Audit Report: Avaleht - estply

Website: https://estply.com/
Date: 09.11.2026
Audit Coverage: 100% — all sources returned data
Confidence: high

Pages Audited (5 of 5):

- https://estply.com/
- https://estply.com/en/privacy-policy/
- https://estply.com/privaatsuspoliitika/
- https://estply.com/kupsiste-poliitika/
- https://estply.com/kontakt/

Summary of results

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

What is pulling the score down

Points are for the weakest page; Pages = how many of 5 pages share the signal.

Signal	Points	Pages	Evidence
Accessibility 91	−2.7	5/5	weighted 30% of 9 points lost
HTML validation	−2	5/5	11 W3C errors
SEO 92	−1.2	5/5	weighted 15% of 8 points lost
Performance 97	−1.2	4/5	weighted 40% of 3 points lost
Field TTFB	−1	5/5	CrUX mobile TTFB p75 914 ms
Image delivery	−1	2/5	PSI estimates 396 KiB image-delivery savings (mobile)
Advanced security headers	0	5/5	Failing: CSP is strict, Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy, Cross-Origin-Resource-Policy
Page score (weakest:	**91**		100 − 9.1 → 91

Signal	Points	Pages	Evidence
https://estply.com/)			

Site overall 92 is the mean of 5 pages; scores range 91 (https://estply.com/) → 92 (https://estply.com/kontakt/).

Per-page scores

 Excellent · https://estply.com/

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
95	91	97	91	100	92	PASS

 Excellent · https://estply.com/en/privacy-policy/

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
94	91	100	91	100	77	PASS

 Excellent · https://estply.com/privaatsuspoliitika/

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
95	92	98	91	100	92	PASS

 Excellent · https://estply.com/kupsiste-poliitika/

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
95	92	97	91	100	92	PASS

 Excellent · https://estply.com/kontakt/

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
96	92	98	92	100	92	PASS

PageSpeed Insights — Mobile vs Desktop

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

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://estply.com/	**97** / 100	**1.07 s** / 281 ms	0.000 / **0.000**
https://estply.com/en/privacy-policy/	100 / 100	**1.07 s** / 297 ms	0.000 / 0.000
https://estply.com/privaatsuspoliitika/	**98** / 100	**1.05 s** / 305 ms	0.000 / 0.000
https://estply.com/kupsiste-poliitika/	**97** / 100	**1.22 s** / 294 ms	0.000 / 0.000
https://estply.com/kontakt/	**98** / 100	**1.06 s** / 281 ms	0.000 / 0.000

Optimization Checklist

4 of 5 passing — 4 pass · 0 warn · 1 fail · 3 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.

Item	Status	Detail
Responsive images (srcset /)	N/A	Only 2 raster images on the page — 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	**Pass**	No render-blocking scripts in .

Fixes

Priority 1: Critical

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

1A. Add accessible names to buttons `Accessibility`

- **Impact:** Accessibility score, screen-reader operability
- **Problem:** Lighthouse `button-name` scores 0.00 with weight 10 — buttons on the page have no accessible name, which is the main driver of the Accessibility 91 (−2.7) row.
- **Solution:**
  - Give every `<button>` visible text or an `aria-label`:

```
<button type="button" aria-label="Sulge küpsiste teade"><svg …>
</svg></button>
```

  - For icon-only controls prefer `<button>` over a clickable `<div>` / `<span>` so the name and role are exposed.

1B. Enlarge touch targets `Accessibility`

- **Impact:** Accessibility score, mobile usability (WCAG 2.5.8)
- **Problem:** Lighthouse `target-size` scores 0.00 (weight 7) — touch targets do not have sufficient size or spacing, and the SEO category also flags `tapTargets`.
- **Solution:**
  - Ensure interactive elements are at least 24×24 px (44×44 px recommended) with ≥8 px spacing.

```
.icon-link { min-width: 44px; min-height: 44px; display: inline-
flex; align-items: center; justify-content: center; }
```

  - Check the header nav and footer link lists, which are the usual offenders on mobile.

1C. Fix W3C validation errors `Best Practices`

- **Impact:** HTML validation row (−2), HTML validity, image loading behaviour, SEO/robustness
- **Problem:** The W3C validator reports 11 errors, the second-largest deduction row (−2): five `text/rocketlazyloadscript` data blocks carry `defer`, one carries `async`, a `<link href="" rel="dns-prefetch">` has an empty href, and several `srcset` / `sizes` combinations are invalid.
- **Solution:**
  - Remove `defer` / `async` from the WP Rocket lazy-load script placeholders (they are data blocks, not JavaScript):

```
<script type="text/rocketlazyloadscript" data-rocket-
type="text/javascript" data-rocket-src="…"></script>
```

  - Drop the empty `<link data-rocket-prefetch href="" rel="dns-prefetch">` or give it a real host.
  - Add a width descriptor to every `srcset` candidate, or remove `sizes` where `srcset` has no widths (lines ~298, ~793, ~813).
  - Add `loading="lazy"` to the image using `sizes="auto …"` (line ~309).

1D. Reduce server response time (TTFB) `Performance`

- **Impact:** Field TTFB row (−1), TTFB, LCP, FCP
- **Problem:** CrUX mobile p75 TTFB is 914 ms ("average") while the lab run measures 2 ms, and the HTML document is served with `cache-control: max-age=0`, so every visit revalidates at the origin.
- **Solution:**
  - Serve the HTML from the CDN edge / full-page cache (WP Rocket is already installed — enable its page cache and a CDN).
  - Raise the document TTL for anonymous visitors, e.g. `Cache-Control: public, max-age=600, s-maxage=3600`.
  - Check origin PHP/DB time for cold cache hits; the 914 ms p75 suggests uncached requests dominate.

1E. Add a meta description `SEO`

- **Impact:** SEO score, search snippet CTR
- **Problem:** The document has no meta description (`Description: not set`) and Lighthouse's `meta-description` audit scores 0, driving the SEO category down to 77.
- **Solution:** Add a unique 120–155 character description in the page head:

  ```
  <meta name="description" content="How Estply collects, uses and retains personal data, your GDPR rights and how to contact us about privacy.">
  ```

  If the site runs WordPress, set it in the SEO plugin's template rather than hard-coding it.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Serve images in WebP/AVIF at the right size `Performance`

- **Impact:** Image delivery row (−1), Image bytes, LCP, Speed Index
- **Problem:** PSI estimates 396 KiB of image-delivery savings on mobile, and the runtime capture shows 8 image requests totalling 2.66 MB — the single largest resource type on the page.
- **Solution:**
  - Convert the remaining JPEG/PNG assets (e.g. `dsc_5118-324x216.jpg`, `estply-cta-1-520x140.jpg`, the two 251×134 PNGs) to WebP/AVIF and serve via `<picture>` with a fallback.
  - Tighten the 28 distinct srcset widths to a handful of real breakpoints so mobile never downloads a desktop-sized candidate.

2B. Remove render-blocking and unused CSS `Performance`

- **Impact:** Speed Index, FCP, render-blocking time
- **Problem:** PSI flags `render-blocking-insight` (est. 720 ms savings) and `unused-css-rules` (32 KiB) as high-priority; mobile Speed Index is 4.32 s while LCP is only 1.1 s.
- **Solution:**
  - Inline the critical above-the-fold CSS and load `global.*.css` (34.3 KB) asynchronously:

```
<link rel="preload" href="/…/global.css" as="style"
onload="this.rel='stylesheet'">
```

- Purge unused rules from the theme stylesheet and the 3 inline style blocks (9.6 KB).
- Re-check the network dependency chain flagged by `network-dependency-tree-insight`.

2C. Add structured data `SEO`

- **Impact:** SEO score, rich-result eligibility
- **Problem:** Lighthouse flags `structuredData` as failing and the single JSON-LD block parses with type "Unknown", so no recognized schema is exposed.
- **Solution:**
  - Replace the unrecognized block with valid `Organization` + `WebSite` markup (and `Product` / `LocalBusiness` where relevant):

```
{"@context":"https://schema.org","@type":"Organization","name":"EST
PLY","url":"https://estply.com/","logo":"https://estply.com/…/logo.
png"}
```

  - Validate with the Rich Results Test after deployment.

2D. Make link text descriptive `SEO`

- **Impact:** SEO score, screen-reader link lists
- **Problem:** Lighthouse `link-text` fails with 2 links, and the inventory shows vague repeated anchors such as "here" ×2 and "about us" ×2.
- **Solution:**
  - Replace "here" with the destination, e.g. `<a href="/en/contact/">contact our privacy team</a>`.
  - Where the visible text must stay short, add `aria-label` with the full purpose.

2E. Load the hero image eagerly `Performance`

- **Impact:** LCP
- **Problem:** The first raster image (`…6c041c12…png` , 251×134) is marked `loading="lazy"` with no `fetchpriority`, delaying the LCP candidate.
- **Solution:**

```
<img src="…6c041c12…png" width="251" height="134" alt=""
     loading="eager" fetchpriority="high" decoding="async">
```

Keep `loading="lazy"` only on images below the fold.

2F. Fix the invalid robots.txt `SEO`

- **Impact:** SEO score, crawl directives
- **Problem:** Lighthouse `robots-txt` fails — robots.txt is not valid, which can prevent crawlers from reading intended directives.
- **Solution:**
  - Fetch `/robots.txt` and correct the syntax (no unknown directives, no malformed `Sitemap:` line).
  - Include an absolute sitemap URL:

```
User-agent: *
Allow: /
Sitemap: https://estply.com/sitemap_index.xml
```

Priority 3: Best Practice

Recommended for long-term maintainability.

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

- **Impact:** XSS defense-in-depth
- **Problem:** The CSP is only `frame-ancestors 'self'` — `default-src` is missing and `object-src` is not `'none'`, so no script or resource restrictions exist. Site signals show no auth, payments or user content, so this is hardening rather than an active exposure.
- **Solution:**
  - Start with a report-only policy, then enforce with nonces and `'strict-dynamic'` rather than a flat allowlist:

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

  - Note the site loads `cdn.jsdelivr.net` (iframemanager) — allow it explicitly or self-host it.

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

- **Impact:** Privacy leakage, cross-origin isolation
- **Problem:** All four headers are missing from the response, and the advanced-header row lists them as failing checks.

- **Solution:**

```
Header always set Referrer-Policy "strict-origin-when-cross-origin"
Header always set Permissions-Policy "geolocation=(), camera=(),
microphone=()"
Header always set Cross-Origin-Opener-Policy "same-origin"
Header always set Cross-Origin-Resource-Policy "same-site"
```

3C. Enable HSTS preload `Security`

- **Impact:** First-visit downgrade protection
- **Problem:** HSTS is set to `max-age=31536000; includeSubDomains` but lacks the `preload` directive, so the very first request can still be downgraded.
- **Solution:**
  - Add `preload` and submit the domain at hstspreload.org:

```
Strict-Transport-Security: max-age=63072000; includeSubDomains;
preload
```

  - Only do this once every subdomain is HTTPS-only.

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

- **Impact:** Supply-chain tampering risk
- **Problem:** The single cross-origin script (`cdn.jsdelivr.net/gh/orestbida/iframemanager@1.3.0/dist/iframemanager.js`) has no `integrity` attribute.
- **Solution:**
  - Add SRI (the pinned version makes this stable):

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

  - Or self-host the 2.7 KB file to remove the third-party dependency entirely.

3E. Hide server version headers `Security`

- **Impact:** Information disclosure
- **Problem:** The response advertises `Server: Apache / ZoneOS`, which the security-basics checklist flags as a technology-disclosure warning.
- **Solution:**

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

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

- **Impact:** Brute-force and enumeration surface
- **Problem:** The security-basics checklist warns that the login form is served on the default `/wp-login.php` path (all other WordPress checks pass).
- **Solution:**
  - Put `/wp-login.php` behind a WAF rate limit or IP allowlist, or move it with a plugin that rewrites the login slug.
  - Keep XML-RPC blocked (already passing) and enforce strong passwords plus 2FA for editors.

3G. Verify color contrast manually `Accessibility`

- **Impact:** WCAG 1.4.3 readability
- **Problem:** axe-core returned 0 violations but could not determine contrast for 9 nodes (gradients/alpha backgrounds), so contrast is unverified rather than confirmed.
- **Solution:**
  - Check the 9 incomplete nodes with DevTools' contrast picker or a contrast analyser against the actual rendered background.
  - Target ≥4.5:1 for body text and ≥3:1 for large text and UI borders.

3H. Cache the HTML document `Performance`

- **Impact:** TTFB, repeat-visit speed
- **Problem:** The document response is served with `cache-control: max-age=0` and an `expires` value equal to the request time, so browsers revalidate the HTML on every navigation.
- **Solution:**
  - Let WP Rocket/CDN serve a short-lived cached HTML document:

```
Cache-Control: public, max-age=600, s-maxage=3600, stale-while-revalidate=60
```

  - Keep `no-cache` only for logged-in or cart sessions.