YARDtwin™
Digital yard management for pharma & supply chain

YARDtwin Vendor Assurance Pack

VENDOR ASSURANCE PACK

Everything a QA, IT-security, privacy or procurement reviewer needs to assess YARDtwin — in one document, before the review.

- QMS index · GAMP 5 categorisation · validation approach
- EU GMP Annex 11 and 21 CFR Part 11 clause mappings
- ALCOA+ statement · security architecture · completed CAIQ-Lite
- An explicit statement of what we do not yet hold

YT-VAP-001 · v1.0

27 July 2026

All control statuses verified against live production infrastructure on 27 July 2026.

Why this document exists

Vendor assurance normally happens the slow way. A pharmaceutical or logistics buyer decides to proceed, and only then does the supplier questionnaire arrive — forty tabs, six weeks, and a quality reviewer asking for a GAMP categorisation the vendor has never written down. The operational decision was made in week two; the assurance work runs until week fourteen.

We would rather hand it over first. This pack contains the answers we would otherwise send you one at a time: our quality-management document set, how we categorise and validate the platform, clause-by-clause mappings to EU GMP Annex 11 and 21 CFR Part 11, an ALCOA+ statement, our security and hosting architecture, a completed CAIQ-Lite, and a plain list of the controls we do not yet have.

> **On the honesty of this document**
> Every status below was verified against live production infrastructure and live source code on 27 July 2026, not copied from a previous document. Where a control is absent, partial, or planned, it is labelled that way — see §13 and §17. We hold neither SOC 2 Type II nor ISO 27001 today, and this pack says so on the page where a reviewer looks for it.

Where to start, by reader

Reader	Read these sections
Quality assurance / CSV	§3 QMS index · §4 GAMP 5 and validation · §5 Annex 11 · §6 Part 11 · §7 ALCOA+ · §8 data integrity
IT security	§2 hosting · §10 security architecture · §11 secure development · §12 CAIQ-Lite · §13 certifications · §14 continuity
Data protection / DPO	§9 GDPR and privacy · §2 residency · §9.4 sub-processors · §9.6 AI governance · §15 breach notification
Procurement / vendor risk	§13 certification status · §14 continuity · §16 responsibility split · §17 open items · §18 audit rights and contacts
In a hurry	Read §13 and §17. They contain everything that is not yet in place; the rest of the pack is what is.

Scope of this pack

This document describes the YARDtwin platform as operated by YARDtwin Ltd as a multi-tenant SaaS service, and the vendor-side controls that apply to it. It does not describe your instance configuration, your validation of that instance, or the process controls that remain yours — §16 sets out that split explicitly. It is offered for vendor-assessment purposes and is not a contractual warranty; contractual commitments live in the MSA and the Article 28 data processing agreement.

1. The service in GxP terms

YARDtwin is a multi-tenant SaaS yard-management platform for pharmaceutical manufacturing and GxP-regulated logistics. It governs the yard boundary: carrier appointment booking, gate check-in and check-out, seal verification, cold-chain verification at arrival and dispatch, weighbridge capture, dock scheduling and unload confirmation, a live digital twin of yard state, and a controlled departure-clearance release.

In GxP terms it is a **GxP-supporting computerised system**. It creates and retains records that support product-release and product-disposition decisions — gate events, seal chain of custody, temperature verification, departure clearance and their audit trail — but it does not itself perform batch certification or release. Annex 11 §15 (batch release) therefore applies to your process, with YARDtwin supplying evidence into it, not to YARDtwin as a release system.

26	Annex 11	EEA	10	0
languages	and 21 CFR Part 11	data residency	QMS documents	pen-test findings, Apr 2026

1.1 Records the platform creates

The following are treated as GxP-relevant and carry the full audit-trail and retention treatment described in §7 and §8:

- Gate entry and exit events, with vehicle, carrier, driver, purpose and controlled timestamps
- Seal verification records — expected value, verified value, outcome, and the retained seal image
- Cold-chain records — measured temperature, set point, logger evidence, in-range determination
- Weighbridge records — gross, tare and derived net, with the derivation method recorded
- Dock and unload records, including pallet or handling-unit scans
- Departure clearance and its electronic signature, with the meaning of signing and a hash chain
- GMP checklist responses configured per site, and any documented waiver with its reason
- The append-only audit trail covering every change to the above

2. Hosting, infrastructure and data residency

YARDtwin runs entirely on Microsoft Azure within the European Economic Area. There is no secondary hosting provider for customer data. The topology below was read from the live subscription on 27 July 2026.

Component	Service	Region
Application	Azure App Service, Linux container	Norway East
Database	Azure Database for PostgreSQL Flexible Server 15	Sweden Central
File and document storage	Azure Blob Storage, private containers only	Norway East
Secrets	Azure Key Vault, RBAC-controlled	Sweden Central
Container registry	Azure Container Registry	Sweden Central
Edge	Azure Front Door with WAF policy attached	Global anycast
Monitoring	Application Insights, Log Analytics, Microsoft Sentinel (90-day retention)	Norway East

2.1 Why "EEA" and not "EU"

Norway is a member of the European Economic Area, not the European Union. The GDPR applies in Norway through the EEA Agreement, so a transfer of personal data to Norway East is an intra-EEA transfer and requires no Chapter V transfer mechanism. We state "EEA" rather than "EU" because it is the accurate description; a reviewer who checks the region against a list of EU member states should not be left with a discrepancy to chase.

2.2 Residency is technically enforced, not only promised

An Azure Policy assignment at subscription scope (**yardtwin-eu-only-locations**, effect **Deny**, enforcement enabled) prevents the creation of resources outside the approved regions. This is a platform-level control, so residency does not depend on operator discipline: an attempt to provision customer-data infrastructure elsewhere fails at the control plane. The assignment can be evidenced on request.

Two sub-processors process limited data outside the EEA — see §9.4. Those transfers are governed by EU Standard Contractual Clauses, are minimised in scope, and in the case of AI document reading can be switched off per site (§9.6).

3. Quality management system

YARDtwin maintains a quality-management document set covering the platform lifecycle. The set below is complete as issued; it is offered to customers and prospective customers under a mutual non-disclosure agreement, in full, on request to **admin@yardtwin.com**.

#	Document	Code	Regulatory basis
1	GMP Audit Requirements Overview	YT-QMS-001	Annex 11, GAMP 5, 21 CFR Part 11
2	User Requirements Specification	YT-QMS-002	Annex 11 §4.4, GAMP 5 Ch. 6
3	Validation Plan	YT-QMS-003	Annex 11 §4, GAMP 5 Ch. 7
4	Risk Assessment (GAMP 5 / ICH Q9)	YT-QMS-004	Annex 11 §1, ICH Q9(R1)
5	System Architecture Document	YT-QMS-005	Annex 11 §4.3, §4.8
6	Access Control and Audit Trail SOP	YT-QMS-006	Annex 11 §9, §12; Part 11 §11.10(d),(e)
7	Data Integrity Policy (ALCOA+)	YT-QMS-007	Annex 11 §7, MHRA DI 2018
8	Change Control SOP	YT-QMS-008	Annex 11 §10, GAMP 5 Ch. 10
9	Incident and Deviation Management SOP	YT-QMS-009	Annex 11 §13
10	CAPA and Open Actions Register	YT-QMS-010	Annex 11, ISO 9001 principles

Document status — stated plainly

The ten documents above are issued at v1.0 with the status **draft for review** and QA approver assignment pending, reflecting that YARDtwin Ltd is a young company formalising a quality function. The controls they describe are implemented and verifiable in the running platform — that is what §5 to §11 of this pack evidence. What is outstanding is the formal approval signature, not the control. We would rather you learn this here than discover it in a document header.

3.1 Supporting operational documents

- **Records of Processing Activities** and a personal-data inventory (GDPR Art. 30)
- **Operational Qualification protocols** for discrete capabilities — for example a 24-case protocol for the Smart Slots scheduling engine and a 28-case protocol with traceability matrix for floor-level batch tracking
- **Penetration test plan** and the April 2026 test report
- **Patch and vulnerability management policy**, with a CVSS-to-SLA remediation table
- **Incident response runbook** with severity classification and a 72-hour breach commitment
- **Validation and configuration manuals** for integration surfaces, including a 45-page SAP EWM configuration and operations manual

4. GAMP 5 categorisation and validation approach

Attribute	Determination
GAMP 5 category	**Category 4 — configured software.** A commercial platform whose GxP-relevant behaviour is configured per site (gate methods and required fields, seal and temperature controls, scheduling rules, checklists, roles), with vendor-developed bespoke logic beneath it.
System type	GxP-supporting operational system — supply-chain and yard execution
GxP criticality	Records support product-release and disposition decisions; the system does not perform release
Data classification	GxP-relevant: gate events, seal chain, cold chain, weighbridge, departure clearance, audit trail
Regulatory frame	EU GMP Annex 11 · 21 CFR Part 11 · EU GDP guidelines · GDPR · MHRA data integrity guidance · ICH Q9(R1) · GAMP 5 2nd edition
Risk basis	Documented risk assessment (YT-QMS-004) using ICH Q9(R1) severity, probability and detectability; validation effort scaled to the resulting risk class

4.1 Lifecycle model

A V-model lifecycle, proportionate to the Category 4 determination. Requirements are documented in the URS (YT-QMS-002) and traced to test evidence; architecture and design qualification sit in YT-QMS-005; verification runs as automated regression in continuous integration plus discrete qualification protocols for GxP-relevant capabilities.

Phase	Vendor deliverable	Who executes
Planning	Validation Plan (YT-QMS-003)	YARDtwin
Requirements	URS (YT-QMS-002), traceable	YARDtwin, reviewable by you
Risk assessment	YT-QMS-004	YARDtwin; your instance risk is yours
Design qualification	System Architecture Document (YT-QMS-005)	YARDtwin
Installation qualification	IQ template and platform evidence	You, supported by us
Operational qualification	OQ protocols and test evidence	You, supported by us
Performance qualification	PQ scenario templates	You
Validation summary	Vendor evidence pack for your VSR	You
Periodic review	Annual platform review; change log for your review	Both

4.2 Continuous verification evidence

Because the platform ships changes continuously, verification is continuous. Every change runs against an automated suite that includes a full-lifecycle regression driving 500 vehicles through booking, gate, yard, dock and departure against a real database, plus end-to-end browser journeys, before it can reach production. Deployment to production is a separate, deliberately manual authorisation step — it cannot happen as a side effect of a merge. Release evidence for any given change can be produced on request under change control (§5, Annex 11 §10).

Validation evidence available today includes qualification runs of the SAP integration surface (a 20-delivery bi-directional message audit and a 50-test live conformance run), labour-capacity qualification with an

18-case scenario suite, and a 152-case full-platform validation. These are listed here as evidence that exists and can be requested — not as a substitute for your own instance qualification.

5. EU GMP Annex 11 — clause mapping

Every clause of Annex 11, with what YARDtwin does about it and where the evidence sits. Clauses that are partial or out of scope say so — §15 is genuinely out of scope, and §8, §11, §16 and §17 are partial.

Clause	Requirement	YARDtwin implementation	Evidence
§1	**Risk management applied across the lifecycle**	Documented risk assessment (YT-QMS-004) on ICH Q9(R1); validation and control effort scaled to risk class.	YT-QMS-004
§2	**Personnel — defined roles and responsibilities**	Validation, technical, product-owner and approver roles defined in YT-QMS-003 §5. Customer-side roles are yours to define.	YT-QMS-003 §5
§3	**Suppliers and service providers; supplier assessment**	This pack is written to support your Annex 11 §3.2 assessment of us. Our own infrastructure supplier (Microsoft Azure) and all sub-processors are registered in §9.4 with transfer safeguards.	This pack; §9.4
§4	**Validation, with a traceable URS and proportionate evidence**	V-model per §4 above; URS traced to test evidence; continuous automated regression plus discrete OQ protocols. Instance IQ/OQ/PQ is a joint activity.	YT-QMS-002/003; OQ protocols
§5	**Data — accuracy of data exchanged electronically**	Structured relational storage with referential integrity and field validation. Integration inputs are HMAC-signed and idempotent; unrecognised message types are rejected rather than partially applied.	YT-QMS-005/007
§6	**Accuracy checks for critical data entered manually**	Seal numbers are checked against an expected value from the booking; temperatures against a required range; weighbridge net against expected net with a variance flag above 5%. AI-extracted document fields are presented for human confirmation and are never committed unconfirmed.	Gate and departure workflows
§7	**Data storage — secure, accessible, with tested restore**	AES-256 encryption at rest in Azure PostgreSQL plus application-layer AES-256-GCM field encryption for sensitive personal fields; automated backups with 7-day point-in-time recovery. Restore testing and high availability: see §14 — HA is not currently enabled.	YT-QMS-007; §14
§8	**Printouts — clear printed copies of electronically stored data**	Records including their audit trail are displayed in human-readable form and can be printed from the application; electronic export is available in CSV and JSON. A dedicated per-record PDF printout with full context is on the roadmap (URNF-010, medium priority) and is **not** implemented today.	Partial — see §17
§9	**Audit trails — who, what, when, and the reason for change**	Append-only audit trail at the application layer: no route in the platform can update or delete an audit record. Each entry carries actor identity, action, entity, description, IP address, timestamp and a GxP-relevance flag; superseded values are retained. Verified by inspection of the codebase.	YT-QMS-006; §7
§10	**Change and configuration management**	All platform change runs through documented change control (YT-QMS-008) with peer review enforced on high-blast-radius paths, automated regression gating, staged deployment and a manual production authorisation. Customer-side configuration changes are themselves audited.	YT-QMS-008
§11	**Periodic evaluation of the validated state**	Annual platform review defined in YT-QMS-003 §8.2. The first formal cycle is scheduled; interim assurance comes from the continuous regression evidence in §4.2.	Partial — see §17

Clause	Requirement	YARDtwin implementation	Evidence
§12	**Security — access control, authorisation and segregation**	Unique named identities with no shared accounts; role-based authorisation checked at every endpoint; TOTP multi-factor enforced at login where enabled; SAML 2.0 single sign-on; SCIM 2.0 provisioning and deprovisioning; optional administrator IP allow-listing; account lockout; session expiry; tenant isolation enforced on every query.	YT-QMS-006; §10
§13	**Incident management**	Incident and deviation SOP (YT-QMS-009) with severity classification, investigation and CAPA; automated breach detection with alerting; 72-hour notification commitment (§15).	YT-QMS-009; §15
§14	**Electronic signature**	Departure clearance is released by an electronic signature that requires password re-authentication at the moment of signing, captures a mandatory meaning-of-signature statement, and stores a SHA-256 hash over a canonical payload that includes the signature image digest and the previous signature hash — a tamper-evident chain. See §6 for the Part 11 detail.	Implemented; §6
§15	**Batch release**	Out of scope for the platform. YARDtwin supplies gate, seal, cold-chain, weighbridge and clearance evidence into your release process; it does not certify or release batches.	Scope statement
§16	**Business continuity**	Automated backups, a staging slot, documented contingency for gate operation during unavailability. High availability is **not** enabled and RTO/RPO are internal targets rather than contractual commitments — stated fully in §14.	Partial — see §14, §17
§17	**Archiving — records readable and retrievable for their retention period**	Defined retention schedule per record class (§8), audit trail and metadata preserved with archived records, and a contracted data-portability route on exit. Automated enforcement of retention is partially implemented — see §8.2.	Partial — see §8.2

6. 21 CFR Part 11 — clause mapping

The controls of §11.10, the signature provisions of §11.50 and §11.70, and the electronic-signature requirements of §11.100, §11.200 and §11.300. Two rows are marked **Customer**: they are obligations that cannot be discharged by a vendor, and §11.100(c) in particular is the one most often left undone.

Clause	Requirement	Implementation	Status
§11.10(a)	Validation of systems for accuracy, reliability and consistent intended performance	V-model validation (§4) plus continuous automated regression including a 500-vehicle full-lifecycle suite gating every change.	Met
§11.10(b)	Ability to generate accurate and complete copies in human-readable and electronic form	Human-readable display and print of records with their audit trail; CSV and JSON export. Dedicated per-record PDF printout not yet implemented.	Partial
§11.10(c)	Protection of records to enable accurate retrieval throughout the retention period	Encrypted storage, automated backup with point-in-time recovery, defined retention schedule, append-only audit trail. Automated retention enforcement is partial (§8.2).	Partial
§11.10(d)	Limiting system access to authorised individuals	Unique identities, role-based authorisation on every endpoint, MFA, SSO, SCIM lifecycle, optional admin IP allow-listing, lockout after repeated failures, enforced tenant isolation.	Met
§11.10(e)	Secure, computer-generated, time-stamped audit trails	Append-only audit trail; no update or delete path exists in the application; retains previous values and change reason; GxP-relevance flagged; timestamps server-generated in UTC.	Met
§11.10(f)	Operational system checks to enforce permitted sequencing	The gate, dock and departure workflows enforce order — for example seal verification before unload, and a completed clearance before a departure signature is accepted.	Met
§11.10(g)	Authority checks on use, signing, access and operations	Role checks on every route; signing requires an authenticated identity plus password re-authentication; overrides are permissioned and audited with a reason.	Met
§11.10(h)	Device checks to determine validity of the data source	Integration inputs are authenticated per source: HMAC-signed webhooks with a per-integration secret, scoped API keys, and signed single-use driver tokens. Physical terminal-level device validation is a customer network control.	Met (shared)
§11.10(i)	Education, training and experience of persons using the system	Vendor-supplied role-based manuals, a getting-started guide, an onboarding primer and per-role training-plan templates. Delivery and training records are yours.	Shared
§11.10(j)	Written policies holding individuals accountable for their electronic signatures	A customer responsibility — see §11.100(c). We provide the technical control and the wording; the policy and the signed certifications must be issued by you.	Customer
§11.10(k)	Controls over systems documentation, including change control of documentation	QMS documents are versioned and revision-controlled; platform change control is documented in YT-QMS-008; audit trail of configuration changes retained.	Met
§11.50	Signature manifestations — printed name, date and time, and meaning of signing	All three are stored with the signature: the signatory identity and full name, a server-generated timestamp, and a mandatory free-text meaning-of-signature statement that the workflow refuses to accept as empty.	Met

Clause	Requirement	Implementation	Status
§11.70	Signature-to-record linking, resistant to excision, copying or transfer	The signature is bound to the record by a SHA-256 hash over a canonical payload containing the record identifiers, tenant, signing time, the signature image digest and the previous signature hash. Altering or moving the signature breaks the chain detectably.	**Met**
§11.100(a)	Signatures unique to one individual, never reused or reassigned	Identities are unique and are never reissued to another person; deactivated accounts retain their historical attribution.	**Met**
§11.100(c)	Written certification that electronic signatures are legally binding equivalents	A customer action. This certification is issued by your organisation to the FDA and is the single most commonly missed Part 11 item; we flag it rather than leave it implied.	**Customer**
§11.200(a)(1)	Non-biometric signatures use at least two distinct identification components	Two components at every signing: the authenticated unique identity, plus password re-authentication verified at the moment of signing. Re-authentication is required for **every** signature, not only the first in a session — stricter than the continuous-session minimum.	**Met**
§11.200(a)(2)	Signatures used only by their genuine owner	Password re-authentication at signing, MFA, session controls, lockout, and audit of every signing event including source IP.	**Met**
§11.300	Controls over identification codes and passwords	Uniqueness of the identity–credential combination, bcrypt password hashing, complexity policy, breached-password screening against a public compromise corpus, lockout on repeated failure, and transaction-safeguard logging of failed signing attempts.	**Met**

7. ALCOA+ statement

The nine ALCOA+ principles as they apply to the records YARDtwin creates. This is the statement we would defend in front of an inspector, not a restatement of the definitions.

Principle	How YARDtwin satisfies it
Attributable	Every GxP record carries the unique identity of the person who created or changed it. Shared and generic accounts are not used; SCIM lifecycle management keeps identity tied to a real person.
Legible	Records are stored as structured relational data, rendered human-readably in the application with their audit trail, and exportable to CSV and JSON.
Contemporaneous	Timestamps are generated server-side in UTC at the moment of the event, not typed by an operator. Gate, seal, temperature and dock events are captured at the point of activity; back-dating is not possible through the interface.
Original	First-capture values are retained. A superseded value remains in the audit trail with its replacement; seal and logger photographs are stored as the original captured evidence alongside any transcribed value.
Accurate	Field validation, mandatory fields, referential integrity, expected-value comparison for seals and temperatures, and a variance flag on weighbridge net against expected net. AI-extracted values require human confirmation before they become the record.
Complete	Partially completed checks are visible as incomplete rather than absent. A waived evidence item requires a reason, which is itself written to the GxP audit trail.
Consistent	Single UTC time base, database constraints, and a chained departure signature hash that makes the sequence of releases verifiable.
Enduring	Retention schedule per record class (§8.1) with encrypted storage and automated backup; audit trail retained for the GxP period.
Available	Records are retrievable throughout the retention period by authorised users, and exportable on demand — including a contracted portability route on exit so availability survives the vendor relationship.

8. Data integrity and retention

8.1 Retention schedule

Retention is set by record class against a regulatory basis. Where a GxP period and a data-protection minimisation requirement pull in opposite directions — gate photographs containing personal data are the clearest case — the GxP record is retained and the personal-data element is minimised separately.

Record class	Retention	Basis
Gate entry and exit events	≥ 5 years	EU GMP Ch. 4
Seal verification records and images	≥ 5 years	EU GMP Ch. 4, EU GDP Ch. 9
Cold-chain and temperature records	≥ 5 years	EU GDP Ch. 9
Weighbridge records	≥ 5 years	EU GMP Ch. 4
Departure clearance and signatures	≥ 5 years	Annex 11 §14, Part 11 §11.10(c)
Audit trail — GxP-relevant	7 years	Annex 11 §9, Part 11 §11.10(e)
Audit trail — non-GxP	1 year	Operational
User account records	Contract duration + 2 years	Annex 11 §12, GDPR

Record class	Retention	Basis
Driver and carrier personal data	Contract duration + 12 months	GDPR Art. 5(1)(e)
Gate photographs containing personal data	Per-site setting, default 14 days	GDPR Art. 5(1)(c)
Configuration change history	≥ 5 years	Annex 11 §10
Integration message logs	Rolling window, configurable	Operational

8.2 Enforcement — stated precisely

Two retention controls run automatically today: deletion of gate photographs containing personal data after a per-site period (default 14 days), and rolling deletion of integration message logs. Scheduled enforcement across the remaining record classes is specified but is **not yet running** in the current architecture — retention for those classes is presently achieved by policy rather than by an automated control. It is listed in §17. GxP records are unaffected: their obligation is to be retained, and they are.

9. Data protection and privacy

9.1 Controller and processor roles

For customer yard data — driver names, vehicle registrations, carrier contacts, gate events and the operational records above — **you are the controller and YARDtwin Ltd is the processor**, acting on your documented instructions under a GDPR Article 28 data processing agreement. For our own account, billing and marketing data we are the controller. An executable DPA template is published at **yardtwin.com/security** and is available before contract so your privacy review can start early.

9.2 Legal bases and record classes

Data class	Typical legal basis (controller-side)
Platform account data	Art. 6(1)(b) contract performance
Driver and gate visit data	Art. 6(1)(c) legal obligation (GMP/GDP) and Art. 6(1)(b)
Carrier contact data	Art. 6(1)(b) contract performance
GMP compliance records	Art. 6(1)(c) legal obligation (Annex 11 / 21 CFR Part 11)
Audit log data	Art. 6(1)(c) legal obligation
Newsletter and marketing	Art. 6(1)(a) consent, with timestamp, IP and consent text retained

9.3 Data subject rights

Rights requests are supported operationally and in the product. A public request route is published at **yardtwin.com/data-request**; administrators can run a subject export by email address, and an erasure routine that **anonymises rather than deletes**.

> **Erasure that does not break the audit trail**
> GDPR Article 17(3)(b) preserves processing required by a legal obligation — and Annex 11 §9 requires the audit trail to survive. Our erasure routine therefore scrubs identifying fields across user, appointment and gate records to a deterministic placeholder, keeps the audit records themselves, and replaces the actor email in them with a deterministic pseudonym so the trail stays coherent but no longer identifies the subject. Row counts per table are returned so you can document the response in your own DSAR file.

9.4 Sub-processors

The complete register. Each is bound by a data processing agreement; material changes are notified in line with Article 28(2).

Sub-processor	Purpose	Location	Safeguard
Microsoft Azure	All platform infrastructure, database, storage, secrets	EEA (Norway, Sweden)	Intra-EEA; Microsoft DPA; residency enforced by Azure Policy
Anthropic	In-app assistant; document data extraction	USA	SCCs + DPA; customer data not used for model training
Google Cloud (Vision)	Driver-licence and shipping-document OCR	EEA / USA	SCCs + DPA; not used for model training; disableable per site
Resend	Transactional email delivery	USA	SCCs + DPA

Sub-processor	Purpose	Location	Safeguard
Stripe	Subscription billing; no yard personal data	EEA / USA	SCCs + DPA; PCI-DSS Level 1
ElevenLabs	Optional text-to-speech voice guidance	USA	SCCs + DPA; opt-in feature

9.5 Impact assessments and breach notification

Data protection impact assessments have been completed for gate audit-trail processing, cross-tenant platform analytics, marketing consent processing, and AI-assisted features. Our incident procedure commits to notifying you without undue delay and within **72 hours** of becoming aware of a personal-data breach affecting your data, with the information required by Article 33(3) — see §15.

9.6 AI processing and governance

AI is used for three things: reading driver licences and shipping documents (OCR), the in-app assistant, and optional voice guidance. Three commitments govern it:

- **No training on your data.** Our AI sub-processors process an input only to return a result for that request.
- **Human oversight.** Extracted fields are presented for review and can be corrected before they become the record. No AI output is committed unconfirmed, and the platform makes no automated decision producing legal or similarly significant effects on an individual (Article 22).
- **Off switch.** AI document reading can be disabled per site, so a site that prefers manual entry never transmits a document to an AI provider.

10. Security architecture

Controls as implemented, with the status recorded from live verification on 27 July 2026. One row is amber and it matters: the WAF policy is attached and in Prevention mode, but it currently has no rule set, so it does not filter application-layer traffic. It is the first item in §17.

10.1 Network and edge

Control	Implementation	Status
TLS	TLS 1.2 minimum, 1.3 preferred; HTTPS enforced with redirect	**Verified**
HSTS	Strict-Transport-Security with includeSubDomains, one-year max-age	**Verified live**
Edge	Azure Front Door in the production request path (verified by response headers)	**Verified live**
WAF	WAF policy attached in Prevention mode — **currently with no rule set**; see §17	**Partial**
Content Security Policy	Strict CSP with a per-request nonce; frame-ancestors self; object-src none	**Verified live**
Security headers	nosniff, Referrer-Policy, COOP, CORP, Origin-Agent-Cluster	**Verified live**
Database exposure	Managed PostgreSQL, firewalled; not reachable from the public internet	**Verified**
Rate limiting	Applied to public endpoints and separately to authentication	**Active**

10.2 Identity and access

Control	Implementation	Status
Unique identities	One account per person; no shared or generic accounts	**Enforced**
RBAC	Role checks at every API endpoint	**Active**
Multi-factor	TOTP enforced at login for accounts with MFA enabled; backup codes	**Active**
Single sign-on	SAML 2.0 (Entra ID, Okta, Google Workspace) plus Google and Microsoft OAuth	**Active**
Provisioning	SCIM 2.0 automated provisioning and deprovisioning	**Active**
Admin IP allow-listing	Optional per-tenant restriction of administrator sessions by source IP	**Available**
Password controls	bcrypt hashing, complexity policy, breached-password screening	**Enforced**
Brute-force defence	Account lockout after repeated failures, with audit	**Active**
Session control	Signed tokens with expiry; re-authentication required for signing	**Active**
Tenant isolation	Every query scoped by tenant; cross-tenant access treated as a P0 incident	**Verified**

10.3 Data protection

Control	Implementation	Status
Encryption at rest	AES-256 for database and blob storage	**Active**
Field-level encryption	AES-256-GCM in the application layer for sensitive personal fields	**Active**

Control	Implementation	Status
Encryption in transit	TLS for all client, API and integration traffic	Active
Key management	Azure Key Vault with RBAC; no secrets in source control or environment files	Active
Customer-managed keys	Platform-managed keys today; CMK/BYOK designed, not implemented	Not available
SQL injection defence	Parameterised queries throughout	Verified
Audit trail	Append-only; no update or delete path exists in the application	Verified
File storage	Private blob containers; no public object access; server-proxied delivery	Verified

10.4 Monitoring and detection

Control	Implementation	Status
SIEM	Microsoft Sentinel attached to Log Analytics, 90-day retention	Active
Customer SIEM export	Security-event export endpoint for ingestion into your own SIEM	Available
Application monitoring	Application Insights with availability, latency and 5xx alerting	Active
Breach detection	Automated detection pass with alerting to a defined action group	Active
Audit review	GxP-relevance flagging supports targeted audit-trail review	Active

11. Secure development and testing evidence

Every change to the platform passes an automated security and quality gate before it can be merged, and a second gate before it can reach production. The controls below run in continuous integration on every pull request.

Control	Tool / mechanism	Gating
Static analysis (SAST)	Semgrep, diff-scoped	Blocks merge
Dependency vulnerabilities	npm audit on backend and frontend, with a documented exception register for non-applicable advisories	Blocks merge
Container scanning	Trivy	Blocks merge
Secret scanning	Gitleaks, plus pre-commit hooks	Blocks merge
Dynamic analysis (DAST)	OWASP ZAP	Reported
Software bill of materials	CycloneDX SBOM generated and retained per build	Artefact
Dependency updates	Dependabot	Continuous
Peer review	Mandatory review on high-blast-radius paths (authentication, database, billing, gate, signatures)	Blocks merge
Functional regression	500-vehicle full-lifecycle suite plus end-to-end browser journeys	Blocks release
Production authorisation	Manual, deliberate dispatch — never automatic on merge	Human gate

11.1 Penetration testing

A penetration test was performed on 17–18 April 2026 across ten OWASP categories with 36 attack payloads, returning **zero vulnerabilities**, alongside functional security testing across more than 1,890 API calls with zero failures. To be precise about what that is and is not: this testing was not performed by a CREST-accredited third party. An independent accredited test is planned and is listed in §17 as an open item. A pen-test plan document is available on request.

12. CAIQ-Lite — completed

A completed lightweight Consensus Assessments Initiative Questionnaire across twelve domains. Five are Met, six are Partial and one — business continuity — is a Gap; the reason sits in the response column of each row and the remediation in §17. We can complete a full CAIQ v4 or a SIG-Lite in your own template on request.

Domain	YARDtwin response	Status
Governance and risk management	Documented QMS (§3), risk assessment on ICH Q9(R1), change control, incident and CAPA SOPs. No formal ISMS certification yet.	**Partial**
Identity and access management	Unique identities, RBAC at every endpoint, TOTP MFA at login, SAML 2.0 SSO, SCIM 2.0 provisioning, admin IP allow-listing, lockout, session controls.	**Met**
Encryption and key management	TLS in transit; AES-256 at rest; AES-256-GCM field encryption; Azure Key Vault with RBAC; bcrypt password hashing. Customer-managed keys not offered.	**Partial**
Data residency and sovereignty	All platform data in the EEA (Norway East, Sweden Central); residency enforced by an Azure Policy Deny assignment; limited sub-processor transfers under SCCs.	**Met**
Application security	Strict CSP with per-request nonce, security headers, parameterised queries, breached-password screening, SAST/DAST/SCA/SBOM in CI. WAF policy has no rule set attached.	**Partial**
Logging and monitoring	Sentinel SIEM on Log Analytics (90 days), Application Insights alerting, append-only application audit trail, customer SIEM export endpoint.	**Met**
Business continuity and resilience	Automated backups with 7-day point-in-time recovery, staging slot, documented gate contingency. High availability not enabled; geo-redundant backup not enabled; RTO/RPO not contractually committed.	**Gap**
Incident response	Documented IR runbook with severity classification, automated breach detection, 72-hour breach notification commitment, published security.txt contact. Tabletop exercise scheduled, not yet run.	**Partial**
Privacy and data protection	Article 28 DPA available pre-contract, RoPA and data inventory, DSAR request route with export and anonymising erasure, DPIAs completed, sub-processor register published. No DPO appointed.	**Met**
AI governance	No-training commitments from AI sub-processors, human confirmation of all extracted values, per-site off switch for document AI, no Article 22 automated decisions, documented AI data-flow.	**Met**
GxP and regulatory compliance	Annex 11 and 21 CFR Part 11 implementation mapped clause by clause (§5, §6), ALCOA+ statement (§7), QMS document set (§3). SOC 2 Type II and ISO 27001 not held.	**Partial**
Vendor viability and exit	JSON and CSV data export for portability; right-to-audit and exit clauses offered in the MSA. Cyber insurance and an escrow arrangement are not in place.	**Partial**

13. Certification and assurance status

The section reviewers turn to first. Nothing here is aspirational: if we do not hold a certification, the row says **not held**.

Framework	Position	Status
EU GMP Annex 11	Implemented and mapped clause by clause in §5; supported by the QMS in §3	**Implemented — not a certification scheme**
21 CFR Part 11	Implemented and mapped clause by clause in §6	**Implemented — not a certification scheme**
GDPR	Article 28 DPA, RoPA, DSAR routes, DPIAs, sub-processor register, EEA residency	**Compliance position, self-assessed**
SOC 2 Type II	Not held. A combined SOC 2 and ISO 27001 programme is planned with a target of Type I at approximately month four and Type II at approximately month twelve from programme start.	**Not held**
ISO/IEC 27001:2022	Not held. Same programme as above; the QMS documents in §3 provide a substantial share of the Annex A control documentation.	**Not held**
Independent CREST penetration test	Not yet performed. Internal and tooling-based testing completed April 2026 with zero findings (§11.1).	**Planned**
Azure inherited certifications	Our infrastructure provider holds ISO 27001, SOC 1/2/3, ISO 27018 and others for the platform services we consume. These are Microsoft's certifications, not ours, and we do not present them as ours.	**Inherited, infrastructure only**

On "compliant" versus "certified"

Annex 11 and 21 CFR Part 11 are regulatory expectations, not certification schemes — no body issues an "Annex 11 certificate", and any vendor offering one is selling something else. What can be evidenced is an implementation mapped clause by clause with artefacts behind it, which is what §5 and §6 are. SOC 2 and ISO 27001 *are* certification schemes, we do not hold them, and we do not describe ourselves as certified.

14. Business continuity, backup and recovery

This is the weakest area of our posture and we would rather you read our own assessment of it than discover it in a questionnaire.

Aspect	Current state
Backups	Azure PostgreSQL automated backups with 7-day point-in-time recovery
Geo-redundant backup	**Not enabled**
High availability	**Not enabled.** The database runs as a single instance without zone redundancy; a zone failure would cause an outage bounded by restore time, not an automatic failover.
Database tier	Burstable — appropriate to current load, not to a high-availability commitment
Deployment resilience	Staging slot with swap-based release and rollback by reverse swap
RTO / RPO	Internal targets of RTO ≤ 4 hours and RPO ≤ 24 hours (YT-QMS-002 URNF-003). These are **not** contractual commitments today.
Restore testing	Point-in-time recovery is a platform capability; a documented restore drill with retained evidence is an open item (§17)
Availability target	99.5% internal target; no published status page or contractual SLA credit scheme today
Gate contingency	Documented manual gate procedure for use during unavailability; customers should rehearse it as part of their Annex 11 §16 arrangements

What this means for your risk assessment

If your qualification requires zone-redundant high availability with a contractual RTO/RPO, YARDtwin does not meet that today, and you should treat it as a risk to be mitigated or a condition to be met before go-live rather than an assumption. A high-availability and BCDR workstream — zone-redundant database, documented drill evidence, published availability commitment — is designed and scoped. We are happy to discuss sequencing it against a specific deployment.

15. Incident response and breach notification

Element	Commitment
Detection	Automated breach-detection pass with alerting to a defined action group; SIEM correlation in Microsoft Sentinel; application and availability alerting
Classification	Severity 1 to 4 with defined response expectations, per the incident response runbook and YT-QMS-009
Investigation and CAPA	Root-cause investigation proportionate to severity; corrective and preventive actions tracked to closure in the CAPA register (YT-QMS-010)
Personal-data breach notification	Notification to you as controller without undue delay and within **72 hours** of becoming aware, with the Article 33(3) content set
GxP incident notification	Notification of incidents affecting the integrity or availability of GxP records, to support your own deviation handling
Vulnerability disclosure	Published security.txt and a monitored disclosure address; CVSS-banded remediation SLAs in the patch management policy
Post-incident	Written post-incident report available to affected customers on request
Tabletop exercise	Scripted exercise and on-call rota template prepared; first run is an open item (§17)

16. Shared responsibility

Vendor assurance goes wrong when both sides assume the other owns a control. This is the split as we understand it; if your quality system allocates any line differently, tell us and we will reflect it in your instance documentation.

Activity	YARDtwin	You (the customer)
Platform validation (vendor side)	YARDtwin	—
Instance IQ / OQ / PQ	Support, protocols, evidence	**Executes and approves**
URS for your intended use	Platform URS provided	**Owns intended-use URS**
Risk assessment of your process	Platform risk assessment provided	**Owns process risk**
Configuration of gate, seal, temperature and checklist controls	Capability and defaults	**Configures and controls**
User provisioning and periodic access review	SCIM, RBAC, review reporting	**Owns the review**
§11.100(c) signature certifications	Technical control and wording	**Issues certifications**
Training and training records	Manuals and training templates	**Delivers and records**
Audit-trail review	GxP flagging, filtering, export	**Performs and documents review**
Platform change control	YARDtwin, with notification	Assesses impact on validated state
Carrier qualification	—	**Owns**
Deviation and CAPA for yard events	Records and evidence	**Owns**
Infrastructure security and patching	YARDtwin	—
Endpoint, network and physical security at your site	—	**Owns**
Personal-data controller obligations	Processor obligations under Art. 28	**Controller**
Annex 11 §16 contingency rehearsal	Documented manual procedure	**Rehearses**

17. Open items — the complete list

Everything not yet in place, in one table, with our own severity assessment. There is no separate list; this is it. Items are reviewed at least every six months and this pack is reissued when a status changes.

Item	Current position	Severity	Type
WAF rule set	The WAF policy is attached in Prevention mode but has no managed or custom rule set, so it does not filter layer-7 traffic today. Attaching a managed OWASP rule set requires the Premium edge tier.	**High**	Edge configuration
SOC 2 Type II	Not held. Combined programme with ISO 27001 planned; Type I targeted at approximately month 4, Type II at approximately month 12 from start.	**High**	Certification programme
ISO/IEC 27001:2022	Not held. Same programme; ISMS charter and QMS-to-Annex-A mapping prepared.	**High**	Certification programme
High availability and BCDR commitments	Zone-redundant database, geo-redundant backup, documented restore drill evidence, published availability commitment and status page.	**High**	Infrastructure
Independent CREST penetration test	Accredited third-party test to replace internal testing as the primary assurance evidence.	**Medium**	Procurement
Automated retention enforcement	Photograph and integration-log retention run automatically today. Full scheduled enforcement across all record classes is specified but not yet running in the Azure architecture.	**Medium**	Engineering
Per-record PDF printout	Human-readable print and CSV/JSON export exist; a dedicated per-record PDF with full context (Annex 11 §8, Part 11 §11.10(b)) is specified at medium priority.	**Medium**	Engineering
Customer-managed keys (CMK/BYOK)	Designed against Azure Key Vault; not implemented.	**Medium**	Engineering
QMS formal approval signatures	The ten QMS documents are issued at v1.0 in draft-for-review status with approver assignment pending.	**Medium**	Quality function
First periodic review cycle	Annual review of the validated state is defined; the first formal cycle has not yet completed.	**Medium**	Quality function
IR tabletop exercise	Script and on-call rota prepared; first exercise not yet run.	**Low**	Operations
Cyber insurance and escrow	Neither is in place today.	**Low**	Commercial
Data protection officer	No DPO appointed. Article 37 appointment is not mandatory for our processing profile; a privacy contact is published.	**Low**	Governance

How to read this table

Four High items: the WAF rule set, the two certifications, and high availability. The first is an edge configuration change. The certifications are a twelve-month programme. High availability is an infrastructure change we can sequence against a specific deployment. Nothing on this list is a defect in the GxP record controls in §5 to §8 — those are implemented and verifiable.

18. Audit rights, contacts and what else you can ask for

We support customer vendor audits, and the MSA offers a right-to-audit clause. Short of a full audit, the following are available on request — several under a mutual non-disclosure agreement:

- The complete ten-document QMS set
- Records of Processing Activities and the personal-data inventory
- The penetration test plan and April 2026 test report
- Operational Qualification protocols and executed test evidence
- Validation reports for integration surfaces, including SAP EWM conformance runs
- The patch and vulnerability management policy with its CVSS-to-SLA table
- The incident response runbook
- A CycloneDX software bill of materials for a nominated release
- The Azure Policy residency assignment, as evidence for §2.2
- A pre-filled CAIQ or SIG-Lite in your own template

Purpose	Contact
Vendor assurance, QMS requests, audit scheduling	admin@yardtwin.com
Privacy, DPA and data subject matters	privacy@yardtwin.com
Security disclosure	admin@yardtwin.com · yardtwin.com/.well-known/security.txt
Published trust information	yardtwin.com/security
Data processing agreement template	yardtwin.com/security

Document control

Prepared by the YARDtwin quality team. Every control status in this pack was verified against live production infrastructure and live source code on 27 July 2026. This document is provided for vendor-assessment purposes; it is not a contractual warranty, and contractual commitments are those in the master services agreement and the Article 28 data processing agreement. It will be reviewed at least every six months, and reissued whenever a status in §13 or §17 changes.

Document	Code	Version	Date	Next review
Vendor Assurance Pack	YT-VAP-001	v1.0	27 July 2026	January 2027