data model)	Type	Level
<u>Position.lat, Position.lon</u> ^[2]	Location data	RESTRICTED
<u>Position.observed_at</u> ^[2]	Movement pattern, when joined	RESTRICTED by association
<u>Technician.name, Technician.hr_id</u> ^[2]	Identity	CONFIDENTIAL
<u>Job.address</u> ^[2]	Customer site: a customer's	CONFIDENTIAL

Field (cites data model)	Type	Level
	location, distinct from technician location	
<u>Assignment.reason_code, Assignment.note</u> ^[2]	Worker-conduct records, when joined with identity	CONFIDENTIAL

Special category: none in this project; the column says so explicitly, which is itself a claim.

Records of processing: the purpose, category, recipient, and retention columns compile the processing record once; no second inventory.

§3 Retention Rules

mandatory

1 decision

1 evidence rule

validators: every_retention_row_has_period_trigger_disposal_legal_hold · architecture_lifecycle_reconciles · rights_versus_holds_precedence_stated

"Keep for two years" is not executable without "from what, deleted how, unless what"; every row carries period, trigger, disposal, and the legal-hold override.

Data class	Period	Trigger (runs from)	Disposal	Legal hold	Authority
Positions	30 days	observed_at	Hard delete	Pauses deletion on N. Duval's written hold	Telemetry retention policy
Assignment history	7 years	creation	Archive at 1 year; delete at 7	Owner: N. Duval	Enterprise contract clause 14 (<u>contract extracts</u> ^[5])
Jobs	Archived with their assignments		Archive-then-delete	Follows assignments	Operations policy
Auth audit events	2 years	event time	Hard delete	Owner: N. Duval	The audit-record rule the auth

Data class	Period	Trigger (runs from)	Disposal	Legal hold	Authority
					policy cites (audit events ^[3])

Reconciliation: matches the architecture's per-entity lifecycle rows exactly ([data architecture^{\[1\]}](#)), checked, no divergence; a divergence is a defect, not a nuance. **Rights versus holds:** deletion requests yield to the contract-mandated assignment retention and to active holds; precedence stated, owner N. Duval.

§4 Lawful Basis & Consent Model

mandatory

1 decision

1 evidence rule

validators: every_purpose_names_lawful_basis · legitimate_interest_claims_carry_assessment · employment_notices_carry_owners

The basis is chosen per processing purpose; consent is not a reflex. Capture and withdrawal mechanics exist only where consent IS the basis; the consent form scales with sensitivity in the governing regime.

Processing purpose	Lawful basis (chosen)	Discipline it carries
Dispatch operations: jobs, assignments, positions	Contract performance + legitimate interest (field-service delivery)	Assessment attached for the location-tracking interest (legitimate-interest assessment^[5])
Override telemetry: reason codes, notes joined with identity	Legitimate interest under the collective agreement's monitoring clauses	Worker monitoring: the meaningful-notice obligation applies; the consent form scales with sensitivity in the governing regime (express versus implied); the dispatcher-facing notice is the open question the security requirements already track (§7), owner N. Duval
Marketing	No purpose exists (stated, so the absence is a decision)	

Consent-based purposes: none, so no capture-and-withdrawal mechanics are owed; recorded. Were consent ever the basis, capture is granular per purpose and withdrawal is as easy as giving; a consent checkbox without a withdrawal path fails review.

§5 Cross-Border Transfer Rules

conditional · OMITTED, with rationale

1 decision

1 evidence rule

validator: cross_border_rows_cite_mechanism_not_placement

Omission note: "cross_border_transfer omitted: processing is single-region; Restricted data never leaves the residency region by handling rule (§1), and no processor sits outside it; the model provider receives anonymized codes only, not personal data (SR-014^[4]). Residency placement is the architecture's (data flow & privacy^[1]). The trigger re-runs if a processor outside the region joins the integration register."

§6 Impact Assessment

conditional · trigger test FIRES, ENGAGED

1 decision

1 evidence rule

validators: dpia_trigger_test_always_runs · dpia_attachment_resolves_when_engaged

The trigger test always runs; only the assessment is conditional. Systematic monitoring of workers is the criterion that most often surprises delivery teams; it fires here.

Trigger test fires: **systematic monitoring of workers** (continuous location tracking of technicians during shifts). Other criteria: large-scale special-category processing, no; novel technology on personal data, no (the AI boundary receives anonymized codes only).

Assessment: attached (privacy impact assessment^[5]), summarized here, analysis in the attachment:

Question	Answer, citing its row
Necessity	Dispatch cannot assign on proximity without positions
Proportionality	30-day purge (§3) · band-level display off the board (§1) · no off-shift tracking
Risks to subjects	Re-identification of movement patterns, mitigated by SR-033, SR-034 ^[4] and the purge; the threat model carries the analysis row (TM-07 ^[6])
Residual risk	Signed by N. Duval , July 15, 2026

§7 Open Questions

mandatory

1 decision

Question	Owner	Answer by	Blocks
Does the dispatcher-facing monitoring notice require union co-signature before pilot start?	N. Duval	Aug 8, 2026	The override-telemetry

Question	Owner	Answer by	Blocks
Shared with the security requirements' question; tracked once, linked twice (open questions^[4])			purpose's notice text only

Refs

References & Package Contents

In this export package

package

[5] Contract extracts · legitimate-interest assessment · privacy impact assessment
./compliance/

In the Specira workspace

- specira
- [1] Architecture: data flow & privacy (residency placement), data architecture (lifecycle rows), system of record [app.specira.ai/projects/dispatch-modernization/artifacts/architecture](#)
- specira
- [2] Data model: field specifications the register cites, both directions [app.specira.ai/projects/dispatch-modernization/artifacts/data-model#fields](#)
- specira
- [3] Auth & authz policy: audit event set whose retention cites §3 [app.specira.ai/projects/dispatch-modernization/artifacts/auth-authz-policy#audit](#)
- specira
- [4] Security requirements: SR-014, SR-033, SR-034; shared open question [app.specira.ai/projects/dispatch-modernization/artifacts/security-requirements](#)
- specira
- [6] Threat model: TM-07 re-identification row [app.specira.ai/projects/dispatch-modernization/artifacts/threat-model#tm-07](#)