Audit Report: Avaleht - Restate

Website: https://restate.ee/
Date: 13.11.2026
Audit Coverage: 100% — all sources returned data
Confidence: high

Pages Audited (1 of 1):

- https://restate.ee/

Summary of results

Overall Score: 92 / 100
Status: **Excellent**

What is pulling the score down

Signal	Points	Evidence
Performance 94	−2.4	weighted 40% of 6 points lost
HTML validation	−2	7 W3C errors
Accessibility 95	−1.5	weighted 30% of 5 points lost
SEO 92	−1.2	weighted 15% of 8 points lost
Image delivery	−1	PSI estimates 495 KiB image-delivery savings (mobile)
Advanced security headers	0	Failing: Content-Security-Policy present, CSP is strict, Cross-Origin-Opener-Policy, Cross-Origin-Resource-Policy
Page score	**92**	100 − 8.1 → 92

HTML validation (7 W3C errors, −2) is the largest single deduction, followed by mobile Performance 94 (−2.4) where lab LCP is 2.7 s versus 0.6 s on desktop and PSI estimates 495 KiB of image savings; SEO 92 (−1.2) is driven by the missing meta description. Field data is healthy (CrUX p75 LCP 887 ms, TTFB 400 ms), so the remaining work is polish rather than breakage.

Per-page scores

Excellent · https://restate.ee/

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
95	92	94	95	100	92	PASS

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	**94** / 100	**2.72 s** / 633 ms	0.000 / **0.000**

Optimization Checklist

6 of 7 passing — 6 pass · 0 warn · 1 fail · 1 n/a

Item	Status	Detail
Page caching plugin / CDN active	**Pass**	Caching plugin detected (WP Rocket)
Response compressed (gzip / brotli)	**Pass**	Document response is compressed with gzip.
Images lazy-loaded	**Pass**	All non-hero raster images use loading="lazy".
Hero image eagerly loaded	**Fail**	Hero image has loading="lazy", which delays LCP (inferred from DOM order/size — Lighthouse LCP element unavailable). Use loading="eager" (or omit loading) and add fetchpriority="high".
Hero is a real (not a CSS background-image)	N/A	No CSS background-images detected on raster-image-eligible elements.
Responsive images (srcset /)	**Pass**	6/6 raster images use srcset or (100%).

Item	Status	Detail
Reasonable number of image sizes	**Pass**	6 distinct srcset widths.
JS scripts not blocking in	**Pass**	No render-blocking scripts in .

Fixes

Priority 1: Critical

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

1A. Fix W3C validation errors `Best Practices`

- **Impact:** HTML validation row (−2), HTML validity, parser robustness
- **Problem:** The W3C validator reports 7 errors, all of the same kind: a `<script type="text/rocketlazyloadscript" … defer>` data block carrying a `defer` attribute (first at line 957).
- **Solution:** WP Rocket's lazyload rewrite emits a non-JS `type` together with `defer`, which HTML forbids.
  - Exclude the affected scripts from Delay JS execution in WP Rocket, or
  - Update WP Rocket to a version that emits `type="rocketlazyloadscript"` without `defer`.
  - Re-run the validator until the 7 errors drop to 0.

1B. Serve images in WebP/AVIF at the right size `Performance`

- **Impact:** Image delivery row (−1), LCP, Speed Index, total page weight
- **Problem:** PSI estimates 495 KiB of image-delivery savings on mobile; the runtime capture shows 6 images totalling 590.6 KB, and the footer PNGs (e.g. chicken-dollar.png at 358×720) are served as PNG.
- **Solution:**
  - Convert the footer PNGs to WebP/AVIF and keep the existing `srcset` widths.
  - Serve via `<picture>` with a raster fallback:

```
<picture>
  <source type="image/webp" srcset="hammer-233.webp 233w, hammer-
466.webp 466w" sizes="233px">
  <img src="hammer.png" alt="" width="233" height="382"
```

```
loading="lazy">
</picture>
```

1C. Load the hero image eagerly `Performance`

- **Impact:** LCP, Speed Index
- **Problem:** The checklist flags the hero image (`…/img/footer/hammer.png`) as `loading="lazy"` with no `fetchpriority` , delaying the mobile LCP of 2.7 s.
- **Solution:**

  ```
  <img src="…/hammer.png" alt="" width="233" height="382"
  loading="eager" fetchpriority="high">
  ```

  Keep `loading="lazy"` on everything below the fold.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Add a meta description `SEO`

- **Impact:** SEO score, SERP snippet quality
- **Problem:** The document has no meta description (`meta-description` audit scores 0) and SEO sits at 92.
- **Solution:** Add a unique 120–155 character description in Estonian, e.g.:

  ```
  <meta name="description" content="Restate — kinnisvara arendus ja
  varahaldus Eestis. Tutvu aktiivsete pakkumiste, uusarenduste ja
  teenustega.">
  ```

2B. Enlarge touch targets `Accessibility`

- **Impact:** Mobile usability, WCAG 2.5.8
- **Problem:** Lighthouse `target-size` scores 0.00 (weight 7) — touch targets lack sufficient size or spacing on mobile.
- **Solution:**
  - Ensure every link/button is at least 24×24 px (44×44 px recommended) with ≥8 px spacing.
  - Add padding to the footer social icons and nav links rather than relying on the glyph box.

2C. Self-host and preload web fonts `Performance`

- **Impact:** FCP, Speed Index, render delay

- **Problem:** PSI's `font-display-insight` estimates 230 ms of savings; the runtime shows two blocking requests to fonts.googleapis.com (128 ms and 126 ms) for Open Sans.
- **Solution:**
  - Host the Open Sans woff2 files on restate.ee and drop the `fonts.googleapis.com` CSS request.
  - Preload the primary weight:

```
<link rel="preload" href="/fonts/open-sans-400.woff2" as="font"
type="font/woff2" crossorigin>
```

  - Keep `font-display: swap` in the `@font-face` rules.

2D. Give duplicate landmarks unique accessible names `Accessibility`

- **Impact:** Screen-reader navigation
- **Problem:** axe reports `landmark-unique` (moderate) on `.footer__social` — two landmarks share the same role without distinguishing labels.
- **Solution:** Add a unique `aria-label` to each landmark:

```
<nav class="footer__social" aria-label="Sotsiaalmeedia">…</nav>
```

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Make link text descriptive `SEO`

- **Impact:** Anchor-text relevance, screen-reader link lists
- **Problem:** Repeated vague anchors appear across the page: "ülevaade" ×4, "tiim" ×3, "äri" ×2, "teenused" ×2, "võta ühendust" ×2.
- **Solution:**
  - Extend anchor text to describe the destination (e.g. "Vaata kinnisvara ülevaadet").
  - Where the visual design requires short text, add `aria-label` with the full context.

3B. Add structured data `SEO`

- **Impact:** Rich-result eligibility
- **Problem:** The single JSON-LD block parses as type "Unknown", and PSI's `structuredData` audit fails — no Organization/LocalBusiness/WebSite markup is

recognised.

- **Solution:** Add a valid `Organization` + `WebSite` graph:

```
{"@context":"https://schema.org","@type":"Organization","name":"Res
tate","url":"https://restate.ee/","logo":"https://restate.ee/logo.p
ng"}
```

3C. Enable HSTS preload `Security`

- **Impact:** First-visit downgrade protection
- **Problem:** HSTS is set (`max-age=31536000; includeSubDomains`) but lacks the `preload` directive, so the domain is not eligible for browser preload lists.
- **Solution:**
  - Add `preload` to the header: `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`
  - Submit the domain at hstspreload.org once all subdomains are HTTPS-only.

3D. Add Subresource Integrity to third-party scripts `Security`

- **Impact:** Supply-chain tampering risk
- **Problem:** Both cross-origin scripts (iframemanager and cookieconsent from cdn.jsdelivr.net) load without an `integrity` attribute.
- **Solution:**

```
<script
src="https://cdn.jsdelivr.net/gh/orestbida/cookieconsent@3.0.1/dist
/cookieconsent.umd.js"
        integrity="sha384-…" crossorigin="anonymous" defer>
</script>
```

Pin exact versions and generate the hash from the served file.

3E. Protect the WordPress login and installer `Security`

- **Impact:** Brute-force and takeover surface
- **Problem:** `/wp-admin/install.php` is reachable and the login form is served on the default `/wp-login.php` path.
- **Solution:**

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

  - Restrict `/wp-login.php` by IP or add a login rate-limit / 2FA plugin.

    - Consider moving the login to a custom path.

3F. Hide server version headers `Security`

- **Impact:** Fingerprinting surface
- **Problem:** The response discloses `Server: Apache / ZoneOS`, flagged as a technology-disclosure warning.
- **Solution:**

```
ServerTokens Prod
ServerSignature Off
Header unset X-Powered-By
```

3G. Harden the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is missing entirely (both `CSP present` and `CSP is strict` fail); with no auth, payments or user content on this site the exposure is limited, so this is best-practice work.
- **Solution:** Deploy a nonce-based policy rather than a flat allowlist:

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

  Add COOP/CORP alongside: `Cross-Origin-Opener-Policy: same-origin`, `Cross-Origin-Resource-Policy: same-origin`.