COMPLIANCE, NOT SCARY

PIM Sync **Compliance Checklist**

A plain-English checklist for selling into the EU and UK without fear. Print it, tick the boxes, and keep it with your store records.

This checklist is practical guidance, not legal advice. For scope questions — especially CRA applicability — confirm with counsel.

Part 1 — EU Omnibus Directive (price transparency)

The rule in one sentence: whenever you show a discount, you must also show the lowest price the product had in the previous 30 days.

WHAT PIM SYNC ALREADY DOES FOR YOU

- [x] Logs every price change (discounts, FX re-pricing, manual edits) to an immutable price history
- [x] Computes the Omnibus price (lowest in prior 30 days) automatically on every change
- [x] Re-audits EU and UK markets daily and flags expired or missing 30-day windows
- [x] Blocks publishing a compare-at price when no valid 30-day history exists
- [x] Shows “Lowest price in last 30 days” on product pages via the Omnibus metafield

WHAT YOU STILL CHECK YOURSELF

- [ ] Sale banners and promo emails reference the Omnibus price, not an inflated “was” price
- [ ] Manual price overrides get a note in the price log (the override restarts the 30-day window)
- [ ] Your theme displays the Omnibus badge wherever a discount is visible
- [ ] Non-EU/UK markets that copy EU pricing content are reviewed separately

Why it matters: national regulators can fine up to 4% of annual turnover for pricing violations under the Omnibus enforcement regime.

Part 2 — EU Cyber Resilience Act (CRA) documentation

The CRA (Regulation (EU) 2024/2847) applies to software products sold into the EU. Reporting obligations apply from 11 September 2026; full obligations from 11 December 2027. Most apps are “default category,” which allows self-assessment — no external auditor needed.

DOCUMENTATION TO PREPARE, IN ORDER

- [ ] **Scope memo (1 page).** Are you the “manufacturer”? Is the product default category? Get this reviewed before investing further.
- [ ] **SECURITY.md / vulnerability disclosure policy.** A contact address, response window, and safe-harbor language for reporters.
- [ ] **SBOM (software bill of materials).** Machine-readable (CycloneDX or SPDX), covering at least top-level dependencies. Generate it in CI so it stays current.
- [ ] **Dependency monitoring.** Automated vulnerability alerts (e.g. Dependabot) plus a triage-and-fix process with target timelines.
- [ ] **Support period declaration.** How long you commit to free security updates (CRA minimum: 5 years or expected product lifetime).
- [ ] **Secure update mechanism doc.** How fixes reach users. Centrally deployed apps update instantly server-side — say so; it is a strength.
- [ ] **Cybersecurity risk assessment.** Map the CRA Annex I essential requirements (secure defaults, access control, logging, data minimization, secure deletion) to what your product does.
- [ ] **Incident reporting runbook.** Actively exploited vulnerability or severe incident: early warning within 24 hours, notification within 72 hours, final report within 14 days. Already in force from September 2026.
- [ ] **User security information.** Intended use, security properties, support period, and where to report vulnerabilities — in your README and app listing.
- [ ] **EU Declaration of Conformity.** Last step, after everything above is stable.

Part 3 — Firmware and connected devices (the highest-risk category)

If your store sells anything with firmware — smart home gear, wearables, chargers, routers, toys, appliances, dev boards — the CRA applies to the **device**, not just your app. Firmware is historically shipped once and abandoned, which is precisely the behavior the CRA was written to end. Many device categories (network equipment, smart locks, home assistants) are “important products” Class I or II, which means harmonized standards or third-party conformity assessment — not just self-assessment.

THE HARD RULES

- [ ] **Field-updatable, or not sellable.** Every device must have a working mechanism to receive security updates in the field. If firmware cannot be patched after sale, it cannot be placed on the EU market.
- [ ] **Signed and verified updates.** Firmware updates must be authenticated (signature verification on-device) with rollback protection. Unsigned OTA is a non-conformity.

- [ ] **No default passwords.** Devices must ship secure-by-default: unique credentials per unit or forced setup, no hardcoded accounts, debug interfaces disabled in production.
- [ ] **No known exploitable vulnerabilities at release.** Check the firmware and its components (RTOS, radio stacks, bundled libraries) against known CVEs before every release.
- [ ] **Firmware SBOM.** The bill of materials must cover firmware components too — the RTOS, bootloader, connectivity stacks, and vendored libraries, not just cloud code.
- [ ] **Declared support period per device.** Minimum 5 years (or expected lifetime) of free security updates, stated at the point of sale. Security updates must remain available after the last unit ships.
- [ ] **Published end-of-life policy.** What happens when support ends: final firmware version, disclosure of remaining risk, and whether the device degrades gracefully or keeps working offline.
- [ ] **Separate security updates from feature updates** where technically feasible — users must be able to take the patch without accepting new features.
- [ ] **White-label and imported devices count.** If you brand or import a device, you take on manufacturer or importer obligations — "the ODM handles firmware" is not a defense. Get the update commitment and SBOM in the supply contract.
- [ ] **Same reporting clock.** An actively exploited firmware vulnerability triggers the 24-hour early warning / 72-hour notification, identical to software.

Why this is the most destructive risk: a compromised firmware fleet cannot be patched by taking a server down. Every shipped unit is an attack surface in someone's home until it is updated or destroyed — and non-compliant products can be recalled or banned from the market, with fines up to EUR 15 million or 2.5% of global turnover.

Quick reference

REGULATION	WHAT IT GOVERNS	KEY DEADLINE
Omnibus Directive (2019/2161)	Discount price transparency	In force now
GDPR	Personal data	In force now
CRA (2024/2847) — reporting	Exploited vulns and incidents	11 Sep 2026
CRA (2024/2847) — full	Product security + documentation	11 Dec 2027
CRA — important products (Class I/II)	Connected devices, firmware	Stricter conformity, same dates

---