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: high

Pages Audited (1 of 1):

- https://avalah.ee/

Summary of results

Overall Score: 83 / 100
Status: **Needs Improvement**

Performance is genuinely strong — PSI mobile 91 / desktop 98, CLS 0.000, TBT 151 ms, and a 217 KB total page weight — but FCP 2.58 s and TTI 4.6 s are held back by a render-blocking cookieyes script in plus 122 KB of unused theme JS and 74 KB of wasted gtag. Accessibility scores 100 in Lighthouse with 0 axe violations, yet the W3C validator reports 4 real markup errors, including an `area-hidden` typo on the header search form and an invalid `aria-label` on the theme-toggle `<label>`, so the a11y picture is not as clean as axe suggests. Image assets are effectively a non-issue (3 SVGs, no raster images, 0 missing alt), so that budget is full credit. The Security basics verdict is FAILED — HSTS and clickjacking protection are missing at the basic tier, with CSP, Referrer-Policy, Permissions-Policy, COOP and CORP also absent — which caps the score below 90. Lab TTFB (4 ms, edge cache HIT) diverges sharply from field p75 802 ms, so real-user server latency is worth watching even though the lab looks perfect.

Per-page scores

 Needs Improvement · https://avalah.ee/

Score	Performance	Accessibility	Best Practices	SEO	Security
83	91	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	**91** / 98	**2.58 s** / 693 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. Add HSTS and clickjacking protection `Security`

- **Impact:** Transport security, clickjacking exposure
- **Problem:** Security basics 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 both headers at the edge/origin (Cloudflare Transform Rules or Kinsta/Apache):

  ```
  Strict-Transport-Security: max-age=31536000; includeSubDomains;
  preload
  Content-Security-Policy: frame-ancestors 'self'
  X-Frame-Options: SAMEORIGIN
  ```

  `frame-ancestors` is the modern control; keep `X-Frame-Options` as a fallback for older browsers. Submit to hstspreload.org once the max-age is stable.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Remove the render-blocking cookieyes script and trim unused JS `Performance`

- **Impact:** FCP, TTI, TBT, Speed Index
- **Problem:** FCP is 2.58 s (score 0.64, weight 10) and TTI 4.6 s; the checklist flags `cdn-cookieyes.com/.../script.js` as the single render-blocking script in , and PSI reports 122 KB wasted in `global.7edaaf903ba7302f.js` plus 74 KB in gtag.
- **Solution:**
  - Add `defer` (or load on interaction) to the cookieyes loader, or self-host it and inject after first paint.
  - Split `global.js` so only above-the-fold behaviour ships in the critical path; drop jQuery Migrate if nothing depends on it.
  - Load gtag after `load` or via a consent-gated snippet rather than in the initial bundle.
  - Target: FCP under 1.8 s on mobile.

2B. Fix the 4 W3C markup errors affecting assistive tech `Accessibility`

- **Impact:** Screen-reader semantics, form labelling
- **Problem:** W3C reports 4 errors: `area-hidden` (typo for `aria-hidden`) on the header search `<form>` at line 435, an empty `name=""` on the theme-toggle checkbox at line 1042, `aria-label` on a `<label for="theme-toggle">` at line 1043, and a `<p>` nested inside a `<span>` at line 1087.

- **Solution:**
  - Rename `area-hidden="true"` → `aria-hidden="true"` on `#header-search` so the collapsed search form is actually hidden from AT.
  - Give the theme-toggle checkbox a real `name` (e.g. `name="theme-toggle"`).
  - Remove `aria-label` from the `<label>`; put the accessible name on the input or use visually-hidden text inside the label.
  - Replace the `<span>` wrapping `<p>2026 © …</p>` in the footer with a `<div>`.

2C. Ship valid, typed structured data `SEO`

- **Impact:** Rich results eligibility, entity understanding
- **Problem:** PSI's modeled `structuredData` audit fails and the single JSON-LD block is reported with type "Unknown", despite the site being an Odoo Gold Partner with clear Organization/Service intent.
- **Solution:** Add explicit `@type` values and validate with the Rich Results Test:

  ```
  {"@context":"https://schema.org","@type":"Organization","name":"Ava
  lah","url":"https://avalah.ee/","logo":"…","sameAs":["…"]}
  ```

  Also consider `Service` / `ProfessionalService` for the ERP consulting offering and `BreadcrumbList` where applicable.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Add a nonce-based Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is missing (advanced-tier fail). Site signals show no auth, payments, or user-generated content on this page, so XSS impact is limited — hence P3 rather than P1.
- **Solution:** Deploy a nonce + `'strict-dynamic'` policy rather than a flat allowlist:

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

  Note the page loads scripts from googletagmanager.com, cdn.jsdelivr.net and cdn-cookieyes.com — inventory these before enforcing.

3B. Add Referrer-Policy, Permissions-Policy, COOP/CORP and SRI `Security`

- **Impact:** Information leakage, cross-origin isolation, third-party script tampering
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing, and 4 of 4 cross-origin scripts lack an `integrity` attribute.
- **Solution:**

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

  For the jsDelivr iframemanager script, pin a version and add `integrity="sha384-…" crossorigin="anonymous"`. gtag and cookieyes cannot be SRI-pinned reliably — self-host or accept the gap.

3C. Harden the WordPress install surface `Best Practices`

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

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

  - Move login behind a custom path (WPS Hide Login) and add rate limiting / 2FA.
  - Keep the existing wins: xmlrpc blocked, no version disclosure, no user enumeration.

3D. Enlarge mobile tap targets and disambiguate repeated link text `Accessibility`

- **Impact:** Mobile usability, WCAG 2.5.8 / 2.4.4
- **Problem:** PSI's modeled `tapTargets` audit fails, and the page repeats vague anchors — "book a consultation" ×3, "services" ×2, "solutions" ×2, "references" ×2, "contact" ×2.
- **Solution:**
  - Ensure interactive elements are at least 44×44 px with adequate spacing on mobile.

- Disambiguate repeated anchors with `aria-label` or visually-hidden context, e.g. `<a href="/services/odoo-manufacturing" aria-label="Odoo manufacturing services">Services</a>`.

3E. Drop legacy JavaScript and jQuery Migrate `Performance`

- **Impact:** Main-thread work, TBT, bundle size
- **Problem:** PSI's `legacy-javascript-insight` estimates 13 KiB of savings, and `jquery-migrate.min.js` plus jQuery are still loaded and appear among the slowest requests (127 ms / 107 ms).
- **Solution:**
  - Remove `jquery-migrate.min.js` once plugins are confirmed compatible.
  - Set an explicit modern browserslist target so the build stops transpiling to ES5 and stops shipping polyfills.
  - Audit the 23 scripts (6 defer, 2 async, 1 blocking) for anything unused on this page.