

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+ · security architecture · completed CAIQ-Lite
- Every correction to v1.1, and every open item, with dates

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.

Why there is a version 1.2

Version 1.1 of this pack, and its wording-only edition 1.1.1, overstated several controls — among them a breached-password check that had not been built, field-level encryption that we do not offer, and a Google OCR sub-processor that we do not use. This edition corrects them. The pages after this one list every correction next to what v1.1 said, because you may already hold v1.1 and should know exactly what changed. Please discard v1.0, v1.1 and v1.1.1.

Every status below was re-verified on **12 October 2026** against the source code running in production (build fd722d8), the live Azure configuration and our public pages. Where something could not be verified it is marked **[CONFIRM]** and stated in its weaker form. We hold neither ISO/IEC 27001 nor SOC 2, and no independent penetration test has been carried out yet; §13 and §17 say so where a reviewer looks.

Where to start, by reader

Reader	Read these sections
In a hurry, or holding v1.1	The changes pages (next), then §13 and §17: together they hold everything that is not yet in place
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 · §15 breach notification
Procurement / vendor risk	§13 certification status · §14 continuity · §16 responsibility split · §17 open items · §18 audit rights, company and insurance

Scope of this pack

This document describes the YARDtwin platform, operated by YARDtwin as a multi-tenant SaaS service, and the vendor-side controls that apply to it; company registration details are available on request. Your instance configuration, its validation and your process controls are yours (§16). The pack is not a contractual warranty: commitments live in the Terms of Service, the Data Processing Agreement and any master subscription agreement. **YARDtwin is founder-led: one person, no employees.** Where that matters for a control — code review, monitoring, support hours, key-person cover — the section says so and §17 gives the dated plan.

Changes since v1.1 — corrections first

Table A lists the statements in v1.1 and v1.1.1 that were not true when they were made, with what is true now. Table B lists what has changed in the platform since v1.1; table C lists work that is in release or planned, with dates. Section references in the middle column are to v1.1.

A. Statements in v1.1 and v1.1.1 that were not true, corrected

#	Topic	v1.1 / v1.1.1 said	True on 12 October 2026
1	Breached passwords	Breached-password screening "against a public compromise corpus" listed as in place (§6 §11.300 Met; §10.2; §12). It had not been built.	Live since 12 October 2026. New passwords are checked against the Have I Been Pwned Pwned Passwords range service using k-anonymity: only the first five characters of the password's SHA-1 hash leave our servers. The check fails open — if the service does not answer within 2 seconds the password is accepted. On by default; a tenant administrator can switch it off.
2	Encryption of personal fields	"Application-layer AES-256-GCM field encryption for sensitive personal fields" (§5 Annex 11 §7; §10.3; §12).	Field-level encryption of customer data is not offered. Customer data is encrypted at rest by Azure (AES-256, Microsoft-managed keys) in the database, file storage and backups. Application-level AES-256-GCM encryption is used only for MFA secrets and chat-webhook URLs.
3	Google OCR sub-processor	Google Cloud listed as a sub-processor for driver-licence and shipping-document OCR (§9.4).	YARDtwin uses no Google OCR or image-analysis service. AI document reading uses Anthropic only. Google appears in the register only as an optional sign-in provider.
4	Security monitoring	Microsoft's cloud SIEM service named as attached to the log workspace, with SIEM correlation of incidents (§2, §10.4, §12, §15).	No SIEM is attached and there is no 24/7 security operations centre. Monitoring is Azure Monitor alerting and availability tests, Azure Service Health alerts, malware alerts on uploads and an application breach monitor that e-mails the founder. Platform logs are kept 90 days.
5	Penetration testing	Cover KPI "0 pen-test findings, Apr 2026"; §11.1 described April 2026 testing as a penetration test that returned zero vulnerabilities.	No penetration test by an independent firm has been carried out. The April 2026 work was internal functional and security testing. Our internal white-box code audit of October 2026 (YT-SEC-AUDIT-001) did find vulnerabilities, including two Critical; the Critical and most High findings are fixed in production. An independent test is planned (§11.2).
6	Backup immutability	"7-year WORM immutability policy" on long-term backups, with delete and overwrite "refused" (§2, §5, §6, §7, §14).	Monthly backups sit under a time-based immutability policy of 2,555 days that is not locked . While it is in force it blocks deletion and overwrite of the backups, but an administrator could still shorten or remove the policy itself. Locking it is planned (§17).
7	Container scanning	Trivy container scanning "blocks merge" (§11).	Trivy runs on every pull request as a required check but is configured not to fail on findings, so it is advisory . A blocking scan of the shipped image is planned (§17).
8	Code review	"Mandatory review on high-blast-radius paths (authentication, database, billing, gate, signatures)" — "blocks merge"; document "prepared by the YARDtwin quality team" (§10, §11, §18).	One person writes, approves and releases code. The branch rules require a pull request and passing checks, but no second human approval . The compensating controls and the plan for a second reviewer are in §11 and §17. This pack is prepared by the founder.
9	AI 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" (§9.6, §12).	At the time, the site switch covered only some AI calls and allowed the call if the setting could not be read. Since 12 October 2026 every AI call checks the site switch and a new tenant-wide "No external AI processing" switch on the server, and is refused if either is off or cannot be confirmed.

#	Topic	v1.1 / v1.1.1 said	True on 12 October 2026
10	Undisclosed AI use	§9.6 listed three AI uses. It did not say that a driver's gate photo could be sent to the AI provider for comparison with the licence photo.	Disclosed in §9.6. Since 12 October 2026 the face comparison is off by default and runs only where a site turns it on.
11	Database exposure	"Managed PostgreSQL, firewalled; not reachable from the public internet" (§10.1).	The database has a public endpoint behind a firewall that admits Azure-hosted services and one administrator address, with TLS required. Private networking is planned with the database rebuild (§17).
12	Erasure and the audit trail	Erasure replaces the actor in audit records with a pseudonym "so the trail ... no longer identifies the subject" (§9.3).	Audit entries carry a pseudonymous actor token, but the token-to-address mapping is kept after erasure. The trail is therefore pseudonymised, not anonymised : YARDtwin could still re-identify the actor (§9.3).
13	E-signatures for SSO-only users	Part 11 signing marked Met (§6) without saying that users who sign in only through SSO could not apply an electronic signature.	Fixed 12 October 2026: SSO-only users set a separate signing password through an authenticated, e-mail-verified flow (§6).
14	Sub-processor register	Omitted Twilio and the Google and Microsoft sign-in providers; described ElevenLabs as opt-in voice guidance only (§9.4).	§9.4 now matches yardtwin.com/subprocessors. Twilio (if enabled) and the sign-in providers are listed, and ElevenLabs is shown to voice the in-app assistant's replies, which can contain operational details such as vehicle registrations.
15	Staging environment	The staging slot listed as a continuity control, without saying it used the production database (§14).	Disclosed in §2.3. Until the separate staging database goes live, staging connects to the production database server, using dedicated test tenants.
16	Impact assessments	"Data protection impact assessments have been completed" for four processing areas (§9.5).	We cannot evidence those as completed DPIAs, so the statement is withdrawn. What exists is a processor-side DPIA input pack for your own DPIA (draft, on request).
17	Dependency alerts	"Dependabot — continuous" (§11).	Weekly Dependabot version-update pull requests do run. Dependabot vulnerability alerts were off when v1.1 was issued; they were switched on 11 October 2026. Automatic security-fix pull requests are not enabled.
18	Logging and monitoring status	CAIQ domain "Logging and monitoring" marked Met (§12).	Marked Partial: no SIEM, no 24/7 monitoring, and no 12-month archive of security logs yet.
19	Smaller corrections	A registered company name stated as the operator; residency policy named "yardtwin-eu-only-locations"; DPA template "published at yardtwin.com/security"; retention rows for account data ("contract + 2 years") and driver data ("contract + 12 months").	Company registration details are available on request. The policy assignment is "yardtwin-eu-only-assignment" (its definition is "yardtwin-eu-only-locations"). The DPA is at yardtwin.com/dpa (v3.2); the template download was withdrawn because it no longer matched the platform. Retention rows now match the live privacy policy (§8.1).

B. What has changed in the platform since v1.1

All live in production on 12 October 2026.

Area	What changed	Live since
Service levels	99.5% monthly availability on paid plans with service credits (Terms of Service section 8); public SLA page; self-reported status page with incident history. RTO and RPO remain internal targets.	Since v1.1
Core printouts	Controlled per-record PDF for core visits (Visit Record, VRC- numbers, content hash) — closes the v1.1 Annex 11 §8 / Part 11 §11.10(b) gap.	Since v1.1

Area	What changed	Live since
Retention	Scheduled daily retention sweep per tenant, opt-in with second-administrator approval and a kill switch; driver-photo retention default 14 days (2–14).	Since v1.1; photos 11 Oct 2026
Backups and storage	Nightly database dump to separate geo-redundant storage in the EEA, kept 35 days; uploaded files read-access geo-redundant (Norway West) with versioning.	11–12 Oct 2026
Platform hardening	Malware scanning of uploads (Defender for Storage); Key Vault purge protection; platform logs 90 days; Service Health alerts; CAA and TLS-RPT records; the application accepts traffic only through Front Door; Dependabot alerts on.	5–11 Oct 2026
Identity and access	Tenant "Require MFA"; server-side idle expiry; administrator MFA reset with four-eyes approval; API keys expire within 365 days; customer-approved, time-boxed support access with audited break-glass; YARDtwin reads of a customer's data written to that customer's audit trail; SCIM groups mapped to roles; breached-password check.	12 Oct 2026
Electronic signatures	Signing password for SSO-only users; the address of a former signer is retired so it is not given to a new account.	12 Oct 2026
Privacy	E-mail addresses, phone numbers and tokens masked in application logs; tenant administrators handle data-subject requests for their own tenant; whole-tenant offboarding with a certificate of deletion.	12 Oct 2026
AI	Tenant "No external AI processing" switch; site switch checked on every AI call and fail-closed; face comparison off by default, its result recorded by the server; driver-photo purge covers the identity-check photos.	12 Oct 2026
GxP change control	Part 11 / Annex 11 impact and validation flags on release notes; opt-in GxP release notices to named customer recipients.	12 Oct 2026
Web security	One security-header and CSP definition for web server and API; rate-limit counters shared across application instances.	12 Oct 2026
Notification clocks	Initial notice within 24 hours of a confirmed security incident affecting your data; personal-data breach notice without undue delay and within 48 hours (was 72 hours).	Oct 2026

C. In release or planned — not yet live

Item	Status	Target
Separate staging database and storage	In release. A staging database (Norway East, test data only) and storage account exist; the staging slot switches to them when the release completes (pull request open).	12–13 Oct 2026 [CONFIRM]
Runtime upgrade	In release. Node.js 24 (digest-pinned) replacing Node.js 20; the API runs as a non-root user; the database server certificate is verified (verify-full); configuration is validated at boot; the token algorithm is pinned (pull request open).	Oct 2026 [CONFIRM] ; by 13 Nov 2026
Pipeline hardening	Planned, not started: OIDC deploy credential in place of a stored secret; blocking scan of the shipped container image; SBOM per release; locking the long-term backup immutability policy.	By 13 Nov 2026 [CONFIRM]
Independent penetration test	Planned. RFQ and scope prepared (YT-SEC-RFQ-001).	Dec 2026 [CONFIRM]
ISO/IEC 27001	Programme under way. Stage 2 audit February 2027.	Certificate targeted Q1 2027

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 languages	Annex 11 and 21 CFR Part 11	EEA data hosting	99.5% monthly availability, paid plans	10 QMS documents
------------------------	---	----------------------------	---	----------------------------

1.1 Records the platform creates

The following are treated as GxP-relevant and carry the 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
- Driver identity checks at the gate, with the staff decision and its reason
- 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
- Where the Life Sciences module is enabled: chain-of-custody events, cold-chain excursion records, and carrier and driver qualification records, with controlled PDF documents issued against them
- The audit trail covering every change to the above

2. Hosting, infrastructure and data residency

YARDtwin runs entirely on Microsoft Azure, with customer data stored in EEA regions only. There is no secondary hosting provider for customer data. The topology below was read from the live subscription on 12 October 2026.

Component	Service	Region
Application	Azure App Service, Linux container (Premium v3, two instances)	Norway East
Database	Azure Database for PostgreSQL Flexible Server 15 (Burstable B1ms, single zone, no high availability)	Sweden Central
File and document storage	Azure Blob Storage, private containers only; versioning; malware scanning on upload; read-access geo-redundant copy	Norway East, copy in Norway West
Secrets	Azure Key Vault, RBAC-controlled, purge protection on	Sweden Central
Container registry	Azure Container Registry	Sweden Central
Edge	Azure Front Door (Standard) with a WAF policy; the application accepts traffic only from Front Door	Global
Monitoring	Application Insights availability tests, Log Analytics (90-day retention), Azure Monitor and Service Health alerts — no SIEM	Norway East; alert rules global or EU
Daily database backup	Nightly full dump, kept 35 days, geo-zone-redundant storage (GZRS)	Sweden Central, replicated to Sweden South
Long-term backup archive	Monthly full backup, GZRS, time-based immutability of 2,555 days (not yet locked) — see §14	Sweden Central, replicated to Sweden South
Staging	App Service staging slot; a separate staging database (test data only) and storage account are in release — see §2.3	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 storing personal data in Norway East is an intra-EEA arrangement 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-assignment**, effect **Deny**, enforcement on) refuses the creation of resources outside an approved list of European regions: the EEA regions plus Switzerland and the United Kingdom, both covered by EU adequacy decisions. Global services such as Front Door and DNS sit outside the policy by design. Every regional resource in use today is in Norway or Sweden, apart from one alert rule in North Europe (Ireland). Residency therefore does not depend on operator discipline, and the assignment can be shown on request.

Some features send limited data to sub-processors outside the EEA — chiefly Anthropic in the United States for AI features — under Standard Contractual Clauses (§9.4). AI processing can be switched off per site or for a whole tenant (§9.6).

2.3 Environments and test data

Changes are released through a staging slot. Production data is not used for development or testing. **Today the staging slot still connects to the production database server**, using dedicated test tenants, and the two slots share the file storage account and the rate-limit counters; the separation is logical, not physical. A separate staging database (Norway East, holding test data only) and a separate staging storage account were created on 12 October 2026, and the switch-over is in release (scheduled 12–13 October 2026

[CONFIRM]).

3. Quality management system

A quality-management document set covers the platform lifecycle; it is available in full under a mutual NDA from 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

Documents are signed under a controlled electronic signing process (YT-SOP-SIGN-001): each signature is bound to the SHA-256 digest of the exact document bytes, chained, and requires passphrase re-authentication. The ten QMS documents above carry **review signatures dated 2 August 2026**; the approval signature has not yet been applied (planned October 2026 **[CONFIRM]**). The 19-document Life Sciences validation set (§3.1) is signed and **issued as controlled copies**; the meaning of those signatures is technical review. Some QMS statements (for example incident notice times and role names) predate this pack; where they differ, this pack and the DPA govern until the QMS approval.

3.1 Supporting documents

- **Life Sciences validation pack** — 19 documents (URS, as-built FS and configuration specification, executed IQ/OQ/PQ, traceability matrix, Annex 11 and Part 11 assessments, supplier assessment, restore-test record, periodic evaluation), issued for release v-1s-1.0 (August 2026); re-execution on the current release targeted January 2027
- **OQ protocols** for discrete capabilities, for example 24 cases for the Smart Slots scheduling engine and 28 cases, with traceability, for floor-level batch tracking
- **Data-protection set**: Records of Processing Activities and personal-data inventory; and, as drafts on request, the signable DPA v4.0, sub-processor register, retention schedule and DPIA input pack
- **Policies** (drafts, on request): Quality Agreement template (YT-QA-001), AI use policy and EU AI Act position (YT-POL-AI-001), supplier ethics and compliance policies (YT-POL-ETH-001), gate contingency procedure (YT-SOP-GATE-001)
- **ISMS documents** (drafts, under NDA): ISMS manual (YT-ISMS-001), incident and breach procedure (YT-ISMS-014), continuity plan (YT-ISMS-015), people security (YT-ISMS-012), ISO/IEC 27001 roadmap (YT-CERT-003)
- **Security testing**: pen-test plan, independent-test RFQ and scope (YT-SEC-RFQ-001), summary of the October 2026 internal code audit (YT-SEC-AUDIT-001) under NDA; integration manuals (SAP EWM, 47 pages)

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; release notes with GxP-impact flags	Both

4.2 Continuous verification evidence

Because the platform ships changes continuously, verification is continuous. Every pull request runs a 100-vehicle full-lifecycle regression against a real database, a reduced cross-tenant isolation sweep and a browser pass over every page. Every merge is deployed to staging and validated there with a 500-vehicle regression that includes the full isolation sweep, plus end-to-end browser journeys, before it can be promoted. Promotion to production is a separate, manual authorisation step: it cannot happen as a side effect of a merge, and it checks that staging is serving the exact commit being released. (An operator can skip the browser journeys on a manual release; the 500-vehicle gate cannot be skipped.)

Release notes carry Part 11 impact, Annex 11 impact and validation-required flags, published at yardtwin.com/changelog; customers can opt in to GxP release notices for up to five named recipients. Automatic recording of each production release is switched on with the staging separation (§2.3); until then release records are entered by hand.

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, a 152-case full-platform validation, a Life Sciences module validation of 585 automated checks plus a 99-step executed IQ/OQ/PQ qualification record run twice consecutively without a failure, a 20-scenario digital-twin visual validation, and a 15-test weighbridge integration validation. Most of these were executed on earlier releases (mid-2026). They are listed 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 out of scope, and §4, §7, §10, §16 and §17 are partial. §8 moved from partial to implemented since v1.1 (per-record Visit Record PDF).

Clause	Requirement	YARDtwin implementation	Evidence / status
§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	Roles defined in YT-QMS-003 §5. YARDtwin is founder-led, so several vendor-side roles are held by one person (§11, §17). 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 assessment of us. Our infrastructure supplier (Microsoft Azure) and all sub-processors are listed 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. The Life Sciences pack was executed on release v-ls-1.0; re-execution on the current release is planned (January 2027). Instance IQ/OQ/PQ is a joint activity.	Partial — YT-QMS-002/003; §17
§5	Data — accuracy of data exchanged electronically	Structured relational storage with referential integrity and field validation. Integration inputs are authenticated per source (signed webhooks, scoped API keys); 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. AI-extracted document fields are presented to staff for confirmation before they become the record.	Gate and departure workflows
§7	Data storage — secure, accessible, with tested restore	Encrypted at rest by Azure (AES-256, Microsoft-managed keys); field-level encryption is not offered. Backups: 7-day point-in-time restore, a nightly dump kept 35 days, and a monthly long-term backup under a 2,555-day time-based immutability policy (not yet locked), all in geo-redundant EEA storage. A production restore test was executed on 1 August 2026 (6 minutes 43 seconds). High availability is not enabled (§14).	Partial — YT-DR-LS-001; §14
§8	Printouts — clear printed copies of electronically stored data	Records and their audit trail are shown in human-readable form and exportable as CSV and JSON. A controlled per-record PDF is issued for a core visit (Visit Record: gate movements, seals, cold chain, weighbridge, departure clearance and signature, and the audit trail, with a document number and content hash). The Life Sciences module issues chain-of-custody certificates and excursion reports on the same basis.	Implemented
§9	Audit trails — who, what, when, and the reason for change	No application route can edit an audit record, and database triggers refuse UPDATE and DELETE on the audit table. Two controlled exceptions exist: deletion through the retention engine (after second-administrator approval) and through tenant offboarding. Entries are SHA-256 hash-chained per entity with sequence counters, so removal or reordering is detectable, and carry actor, action, entity, old and new values, IP address, timestamp and a GxP flag.	YT-QMS-006; §7

Clause	Requirement	YARDtwin implementation	Evidence / status
§10	Change and configuration management	Change control (YT-QMS-008): every change through a pull request with required automated checks, staging validation and a manual production authorisation. One person approves changes; there is no second human reviewer yet (§11). Release notes carry GxP-impact flags; customer configuration changes are audited.	Partial — YT-QMS-008; §11
§11	Periodic evaluation of the validated state	Annual platform review defined in YT-QMS-003 §8.2. The first cycle was executed in August 2026: a QMS annual review (YT-QMS-AR-001) and a periodic evaluation of the validated state (YT-PE-LS-001), both issued as controlled copies.	YT-QMS-AR-001; YT-PE-LS-001
§12	Security — access control, authorisation and segregation	Unique named identities; role checks on the API; TOTP MFA (mandatory for YARDtwin platform administrators, and for all your staff if you turn on "Require MFA"); SAML 2.0 SSO; SCIM 2.0; optional administrator IP allow-list; logout; server-side idle expiry; tenant isolation tested before every release; YARDtwin access to your data only with your time-boxed grant.	YT-QMS-006; §10
§13	Incident management	Incident and deviation SOP (YT-QMS-009) and an incident and breach procedure (YT-ISMS-014, draft); automated anomaly detection with e-mail alerting; initial notice within 24 hours of a confirmed security incident, personal-data breach notice within 48 hours (§15).	YT-QMS-009; §15
§14	Electronic signature	Departure clearance is released by an electronic signature that requires password re-authentication at every signing (a separate signing password for SSO-only users), records the meaning of the signature and the signer's own 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.	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	Backups with an executed restore drill, geo-redundant copies in a second EEA region, a contractual 99.5% monthly availability commitment on paid plans, and a gate contingency procedure template. High availability is not enabled and RTO/RPO are internal targets, not contractual (§14).	Partial — §14, §17
§17	Archiving — records readable and retrievable for their retention period	Retention by record class (§8), audit trail and metadata kept with the records, export in CSV and JSON for portability, and monthly backups held up to 7 years. At contract end your records are exported to you and then deleted; how long YARDtwin keeps the GMP audit trail after exit is being reconciled (§9.3) [CONFIRM] .	Partial — §8, §9.3

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. Rows marked **Customer** or **shared** cannot be discharged by a vendor alone; §11.100(c) is the one most often left undone, and §11.100(a) now carries a documented residual that your SOP closes.

Clause	Requirement	Implementation	Status
§11.10(a)	Validation of systems for accuracy, reliability and consistent intended performance	V-model validation (§4) plus continuous regression: a 100-vehicle suite on every pull request and a 500-vehicle suite in staging validation before every release.	Met
§11.10(b)	Ability to generate accurate and complete copies in human-readable and electronic form	Human-readable display and print with the audit trail; CSV and JSON export; controlled per-record PDFs for core visits (Visit Record) and Life Sciences records.	Met
§11.10(c)	Protection of records to enable accurate retrieval throughout the retention period	Encrypted storage; point-in-time restore (7 days), nightly dumps (35 days) and monthly backups (up to 7 years, time-based immutability not yet locked) in geo-redundant EEA storage; defined retention; executed restore test (YT-DR-LS-001).	Met
§11.10(d)	Limiting system access to authorised individuals	Unique identities, role checks, MFA (platform administrators always; your staff if you require it), SSO, SCIM, optional admin IP allow-list, lockout, idle expiry, tenant isolation.	Met
§11.10(e)	Secure, computer-generated, time-stamped audit trails	Server-generated UTC timestamps; previous and new values retained; database triggers refuse direct UPDATE and DELETE except the controlled retention and offboarding purge; entries hash-chained per entity; GxP flag.	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 routes; 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: signed webhooks, scoped API keys and signed single-use driver links. Terminal-level device validation is a customer network control.	Met (shared)
§11.10(i)	Education, training and experience of persons using the system	Role-based manuals and a self-refreshing help centre, an onboarding primer and 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.	Customer

Clause	Requirement	Implementation	Status
§11.10(k)	Controls over systems documentation, including change control of documentation	QMS documents are versioned and signed under YT-SOP-SIGN-001; platform change control in YT-QMS-008; configuration changes audited.	Met
§11.50	Signature manifestations — printed name, date and time, and meaning of signing	Stored with the signature: the signer's identity and full name, a server-generated timestamp, the meaning of the signature (set by the server for the action) and a mandatory statement from the signer of at least 10 characters.	Met
§11.70	Signature-to-record linking, resistant to excision, copying or transfer	A SHA-256 hash over a canonical payload containing the record identifiers, tenant, signing time, the signature image digest and the previous signature hash, chained per site. Altering or moving a signature breaks the chain detectably.	Met
§11.100(a)	Signatures unique to one individual, never reused or reassigned	Identities are unique and shared accounts cannot sign. Since 12 October 2026 the address of a person who has signed is retired and cannot be given to a new account in the tenant. Residual: an administrator or your SCIM directory can change the e-mail address of an existing signer's account. That cannot be blocked, so it is detected: the signing password is cleared, a GMP audit entry is written, and the old address is notified and retired. Your SOP should forbid re-addressing a signer's account to another person.	Met (shared)
§11.100(c)	Written certification that electronic signatures are legally binding equivalents	A customer action, issued by your organisation to the FDA. It is the most commonly missed Part 11 item, so 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 a password verified at the moment of signing (the account password, or the signing password for SSO-only users). Required for every signature, not only the first in a session; locked after 5 failures in 15 minutes.	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	Unique identity–credential pairs; bcrypt (cost 12); at least 12 characters with upper, lower and digit by default (a tenant administrator can relax the character classes, not the length); breached-password check since 12 October 2026 (fails open); lockout; failed signing attempts logged. Accounts created before 12 October 2026 can still sign with their account password.	Met

7. ALCOA+ statement

The nine ALCOA+ principles as they apply to the records YARDtwin creates — 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 accounts cannot sign; 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, printable as a controlled Visit Record PDF 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. 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 captured evidence alongside any transcribed value.
Accurate	Field validation, mandatory fields, referential integrity, expected-value comparison for seals and temperatures, and a weighbridge variance flag. AI-extracted values are shown to staff for 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 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 per record class (§8.1) with encrypted storage, point-in-time restore, nightly dumps and monthly long-term backups in geo-redundant EEA storage.
Available	Records are retrievable by authorised users throughout the subscription and exportable on demand, including at exit, so availability survives the vendor relationship.

8. Data integrity and retention

8.1 Retention schedule

How long YARDtwin keeps each class of data, as stated in the live privacy policy and DPA on 12 October 2026. Where a GxP period and data minimisation pull in opposite directions — gate photographs are the clearest case — the GxP record is retained and the personal-data element is minimised separately. GxP retention beyond the subscription is met on your exit export.

Data class	Retention	Basis
GxP records — gate, seal, cold chain, weighbridge, dock, departure	Life of the subscription; at the end, exported to you and then deleted within 30 days	Your GMP/GDP retention (EU GMP Ch. 4, EU GDP Ch. 9) continues on your export
Audit trail — GMP-relevant entries	At least 7 years after the event while the subscription runs; after exit see §9.3 [CONFIRM]	Annex 11 §9, Part 11 §11.10(e)
Audit trail — other entries	365 days	Operational
Account data	Life of the subscription; deleted within 30 days after it ends; pseudonymised on an erasure request	GDPR Art. 5(1)(e)

Data class	Retention	Basis
Driver name, phone, e-mail and licence details	On closed bookings anonymised after 365 days (booking kept); gate driver log identity fields 90 days — once you enable the retention schedule	GDPR Art. 5(1)(e)
Driver licence and face photos	Per-site setting 2–14 days, default 14; deleted automatically every 6 hours	GDPR Art. 5(1)(c)
Identity-check records (result and confidence, no image)	30 days; the decision stays in the audit trail	GDPR Art. 5(1)(c)
Integration message logs	Rolling window	Operational
Platform logs	90 days, EEA	Security operations
Backups	Point-in-time 7 days; nightly dumps 35 days; monthly backups up to 7 years, restored only to recover the service	Continuity; DPA §11

8.2 Enforcement — stated precisely

Running automatically for every site: deletion of driver licence and face photographs after the site's period (2–14 days, default 14, every 6 hours), the identity-check record purge (30 days) and the rolling integration-log window. The per-class retention engine separates the personal-data clock (identifying fields anonymised in place) from the GxP-record clock (the event, decision and hash survive to their own horizon); every run can be previewed as a dry run and every sweep is written to the audit trail. A daily scheduled sweep runs for tenants that turn it on, which needs a second administrator's approval; it is **off until you enable it**, and the driver-data rows in §8.1 marked "once you enable the retention schedule" depend on it. 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 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. The web edition of the DPA (v3.2) is published at yardtwin.com/dpa and accepted in the product. A signable edition (v4.0, with annexes for processing, security measures and sub-processors) is being finalised; a review copy is available from dpo@yardtwin.com, and a countersigned edition is issued once company registration is complete.

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, erasure and exit

Requests can be made through the public portal at yardtwin.com/data-request, confirmed by a single-use e-mailed link. Your tenant administrators can see and handle requests for your own tenant. YARDtwin can produce a machine-readable export of every record held for an e-mail address, and run an erasure that anonymises the person's user accounts and deletes their sessions, tokens, notifications, pending invitations and avatar; operational records you hold (bookings, gate and visit records, driver roster, contacts) are listed for you to act on.

Erasure and the audit trail — pseudonymised, not anonymised

GDPR Article 17(3)(b) preserves processing required by a legal obligation, and Annex 11 §9 requires the audit trail to survive. Audit entries therefore carry a pseudonymous actor token in place of the e-mail address, and erasure keeps those entries. The mapping from token to address is **kept** after erasure, so YARDtwin could still re-identify the actor: the trail is pseudonymised, not anonymised. Whether erasure should also clear the mapping is under review

[CONFIRM].

At contract end. You can export your data (JSON or CSV) within 30 days; operational data is then deleted within 30 days. YARDtwin has a whole-tenant offboarding routine, run by YARDtwin, that locks the tenant, deletes its data and files and issues a **certificate of deletion** (rows by category, files, what was kept and why, a record hash, and a statement on backups). It has been tested on test databases and not yet run for a production customer. Two points are stated precisely: data in backups expires with the backup (up to 7 years for monthly backups, which are restored only to recover the service); and the routine as built deletes the tenant's audit trail, whereas the web DPA (section 11) says GMP-relevant audit entries are kept pseudonymised for at least 7 years. Which applies is being reconciled **[CONFIRM]**; until it is, keep the audit trail from your exit export in your own archive.

9.4 Sub-processors

The register as published at yardtwin.com/subprocessors on 12 October 2026. Each provider acts under a data processing agreement. We give at least 30 days' notice of a new sub-processor, and you may object; if the objection cannot be resolved you may terminate the affected service without penalty (DPA section 6). Transfer impact assessments are being completed (target November 2026).

Sub-processor	Purpose	Location	Transfer safeguard
Microsoft Azure	Hosting, database and file storage	EEA (Sweden Central, Norway East; file copy in Norway West)	Microsoft Products and Services DPA; data stays in the EEA
Anthropic	AI reading of driver licences and documents (on by default; a site can switch it off); one-to-one gate face comparison (off by default); the in-app assistant	USA	SCCs and a transfer impact assessment (Anthropic does not participate in the EU-US Data Privacy Framework); API data not used for training, deleted within 30 days under its commercial terms
Resend	Transactional e-mail	USA	SCCs (its Data Privacy Framework participation is under review)
Stripe	Billing contact and payment data; YARDtwin stores no card numbers	EU / USA	SCCs; PCI DSS Level 1
Twilio	SMS and WhatsApp notifications, only if you enable them	USA	SCCs
Google and Microsoft	Sign-in identity data, only if you use those sign-in options	EU / USA	SCCs / EU-US Data Privacy Framework
ElevenLabs	Optional text-to-speech: voices the in-app assistant's replies, which can contain operational details such as vehicle registrations	USA	EU-US Data Privacy Framework and SCCs

The LinkedIn Insight Tag runs on public website pages only, after marketing-cookie consent; it receives no customer operational data and is not a sub-processor of it.

9.5 Impact assessments and breach notification

As controller you decide whether your processing needs a DPIA. A processor-side DPIA input pack covering driver identity data, licence and face images, vehicle registrations and AI processing is available for your own DPIA (draft, on request). We notify you of a personal-data breach affecting your data **without undue delay and within 48 hours** of becoming aware of it, and give an **initial notice within 24 hours** of any confirmed security incident affecting your data (DPA section 8; §15).

9.6 AI processing and governance

AI is used for four things: reading driver licences and shipping documents to pre-fill fields; an optional one-to-one comparison of a driver's gate photo with the licence or stored driver photo; the in-app assistant; and optional voice. The AI provider is Anthropic (Claude, through its commercial API); voice is ElevenLabs. YARDtwin trains no models.

- **No training on your data.** Anthropic's commercial terms exclude training on API data, and API data is deleted within 30 days under its standard terms.

- **People decide.** Extracted fields are shown to staff, who confirm or correct them before they become the record. No AI output makes a decision with legal or similarly significant effect on a person (GDPR Article 22). One AI exception exists, off by default: a site administrator can enable the assistant's "auto" mode, in which the assistant, used by a manager, applies dock assignments, move tasks and anomaly flags without confirming each one. Automatic gate check-in where a site configures number-plate recognition or unmanned check-in is rule-based, not AI, and is configured by you.
- **Switches, checked on the server and fail-closed.** AI document reading is on by default and a site administrator can switch it off for a site. A tenant administrator can switch off all external AI processing (Anthropic and ElevenLabs) for the whole tenant. Since 12 October 2026 every AI call checks these switches and is refused if a switch is off or cannot be confirmed. Where only the site switch is off, the assistant still answers but receives no live data from that site. Voice can be turned off per user, and is off for the tenant when external AI is off.

AI face comparison at the gate — exactly as it works today

Off by default. It runs only where a site turns it on. Where it is off, no face photo is sent to the AI provider and staff compare the driver with the licence photo themselves.

One-to-one. The driver's gate photo is compared with that driver's licence photo or one stored photo of that driver — never searched against other people.

Staff decide. The result is advice. Staff can admit a driver the comparison did not confirm, and must then give a reason; the server never blocks on the AI result.

Recorded server-side. Each comparison is recorded by the server, bound to the booking, site and user, usable once within 30 minutes, and cannot be supplied by the browser. The record (result and confidence) is kept 30 days; the decision is written to the audit trail.

No templates. No face template or biometric model is created or stored. Gate photos are deleted with the site's photo retention (2–14 days, default 14). A driver photo that you choose to keep on the driver roster is not covered by that purge. Drivers are shown a notice at the identity step. If you turn the comparison on, include it in your DPIA.

10. Security architecture

Controls as implemented, verified on 12 October 2026 against the production source code and the live Azure configuration. Amber rows are partial; red rows are not in place. The ones that matter most: the WAF carries no managed OWASP rule set, the database has a firewalled public endpoint, and there is no SIEM or 24/7 monitoring. All are in §17 with dates.

10.1 Network and edge

Control	Implementation	Status
TLS	TLS 1.2 minimum, 1.3 preferred at Front Door; HTTPS enforced; App Service minimum TLS 1.2	Verified live
HSTS	Two-year max-age, includeSubDomains, preload	Verified live
Origin lock	The application accepts traffic only from Azure Front Door; other sources are refused	Verified
WAF	Prevention mode with 5 custom rate-limit rules (Block) — login, signup, password reset, DSAR and a global ceiling; no managed OWASP rule set (needs the Premium tier)	Partial
Content Security Policy	One shared definition for web server and API; per-request nonce for scripts; no unsafe-eval; inline styles still allowed	Verified
Security headers	nosniff, X-Frame-Options, Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy, Cross-Origin-Resource-Policy	Verified
Database exposure	Public endpoint behind a firewall admitting Azure services and one administrator address; TLS required (minimum 1.2); private networking planned	Partial
Rate limiting	Per-route limits, tighter on authentication; counters shared across instances in the database (per-instance memory if the database is unavailable)	Active
Malware scanning	Uploaded files scanned on upload (Microsoft Defender for Storage)	Active
DNS	CAA records restrict certificate issuance; TLS reporting (TLS-RPT)	Active

10.2 Identity and access

Control	Implementation	Status
Unique identities	One account per person; shared accounts cannot apply e-signatures	Enforced
Role-based access	Role checks on the API, with the role-permission matrix compared against a saved reference on every regression run; a few read routes require sign-in but no specific role	Active
Multi-factor	TOTP and 8 single-use backup codes; MFA secrets encrypted (AES-256-GCM). Mandatory for YARDtwin platform administrators. "Require MFA" for all your staff is a tenant setting, off by default; SSO satisfies it when the identity provider asserts MFA (SAML/Entra, Microsoft) — Google sign-in never does	Active
Single sign-on	SAML 2.0 (for example Entra ID, Okta, Google Workspace), Google and Microsoft sign-in	Active

Control	Implementation	Status
Provisioning	SCIM 2.0 users and groups; groups mapped to roles (platform roles can never be mapped)	Active
Admin IP allow-list	Optional per tenant, for the administrator role	Available
Passwords	At least 12 characters (no tenant can lower it); upper, lower and digit by default (a tenant administrator can relax them); bcrypt cost 12; breached-password check (k-anonymity, fails open, tenant can switch off)	Enforced
Brute-force defence	5 failures per address and IP, or 30 per account in an hour, lock for 15 minutes; stored in the database; audited	Active
Sessions	1-hour access tokens; 7-day rotating refresh tokens; 30-day absolute limit; server-side idle expiry by role (about 2 hours for administrators, 20 minutes for gate and operator roles; you can shorten it); logout revokes the session	Active
MFA reset	Re-authentication and a reason; resetting an administrator needs a second administrator's approval within 24 hours; refused within 7 days of an e-mail change made by someone else	Active
API keys	Scoped, deny by default; new keys expire within the tenant maximum (365 days or less). Keys created before 12 October 2026 without an expiry still work and are flagged	Partial
YARDtwin access to your data	Without your grant, a platform administrator cannot see your users, sites, audit trail or files. Your administrator grants time-boxed access (1–72 hours, with a reason, revocable). Break-glass: 1 hour, reason required, all your administrators and dpo@yardtwin.com e-mailed. Every such access is written to your audit trail. Billing, usage, health and DSAR handling stay visible without a grant	Active
Tenant isolation	Every query scoped by tenant. An automated sweep tries every API endpoint with another tenant's identifiers: reduced on every pull request, full (at least 655 probes) before every release	Verified

10.3 Data protection

Control	Implementation	Status
Encryption at rest	AES-256 by Azure for database, file storage and backups (Microsoft-managed keys)	Active
Field-level encryption	Not offered for customer data. Application-level AES-256-GCM protects only MFA secrets and chat-webhook URLs	Not offered
Encryption in transit	TLS 1.2+ for client, API and integration traffic; database connections encrypted (TLS required). The application does not yet verify the database server certificate — in release	Partial
Key management	Azure Key Vault (RBAC, managed identity, purge protection); no secrets in source control; JWT and database secrets rotated October 2026	Active
Customer-managed keys	Not offered (Microsoft-managed keys)	Not available
SQL injection defence	Parameterised queries; static analysis on every pull request	Verified
Audit trail	Database triggers refuse UPDATE and DELETE except the controlled retention and offboarding purge; per-entity SHA-256 hash chain	Verified

Control	Implementation	Status
File storage	Private containers; no public access; files served through the application; versioning; malware scan on upload	Verified
Personal data in logs	E-mail addresses, phone numbers and tokens masked in application logs since 12 October 2026; names, licence numbers or registrations can still appear in free-text error messages	Partial

10.4 Monitoring and detection

Control	Implementation	Status
SIEM / 24x7 SOC	Not in place. No SIEM is attached to the log workspace, and nobody watches alerts around the clock	Not in place
Alerting	Azure Monitor alerts (5xx spikes, slow responses, availability tests), a schema-drift alert, Azure Service Health alerts; e-mail to the founder	Active
Breach monitor	Application worker every 5 minutes: failed-login spikes, many source addresses against one account, sign-ins from a new source; writes a breach register and e-mails the founder	Active
Customer SIEM export	Security-event export endpoint for your own SIEM	Available
Audit review	GxP flagging supports targeted audit-trail review	Active

11. Secure development and testing evidence

Every change goes through a pull request. The checks marked "blocks merge" are required by the repository's branch rules; the others run but cannot stop a change.

Control	Tool / mechanism	Gating
Static analysis (SAST)	Semgrep (OWASP Top 10, JavaScript, Node.js, React, secrets rules); new findings fail the pull request	Blocks merge
Dependency vulnerabilities	npm audit on backend (high and above) and frontend, with a documented exception register	Blocks merge
Secret scanning	gitleaks over the full history	Blocks merge
Container scanning	Trivy on the backend image, configured not to fail on findings; a blocking scan of the shipped image is planned	Advisory
Dynamic analysis (DAST)	OWASP ZAP baseline (passive) scan of the production site on every merge and nightly	Advisory
Software bill of materials	CycloneDX for backend and frontend npm dependencies on every run, kept 90 days; the container OS layer is not covered; a per-release SBOM is planned	Artefact
Dependency updates	Dependabot weekly version updates with a cool-down; vulnerability alerts on since 11 October 2026	Continuous
Functional regression	100-vehicle lifecycle gate, browser pass and isolation sweep on every pull request; 500-vehicle gate and full isolation sweep before release	Blocks merge and release
Code review	One person; no second human approval is required. AI-assisted adversarial review of high-risk changes	Not enforced
Production authorisation	Manual dispatch; staging must serve the exact commit; every instance verified to run the new build after the swap	Human gate
Deploy credential	Stored service-principal secret; an OIDC federated credential is planned	Planned

How the one-person risk is handled. The founder writes, approves and releases every change.

Compensating controls: the required checks above, a 500-vehicle regression before every release, an AI-assisted adversarial review of high-risk changes before merge, and a database-enforced audit trail. A part-time second human reviewer for high-risk changes and a contracted back-up engineer with runbooks are planned (§17).

11.1 Runtime platform

The production container runs **Node.js 20, which reached the end of upstream support in April 2026, and runs as root**. The database connection is encrypted, but the application does not yet verify the database server's certificate. A release that moves to Node.js 24 (pinned by digest), runs the API as a non-root user, verifies the database certificate (verify-full), pins the token-signing algorithm and validates configuration at boot is built, reviewed and in release (target October 2026 **[CONFIRM]**; no later than 13 November 2026).

11.2 Penetration testing and code audit

No penetration test by an independent firm has been carried out yet. An RFQ and scope for a grey-box test of the web application, API, tenant isolation and single sign-on, with a retest, is prepared (YT-SEC-RFQ-001); the proposed testing window is December 2026 **[CONFIRM]**, and the executive

summary will be shared under NDA.

In October 2026 we ran an internal white-box security code audit (YT-SEC-AUDIT-001): a review of the full source code with read-only checks of the live service. It found vulnerabilities, including two Critical. The Critical findings and most High findings were fixed and released to production in October 2026; the remaining items are scheduled. A summary is available under NDA. Earlier, in April 2026, internal functional security testing exercised more than 1,890 API calls — internal testing, not a penetration test.

11.3 Vulnerability remediation and disclosure

Findings are prioritised by severity against remediation targets (Critical 7 days, High 30 days, Medium 90 days **[CONFIRM]**) and tracked to closure; the written vulnerability-management procedure is part of the ISMS set being drafted. Researchers report to admin@yardtwin.com (published in security.txt); receipt is acknowledged within 2 business days and critical issues are patched within 7 days where possible.

12. CAIQ-Lite — completed

A lightweight Consensus Assessments Initiative Questionnaire across twelve domains: two Met, ten Partial, none a Gap. v1.1 marked five domains Met; logging and monitoring, privacy and AI governance are now Partial because the re-verification found less in place than v1.1 said, or paperwork still open. The reason for each Partial sits in its response and the remediation in §17. A full CAIQ v4 or SIG Lite in your own template is available 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; ISO/IEC 27001 programme with policies in draft for approval. Founder-led; no certificate yet.	Partial
Identity and access management	Unique identities, role checks, TOTP MFA (mandatory for platform administrators; tenant can require it), SAML 2.0, SCIM 2.0 with group mapping, admin IP allow-list, lockout, idle expiry, customer-approved support access.	Met
Encryption and key management	TLS in transit; AES-256 at rest by Azure (Microsoft-managed keys); Key Vault with purge protection; bcrypt. No field-level encryption of customer data, no customer-managed keys; database certificate verification in release.	Partial
Data residency and sovereignty	Customer data in EEA regions (Norway, Sweden); creation of resources outside approved European regions denied by Azure Policy; sub-processor transfers under SCCs.	Met
Application security	Shared CSP with nonces, security headers, parameterised queries, breached-password check, blocking SAST, dependency and secret scanning. WAF has custom rate-limit rules only; container scan advisory; Node.js 20 runtime until the release in progress.	Partial
Logging and monitoring	Azure Monitor and Service Health alerts, breach monitor, malware alerts, audit trail with hash chains, customer SIEM export. No SIEM, no 24/7 monitoring, no 12-month security-log archive.	Partial
Business continuity and resilience	Point-in-time restore, nightly and monthly backups in geo-redundant EEA storage, restore drill executed, 99.5% availability commitment. No high availability; RTO/RPO not contractual; founder is a key person.	Partial
Incident response	24-hour initial notice and 48-hour breach notice, breach register, anomaly detection, security.txt. Procedure in draft; tabletop exercise not yet run.	Partial
Privacy and data protection	Web DPA, RoPA, DSAR portal with tenant-admin handling, public sub-processor register with 30 days' notice, offboarding with a certificate of deletion. Transfer impact assessments and the signable DPA are being completed.	Partial
AI governance	No training on customer data, staff confirmation of extracted values, tenant and site switches checked on every call, face comparison off by default and recorded server-side. AI use policy in draft.	Partial
GxP and regulatory compliance	Annex 11 and Part 11 mapped clause by clause (§5, §6), ALCOA+ (§7), QMS set (§3), GxP release flags. QMS approval signature pending; re-validation on the current release planned.	Partial
Vendor viability and exit	JSON and CSV export, certificate of deletion, right to audit. Founder-led; insurance being arranged; no escrow agreement in place.	Partial

13. Certification and assurance status

The section reviewers turn to first. Nothing here is aspirational: if we do not hold something, 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	DPA, RoPA, DSAR routes, sub-processor register, EEA hosting	Compliance position, self-assessed
ISO/IEC 27001:2022	Not held — programme in progress . ISMS opened August 2026; policy set in draft for approval; certification audit Stage 2 planned for February 2027; certificate targeted Q1 2027.	Not held — in progress
SOC 2	Not held. A SOC 2 engagement can be considered on customer request after ISO/IEC 27001.	Not held
Independent penetration test	Not yet performed. RFQ and scope prepared (YT-SEC-RFQ-001); internal white-box code audit October 2026 (§11.2).	Planned
CSA STAR Level 1	Not published. A CAIQ v4 self-assessment is drafted for publication by January 2027; a completed CAIQ v4 is available on request.	Planned
Azure inherited assurance	Microsoft holds ISO/IEC 27001, SOC 1/2/3, ISO/IEC 27018 and others for the Azure services we consume. These are Microsoft's, not ours, and we do not present them as ours.	Inherited, infrastructure only

On "compliant" versus "certificate"

Annex 11 and 21 CFR Part 11 are regulatory expectations, not certification schemes — no body issues an "Annex 11 certificate". What can be evidenced is an implementation mapped clause by clause with artefacts behind it, which is what §5 and §6 are. ISO/IEC 27001 and SOC 2 *are* certification schemes. We hold neither, and we do not describe ourselves as holding either.

14. Business continuity, backup and recovery

This remains the weakest area of our posture, and we would rather you read our own assessment of it than discover it in a questionnaire. Since v1.1 a nightly database backup, geo-redundant file storage and a contractual availability commitment have been added. High availability has not.

Aspect	Current state
Availability commitment	99.5% monthly availability on paid plans , with service credits of 5%, 10% and 25% of the monthly fee below 99.5%, 99.0% and 95.0% (Terms of Service section 8). Measured by our own monitoring; a self-reported status page shows current status and incident history.
Point-in-time restore	Any point in the last 7 days (Azure PostgreSQL)
Daily backup	Nightly full dump since 12 October 2026, run in a container in Norway East and written to separate geo-zone-redundant storage (Sweden Central, replicated to Sweden South), kept 35 days. A test restore of the dump is planned (November 2026).
Long-term backups	Monthly full backup to the same storage under a time-based immutability policy of 2,555 days, which blocks deletion and overwrite while in force. The policy is not locked ; locking is planned. Scheduled runs succeeded on 1 September and 1 October 2026.
Uploaded files	Read-access geo-redundant storage (Norway East, copy in Norway West) with versioning and 14-day soft delete
Geo-redundant database backup	Not enabled at the database server . The nightly and monthly backups above are geo-replicated; server-level geo-backup needs the planned database rebuild.
High availability	Not enabled . The database is a single instance in one zone; a zone failure would be recovered by restore, not by automatic failover. The application runs on two instances.
Database tier	Burstable (B1ms) — appropriate to current load, not to a high-availability commitment
Release resilience	Staging-slot swap with a pre-swap commit check and post-swap build verification on every instance. Rollback is done by releasing the previous version again; a written rollback runbook is not yet in place.
RTO / RPO	Internal targets of $RTO \leq 4$ hours and $RPO \leq 24$ hours, not contractual. A database restore measured 6 minutes 43 seconds in August 2026; recovery from the loss of a whole Azure region has not been exercised.
Restore testing	Executed 1 August 2026 (YT-DR-LS-001): point-in-time restore of the production database to an isolated throwaway server, 19 of 19 checks including table counts, audit-trail immutability and signature-chain integrity. Production was not modified.
Key person	Founder-led. A business continuity plan (YT-ISMS-015, draft) covers founder unavailability; a contracted back-up engineer with runbooks is planned (December 2026).
Gate contingency	A manual gate procedure template (YT-SOP-GATE-001, draft) 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. Treat it as a risk to be mitigated or a condition to be met before go-live, not an assumption. The restore path is tested and evidenced and backups are geo-redundant in the EEA. The remaining workstream — a General Purpose database tier with zone-redundant HA, server-level geo-backup and private networking — is planned (target February 2027 **[CONFIRM]**), and we are happy to sequence it against a specific deployment.

15. Incident response and breach notification

Element	Commitment
Detection	Azure Monitor and Service Health alerts, malware alerts on uploads, and an application breach monitor every 5 minutes; alerts e-mail the founder. No SIEM and no 24/7 monitoring.
Classification	Severity model in the incident and breach procedure (YT-ISMS-014, draft) and YT-QMS-009
Security incident notice	Initial notice within 24 hours of a confirmed security incident affecting your data (DPA section 8)
Personal-data breach notice	Notification to you as controller without undue delay and within 48 hours of becoming aware, with the Article 33(3) content as it becomes available. Where YARDtwin is itself controller, it notifies the Data Protection Commission within the regulator's 72 hours.
GxP incident notification	Notification of incidents affecting the integrity or availability of GxP records, to support your own deviation handling
Investigation and CAPA	Root-cause investigation proportionate to severity; corrective and preventive actions tracked to closure (YT-QMS-010)
Vulnerability disclosure	security.txt (expires April 2027) and admin@yardtwin.com; acknowledgement within 2 business days
Post-incident	Written post-incident report available to affected customers on request
Tabletop exercise	Script prepared in YT-ISMS-014; first exercise planned by 13 November 2026; none recorded yet
Breach history	No personal-data breach has been notified to a customer or a supervisory authority to date [CONFIRM]

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
MFA requirement, session limits, password rules, IP allow-list	Capability; MFA always on for YARDtwin administrators	Sets tenant policy
AI switches and face comparison	Switches, fail-closed checks, defaults (face comparison off)	Decides; covers it in the DPIA
YARDtwin support access to your data	Requests, uses only within a grant, audited	Grants and revokes
User provisioning and periodic access review	SCIM, roles, user export	Owns the review
Signer accounts (§11.100)	Retires former signers' addresses; detects re-addressing	SOP: never re-address a signer to another person
§11.100(c) signature certifications	Technical control and wording	Issues certifications
Training and training records	Manuals, help centre, templates	Delivers and records
Audit-trail review	GxP flagging, filtering, export	Performs and documents review
Platform change control	YARDtwin, with release notes and opt-in GxP notices	Assesses impact on validated state
Records after exit	Export, then deletion with a certificate	Archives the export
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	Procedure template	Rehearses

17. Open items — the complete list

Everything not yet in place, in one table, with our own severity assessment and a date where one exists. 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
ISO/IEC 27001:2022	Not held. ISMS policies in draft for approval (November 2026); Stage 2 audit February 2027; certificate targeted Q1 2027.	High	Certification
High availability and contractual RTO/RPO	Database rebuild: General Purpose tier, zone-redundant HA, server-level geo-backup, private networking (target February 2027 [CONFIRM]). Availability is contractual (99.5%); RTO/RPO are not.	High	Infrastructure
Independent penetration test	Not yet performed. RFQ and scope prepared (YT-SEC-RFQ-001); proposed window December 2026 [CONFIRM] , with a retest.	High	Assurance
Runtime platform	Node.js 20 (end of support April 2026), container runs as root, database certificate not verified. Fix built and in release (§11.1).	Medium	In release
Separate staging database and storage	Staging still uses the production database server with test tenants. Separate database and storage created; switch-over in release (12–13 October 2026 [CONFIRM]).	Medium	In release
Pipeline hardening	Blocking image scan, per-release SBOM, OIDC deploy credential, locking the backup immutability policy. Not started; target 13 November 2026 [CONFIRM] .	Medium	Planned
Security monitoring	No SIEM, no 24/7 monitoring, no 12-month security-log archive. Archive planned with the ISMS go-live (November 2026).	Medium	Planned
Code review and key person	One person approves and releases code; second human reviewer for high-risk changes planned (January 2027 [CONFIRM]); back-up engineer with runbooks planned (December 2026).	Medium	People
Managed WAF rule set	Five custom rate-limit rules only; a managed OWASP rule set needs the Premium edge tier. Planned with the production rebuild.	Medium	Edge
Audit trail after exit	Offboarding as built deletes the tenant's audit trail; the web DPA says GMP-relevant entries are kept pseudonymised for 7 years. Being reconciled [CONFIRM] .	Medium	Privacy / GxP
Re-validation on the current release	The Life Sciences validation pack was executed on v-Is-1.0 (August 2026); re-execution on the current release targeted January 2027.	Medium	Validation
Data-protection paperwork	Transfer impact assessments (target November 2026); signable DPA v4.0 being finalised; countersigned edition once company registration is complete.	Medium	Privacy
Company and insurance	Company registration details on request. Professional indemnity and public liability cover are being arranged, and cyber cover is arranged at the limits your contract requires; certificates are provided before contract signature. No cover is in force today.	Medium	Commercial
Incident procedure and tabletop	YT-ISMS-014 in draft for approval; first tabletop exercise by 13 November 2026.	Medium	Operations
Customer-managed keys (CMK/BYOK)	Not offered; can be added with the database rebuild if a contract requires it.	Medium	Engineering
SOC 2	Not held; considered on customer request after ISO/IEC 27001.	Low	Certification

Item	Current position	Severity	Type
QMS approval signature	Ten QMS documents review-signed 2 August 2026; approval signature planned October 2026 [CONFIRM] .	Low	Quality
Erasure and the actor mapping	Erasure keeps the audit actor token-to-address mapping, so the trail is pseudonymised, not anonymised (§9.3). Under review.	Low	Privacy
Older API keys and signer accounts	API keys created before 12 October 2026 without an expiry still work (flagged); accounts created before that date can sign with their account password.	Low	Engineering
Free text in logs	Names, licence numbers or registrations can still appear in free-text error messages in logs (90 days, EEA).	Low	Engineering
Backup restore evidence	A test restore of the nightly dump is planned (November 2026); region failover has not been exercised.	Low	Operations
Independent availability monitoring	Availability is measured by our own monitoring and shown on a self-reported status page; independent monitoring with public history is on the roadmap.	Low	Operations
Escrow	Offered for enterprise contracts; no escrow agreement in place.	Low	Commercial
Data protection officer	No statutory DPO designated: the Article 37(1) conditions do not apply. A named responsible person is reachable through the role mailbox dpo@yardtwin.com; we publish the address rather than the person's name.	Low	Governance

How to read this table

Three High items: ISO/IEC 27001 (clock-bound — an ISMS must operate before it can be audited), high availability (an infrastructure change we can sequence against a specific deployment), and the independent penetration test, raised from Medium in v1.1 because nothing independent has yet tested the platform. Since v1.1 the core per-record printout, the scheduled retention sweep, the availability commitment, the breached-password check and the SSO signing gap have closed. The GxP record controls of §5 to §8 are implemented and verifiable; the open items that touch them — the audit trail after exit and re-validation on the current release — are stated as they are.

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

You may audit YARDtwin remotely or on site with at least 30 days' notice (DPA section 12), and audit the QMS and development process under the Quality Agreement. Once ISO/IEC 27001 certification is achieved we will offer the certificate as substitute evidence. Short of an audit, the following are available on request — several under a mutual non-disclosure agreement:

- The ten-document QMS set; the 19-document Life Sciences validation pack with executed IQ/OQ/PQ records; the restore test record (YT-DR-LS-001) and backup run records
- Records of Processing Activities; the DPA v4.0 review copy (from dpo@yardtwin.com), sub-processor register, retention schedule and DPIA input pack
- The Quality Agreement template, AI use policy and EU AI Act position, and ethics policies (drafts)
- ISMS documents and the ISO/IEC 27001 roadmap (drafts, under NDA)
- A summary of the October 2026 internal code audit (under NDA), and the pen-test scope; the executive summary of the independent test once it has been carried out
- OQ protocols and executed test evidence, including SAP EWM conformance runs; a CycloneDX SBOM of npm dependencies for a nominated build
- The Azure Policy residency assignment and other Azure settings (by demonstration); a completed CAIQ v4 or SIG Lite in your own template
- Company registration details, and insurance certificates before contract signature

Purpose	Contact
Vendor assurance, QMS requests, audit scheduling	admin@yardtwin.com
Privacy, DPA and data subject matters (data-protection contact)	dpo@yardtwin.com
Security disclosure	admin@yardtwin.com · yardtwin.com/.well-known/security.txt
Published trust information	yardtwin.com/security · /subprocessors · /supplier-documents · /dpa · /sla · /status

Document control

Prepared by YARDtwin (the founder). Every status in this pack was verified on 12 October 2026 against the source code running in production (build fd722d8), the live Azure configuration and the public pages listed above; the verification ledger is kept with the document source. This document is provided for vendor-assessment purposes; it is not a contractual warranty, and contractual commitments are those in the Terms of Service, the Data Processing Agreement and any master subscription agreement. It is reviewed at least every six months and reissued whenever a status in §13 or §17 changes. Items marked **[CONFIRM]** are stated in their weaker form until confirmed. **v1.2** corrects the overstated statements of v1.1 and v1.1.1 (see "Changes since v1.1"); v1.0, v1.1 and v1.1.1 are withdrawn — please discard them.

Document	Code	Version	Date	Status
Vendor Assurance Pack	YT-VAP-001	v1.0	27 July 2026	Withdrawn
Vendor Assurance Pack	YT-VAP-001	v1.1	23 August 2026	Withdrawn — overstated controls
Vendor Assurance Pack	YT-VAP-001	v1.1.1	26 September 2026	Withdrawn — wording only
Vendor Assurance Pack	YT-VAP-001	v1.2	12 October 2026	Current; next review April 2027