Audit Report: Odoo Manufacturing ERP Partner in Europe | Avalah — Odoo Gold Partner

Website: https://avalah.ee/
Date: 26.10.2026
Audit Coverage: 100% — all sources returned data
Confidence: medium

Pages Audited (1 of 1):

- https://avalah.ee/

Summary of results

Overall Score: 76 / 100
Status: **Needs Improvement**

PSI mobile 73 vs desktop 100 — a 27-point gap driven almost entirely by LCP 5.3 s and FCP 3.23 s on mobile (desktop 0.7 s / 0.69 s), while CLS 0.000 and TBT 82 ms are clean. Field CrUX is far kinder (LCP 1042 ms p75, FCP 1021 ms p75), so the lab penalty is throttling-sensitive, but mobile-first scoring still applies. Accessibility is essentially perfect — axe 0 violations / 41 passes and Lighthouse a11y 100 — though 19 contrast nodes and 1 ARIA node were left undetermined, and W3C reports 4 markup errors including an `area-hidden` typo that silently breaks the header search form's ARIA hiding. Security basics FAILED (HSTS, clickjacking, CSP, Referrer-Policy, Permissions-Policy, COOP, CORP all missing; 4/4 cross-origin scripts lack SRI), which caps the score below 90. Image assets are a non-issue — only 3 SVGs, no raster images, no missing alt — so the drag comes from JS (122 KB unused in global.js, 188 KB gtag) and one render-blocking cookieyes script in `<head>`.

Per-page scores

 Needs Improvement · https://avalah.ee/

Score	Performance	Accessibility	Best Practices	SEO	Security
76	73	100	100	100	FAILED

PageSpeed Insights — Mobile vs Desktop

*Lower is worse for Performance; higher is worse for LCP and CLS. Worse value is **bolded**.*

Strategy	Performance (M / D)	LCP (M / D)	CLS (M / D)
Mobile vs Desktop	**73** / 100	**5.29 s** / 688 ms	0.000 / **0.000**

Optimization Checklist

2 of 3 passing — 2 pass · 1 warn · 0 fail · 5 n/a

Item	Status	Detail
Page caching plugin / CDN active	**Pass**	Caching plugin detected (WP Rocket) + CDN Cloudflare/Kinsta
Response compressed (gzip / brotli)	**Pass**	Document response is compressed with br.
Images lazy-loaded	N/A	No raster elements found (3 SVGs excluded).
Hero image eagerly loaded	N/A	No raster elements found (3 SVGs excluded).
Hero is a real (not a CSS background-image)	N/A	No CSS background-images detected on raster-image-eligible elements.
Responsive images (srcset /)	N/A	Only 0 raster images on the page (3 SVGs excluded) — responsive-image rule does not apply.
Reasonable number of image sizes	N/A	Too few raster images to evaluate srcset width variety.
JS scripts not blocking in	**Warn**	1 render-blocking script in . Move to footer or add defer/async.

Fixes

Priority 1: Critical

Immediate action — impacts user experience, search rankings, or site safety.

1A. Cut mobile LCP (5.3 s) and FCP (3.23 s) `Performance`

- **Impact:** LCP, FCP, Speed Index, TTI
- **Problem:** Mobile LCP is 5.3 s (Lighthouse score 0.22, weight 25) and FCP 3.23 s versus 0.7 s / 0.69 s on desktop; Speed Index 3.52 s and TTI 5.3 s.
- **Solution:**
  - Remove the render-blocking `<script src="https://cdn-cookieyes.com/client_data/.../script.js">` from `<head>` — add `defer` or load it after first paint.
  - Preload the LCP element (hero image/font) with `<link rel="preload" as="image" fetchpriority="high">` or `as="font" crossorigin`.
  - Inline critical above-the-fold CSS and defer the 4 external stylesheets.
  - Delay GTM (`gtag/js?id=G-YV6V380PD6`, 188 KB, 105 ms long task) until after `load` or first interaction.
  - Re-measure with PSI mobile after each change; target LCP ≤2.5 s.

1B. Add HSTS and clickjacking protection `Security`

- **Impact:** Transport security, clickjacking
- **Problem:** Security basics verdict is FAILED: Strict-Transport-Security is missing and neither X-Frame-Options nor CSP frame-ancestors is set, so the page can be framed.
- **Solution:** Send from the origin (Kinsta/Cloudflare) or via `.htaccess`:

  ```
  Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
  Header always set X-Frame-Options "SAMEORIGIN"
  ```

  Or, if you ship a CSP, use `frame-ancestors 'self'` instead of X-Frame-Options. Then submit the domain to hstspreload.org once max-age ≥ 1 year.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Eliminate unused and legacy JavaScript `Performance`

- **Impact:** TBT, LCP, main-thread work
- **Problem:** `global.7edaaf903ba7302f.js` wastes 122 KB and `gtag/js` 74 KB; Lighthouse flags `legacy-javascript-insight` with ~13 KiB savings and a 77 ms long task from global.js.
- **Solution:**

- Audit `global.js` for unused modules (likely jQuery + jQuery Migrate + theme helpers) and split per-page bundles.
- Drop `jquery-migrate.min.js` if no legacy plugin depends on it.
- Replace legacy polyfills with `browserslist` targeting modern browsers so the build stops shipping ES5 transpilation.
- Load GTM only after consent/interaction rather than on every page view.

2B. Fix forced reflow `Performance`

- **Impact:** LCP, INP, rendering
- **Problem:** Lighthouse reports `forced-reflow-insight` at score 0.00 — synchronous layout reads/writes are blocking rendering on mobile.
- **Solution:**
  - Find the offending pattern in `global.js` / theme JS: interleaved `offsetWidth` / `getBoundingClientRect()` reads followed by style writes.
  - Batch all DOM reads first, then all writes, or wrap in `requestAnimationFrame`.
  - Avoid measuring layout inside scroll/resize handlers.

2C. Add Subresource Integrity to cross-origin scripts `Security`

- **Impact:** Supply-chain tampering
- **Problem:** 4 of 4 cross-origin scripts lack an `integrity` attribute (jsDelivr iframemanager, CookieYes, Google Tag Manager).
- **Solution:** Add SRI hashes to pinned versions:

  ```
  <script
  src="https://cdn.jsdelivr.net/gh/orestbida/iframemanager@1.3.0/dist
  /iframemanager.js"
          integrity="sha384-..." crossorigin="anonymous" defer>
  </script>
  ```

  For GTM/CookieYes, self-host or pin a version you control — their URLs are unversioned and cannot be SRI-pinned reliably.

2D. Harden the WordPress install surface `Best Practices`

- **Impact:** Attack surface, brute-force exposure
- **Problem:** `/wp-admin/install.php` is reachable and the login form is served on the default `/wp-login.php` path.
- **Solution:**
  - Block the installer in `.htaccess`:

```
<Files "install.php">
  Require all denied
</Files>
```

- Move login behind a custom path (WPS Hide Login or a server-level rewrite) and add rate limiting / 2FA.
- Keep xmlrpc.php blocked (already passing) and continue hiding the WP version.

2E. Fix the four W3C markup errors that affect assistive tech `Accessibility`

- **Impact:** ARIA correctness, screen-reader output
- **Problem:** W3C reports `area-hidden` (typo for `aria-hidden`) on `<form id="header-search">`, `aria-label` on `<label for="theme-toggle">`, an empty `name=""` on the theme-toggle checkbox, and a `<p>` nested inside `<span class="copyright">`.
- **Solution:**
  - Rename `area-hidden="true"` → `aria-hidden="true"` on the header search form (or better, use the `hidden` attribute so focusable children are removed from the tab order too).
  - Remove `aria-label` from `<label for="theme-toggle">`; put the accessible name on the checkbox itself or use visible text.
  - Give the theme-toggle input a real `name` value.
  - Change `<span class="copyright"><p>…</p></span>` to `<div class="copyright"><p>…</p></div>`.

2F. Emit valid structured data and fix tap targets `SEO`

- **Impact:** Rich results eligibility, mobile usability
- **Problem:** PSI flags `structuredData` and `tapTargets` as failing SEO audits; the single JSON-LD block is parsed with type "Unknown".
- **Solution:**
  - Replace the JSON-LD block with a valid `Organization` + `Service` / `ProfessionalService` graph using schema.org types and `@context: https://schema.org`.
  - Validate with the Rich Results Test and Schema Markup Validator.
  - Enlarge interactive targets to ≥44×44 px (WCAG 2.5.8) — check the header nav and footer link rows.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Add CSP, Referrer-Policy, Permissions-Policy, COOP/CORP `Security`

- **Impact:** XSS defense-in-depth, referrer leakage
- **Problem:** CSP, Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing. Site signals show no auth, payments, user content or e-commerce, so XSS impact is limited — hence P3.
- **Solution:** Start with the cheap, zero-risk headers:

  ```
  Referrer-Policy: strict-origin-when-cross-origin
  Permissions-Policy: camera=(), microphone=(), geolocation=()
  Cross-Origin-Opener-Policy: same-origin
  ```

  If you later add a login or user content, deploy a nonce-based CSP rather than a flat allowlist:

  ```
  Content-Security-Policy: script-src 'nonce-{random}' 'strict-
  dynamic'; object-src 'none'; base-uri 'none'; frame-ancestors
  'self'
  ```

3B. Verify the 19 undetermined color-contrast nodes `Accessibility`

- **Impact:** WCAG 1.4.3 contrast
- **Problem:** axe returned 0 violations but left 19 nodes with undetermined color contrast (gradients/alpha) and 1 node with an invalid ARIA attribute value.
- **Solution:**
  - Manually check contrast on the 19 flagged nodes with a contrast picker against the rendered background.
  - Resolve the `aria-valid-attr-value` node — likely the same `area-hidden` typo reported by W3C.

3C. Disambiguate repeated vague link text `SEO`

- **Impact:** Anchor-text relevance, screen-reader navigation
- **Problem:** 58 anchors include "book a consultation" ×3, "services" ×2, "solutions" ×2, "references" ×2, "about us" ×2 and "contact" ×2.
- **Solution:**
  - Add distinguishing context to each repeated link, e.g. `Book a consultation about Odoo Manufacturing`.

    - Where the visible text must stay short, add `aria-label` with the fuller description.

3D. Give the 3 SVG images explicit dimensions `Performance`

- **Impact:** CLS, layout stability
- **Problem:** All 3 images (CookieYes revisit/close/powered-by SVGs) lack `width` / `height` attributes.
- **Solution:**

  ```
  <img src=".../close.svg" alt="" width="24" height="24"
  loading="lazy">
  ```

  Also set `alt=""` on the close icon, which currently has an empty alt but is a functional button — give it an accessible name instead.