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
Field TTFB	−1	5/5	CrUX mobile TTFB p75 914 ms
Image delivery	−1	1/5	PSI estimates 396 KiB image-delivery savings (mobile)
Performance 98	−0.8	1/5	weighted 40% of 2 points lost
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 − 8.7 → 91

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

Site overall 92 is the mean of 5 pages; scores range 91 (https://estply.com/) → 93 (https://estply.com/kontakt/).

Per-page scores

 Excellent · https://estply.com/

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

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

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
95	92	100	91	100	85	PASS

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

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
96	93	100	91	100	92	PASS

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

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
96	93	100	91	100	92	PASS

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

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
96	93	100	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/	**98** / 99	**1.06 s** / 287 ms	0.000 / **0.001**
https://estply.com/en/privacy-policy/	100 / 100	**1.05 s** / 309 ms	0.000 / **0.015**
https://estply.com/privaatsuspoliitika/	100 / 100	**1.07 s** / 306 ms	0.000 / 0.000
https://estply.com/kupsiste-poliitika/	100 / 100	**1.05 s** / 281 ms	0.000 / 0.000
https://estply.com/kontakt/	100 / 100	**1.05 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 usability
- **Problem:** Lighthouse `button-name` scores 0.00 with weight 10 — buttons on the page have no accessible name, which is the single heaviest accessibility failure.
- **Solution:**
  - Give every `<button>` visible text or an `aria-label`:

```
<button type="button" aria-label="Ava menüü"><svg …></svg></button>
```

  - For icon-only controls, keep the label in sync with the action and never rely on the SVG alone.

1B. Enlarge touch targets `Accessibility`

- **Impact:** Accessibility score, mobile tap accuracy
- **Problem:** Lighthouse `target-size` scores 0.00 with weight 7 — touch targets do not meet the minimum size or spacing on mobile.
- **Solution:**
  - Ensure interactive elements are at least 24×24 px (WCAG 2.5.8) and ideally 44×44 px.

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

- Add spacing between adjacent links in the footer and navigation.

1C. Fix W3C validation errors `Best Practices`

- **Impact:** HTML validation row (−2), HTML validity, image loading behaviour, SEO
- **Problem:** The W3C validator reports 11 errors, including 5 `script type="text/rocketlazyloadscript"` elements carrying `defer`, an empty `href` on a `dns-prefetch` link, and `srcset` / `sizes` mismatches on images.
- **Solution:**
  - Remove `defer` / `async` from the WP Rocket lazyload data-block scripts, or let the plugin emit them without those attributes.
  - Drop the empty `<link data-rocket-prefetch href="" rel="dns-prefetch">` or give it a real host.
  - Add width descriptors to every `srcset` candidate when `sizes` is present, and only use `sizes="auto"` together with `loading="lazy"`.
  - Re-run the validator until the error count is 0.

1D. Add a meta description `SEO`

- **Impact:** SEO score, search snippet quality
- **Problem:** The document has no meta description (`meta-description` audit scores 0.00) and the HTML inventory confirms `Description: not set`, which is the main reason SEO sits at 85.
- **Solution:** Add a unique 120–155 character description per page:

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

  Keep the `en` and `et` versions distinct rather than translating word-for-word.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Reduce server response time (TTFB) `Performance`

- **Impact:** Field TTFB row (−1), TTFB, FCP, LCP
- **Problem:** CrUX mobile TTFB p75 is 914 ms ("average" band) while the lab TTFB is only 21 ms, and the document is served with `cache-control: max-age=0`, so real users often hit an uncached origin.
- **Solution:**

- Warm the page cache for the canonical URL after each deploy and keep WP Rocket's page cache enabled for anonymous traffic.
- Check origin/PHP response time for cold requests (object cache, slow queries, plugin boot).
- Serve cached HTML from the CDN edge rather than revalidating at origin.

2B. 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 images totalling 2.66 MB, including PNG and JPEG assets.
- **Solution:**
  - Convert the remaining PNG/JPEG assets (e.g. the two 251×134 PNGs and the 324×216 JPEGs) to WebP/AVIF with a fallback.
  - Keep the existing `srcset` but verify the largest candidate is not oversized for its rendered slot.

```
<picture>
  <source type="image/avif" srcset="img-640.avif 640w, img-
1280.avif 1280w" sizes="100vw">
  <img src="img-640.jpg" srcset="img-640.jpg 640w, img-1280.jpg
1280w" sizes="100vw" width="1280" height="720" alt="">
</picture>
```

2C. Make link text descriptive `Accessibility`

- **Impact:** Link purpose (WCAG 2.4.4), SEO anchor quality
- **Problem:** The inventory flags 8 groups of vague, repeated link text — e.g. "meist" ×2, "tooted" ×2, "kontakt" ×2, "liitu meiega" ×2 — which are ambiguous out of context.
- **Solution:**
  - Rewrite anchors so they describe the destination ("Tutvu ESTPLY toodetega", "Võta ühendust").
  - Where the visual design requires short text, add `aria-label` with the full purpose.

2D. Load the hero image eagerly `Performance`

- **Impact:** LCP
- **Problem:** The optimized-web checklist fails "Hero image eagerly loaded": the first raster image (`…6c041c12…png`) uses `loading="lazy"` with no `fetchpriority` ,

delaying the LCP candidate.

- **Solution:**

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

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

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

- **Impact:** FCP, LCP, Speed Index
- **Problem:** PSI flags `render-blocking-insight` (est. 560 ms savings) and `unused-css-rules` (33 KiB); the page loads 2 external stylesheets plus 3 inline blocks (9.6 KB).
- **Solution:**
  - Inline the critical above-the-fold CSS and load the rest asynchronously:

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

  - Purge unused rules from the theme stylesheet (WP Rocket "Remove Unused CSS" can do this).
  - Merge the 3 inline style blocks into one.

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'`. Site signals show no auth, payments or user content, so this is low-risk today.
- **Solution:**
  - Add the missing directives now:

```
Content-Security-Policy: default-src 'self'; object-src 'none';
base-uri 'none'; frame-ancestors 'self'
```

  - When you add forms or a login, move to a nonce + `'strict-dynamic'` policy rather than a flat allowlist.

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

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

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

3C. Enable HSTS preload `Security`

- **Impact:** TLS downgrade protection
- **Problem:** HSTS is set to `max-age=31536000; includeSubDomains` but lacks the `preload` directive, so first-visit downgrade protection is absent.
- **Solution:**
  - Append `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 integrity
- **Problem:** The single cross-origin script (`cdn.jsdelivr.net/.../iframemanager.js`) has no `integrity` attribute.
- **Solution:**

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

  - Pin the exact version (already `@1.3.0`) and regenerate the hash on upgrade.

3E. Hide server version headers `Security`

- **Impact:** Attack-surface reduction
- **Problem:** The response discloses `Server: Apache / ZoneOS`, and the security-basics technology-disclosure check is a warning.
- **Solution:**

```
ServerTokens Prod
```

```
ServerSignature Off
```

- Also strip any `X-Powered-By` header at the reverse proxy.

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

- **Impact:** Brute-force exposure
- **Problem:** The login form is still served on the default `/wp-login.php` path (security-basics warning), even though xmlrpc, user enumeration and installer paths are already blocked.
- **Solution:**
  - Move or restrict login: a custom login slug, HTTP basic auth in front of `/wp-login.php`, or IP allowlisting.
  - Add rate limiting / 2FA on the login form.

3G. Verify color contrast manually `Accessibility`

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

3H. Add structured data `SEO`

- **Impact:** Rich-result eligibility
- **Problem:** The SEO `structuredData` audit fails; the page carries one JSON-LD block whose type resolves to "Unknown", so no recognised schema is exposed for a privacy-policy page.
- **Solution:** Add a valid `WebPage` / `Organization` graph:

  ```
  {"@context":"https://schema.org","@type":"WebPage","name":"Privacy Policy","url":"https://estply.com/en/privacy-policy/","inLanguage":"en","isPartOf":{"@type":"WebSite","name":"estply","url":"https://estply.com/"}}
  ```

  Validate with the Rich Results Test.