Audit Report: Avaleht - estply

Website: https://estply.com/
Date: 28.10.2026
Audit Coverage: 100% — all sources returned data
Confidence: medium

Pages Audited (5 of 5):

- https://estply.com/
- https://estply.com/en/2026/07/06/vineeri-kvaliteediklassid-selgeks
- https://estply.com/en/kupsiste-poliitika
- https://estply.com/kupsiste-poliitika
- https://estply.com/kontakt

Summary of results

Overall Score: 70 / 100
Status: **Needs Improvement**

Site overall 70 is the mean of 5 pages. Scores range 62 (https://estply.com/) → 74 (https://estply.com/kontakt). Weakest page: Mobile performance is the dominant drag: PSI mobile 64 vs desktop 95, with LCP 8.0 s and Speed Index 8.07 s against a 0.7 s / 2.19 s desktop result — a >7 s LCP delta that lands squarely in the heavy-penalty band. PSI attributes the gap to image-delivery (544 KiB savings) and font-display (500 ms), and the runtime capture confirms a single 464 KB hero WebP plus 161 KB of fonts out of 963 KB total. Accessibility is close but not clean: axe-core reports 0 violations, yet PSI accessibility is 91 with `button-name` (weight 10) and `target-size` (weight 7) both scoring 0, and 17 color-contrast nodes were left undetermined. SEO loses points for a missing meta description and failing structured data, and W3C logs 8 errors (5× `text/rocketlazyloadscript` with `defer`, 2× srcset candidates without width descriptors). Security basics PASSes, but the CSP is only `frame-ancestors 'self'` with no `default-src` or `object-src 'none'`, and Referrer-Policy/Permissions-Policy/COOP/CORP are absent. The CrUX field values (0 ms p75 for LCP/TTFB/INP, all labelled "slow") are internally inconsistent and were not used for scoring.

Per-page scores

 Needs Improvement · https://estply.com/

Score	Performance	Accessibility	Best Practices	SEO	Security
62	64	91	96	92	PASS

 Needs Improvement · https://estply.com/en/2026/07/06/vineeri-kvaliteediklassid-selgeks

Score	Performance	Accessibility	Best Practices	SEO	Security
69	62	91	100	100	PASS

 Needs Improvement · https://estply.com/en/kupsiste-poliitika

Score	Performance	Accessibility	Best Practices	SEO	Security
74	78	91	100	85	PASS

 Needs Improvement · https://estply.com/kupsiste-poliitika

Score	Performance	Accessibility	Best Practices	SEO	Security
71	78	91	100	92	PASS

 Needs Improvement · https://estply.com/kontakt

Score	Performance	Accessibility	Best Practices	SEO	Security
74	81	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/	**64** / 95	**7.97 s** / 728 ms	**0.006** / 0.001
https://estply.com/en/2026/07/06/vineeri-kvaliteediklassid-selgeks	**62** / 93	**3.84 s** / 876 ms	**0.491** / 0.001

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://estply.com/en/kupsiste-poliitika	**78** / 98	**4.40 s** / 969 ms	0.000 / **0.001**
https://estply.com/kupsiste-poliitika	**78** / 98	**4.43 s** / 938 ms	0.000 / **0.001**
https://estply.com/kontakt	**81** / 98	**4.28 s** / 987 ms	**0.009** / 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.
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.

Item	Status	Detail
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. Cut mobile LCP from 8.0 s by fixing hero image delivery and font loading

`Performance`

- **Impact:** LCP, Speed Index, FCP
- **Problem:** Mobile LCP is 8.0 s and Speed Index 8.07 s (desktop 0.7 s / 2.19 s); PSI flags image-delivery-insight (544 KiB) and font-display-insight (500 ms), and the runtime capture shows a single 464 KB hero WebP plus 161 KB of fonts.
- **Solution:**
  - Serve a properly sized hero: the LCP image is `kaasik-kaupo-kalda-1600x900.webp` at 464 KB — generate 640/960/1280 widths and let `srcset` / `sizes` pick the right one.
  - Prioritise it explicitly:

```
<img src=".../hero-960.webp" srcset=".../hero-640.webp 640w,
.../hero-960.webp 960w, .../hero-1280.webp 1280w"
     sizes="100vw" width="960" height="540"
     fetchpriority="high" loading="eager" alt="...">
<link rel="preload" as="image" href=".../hero-960.webp"
imagesrcset="..." imagesizes="100vw" fetchpriority="high">
```

  - Add `font-display: swap` to the Open Sans `@font-face` rules and preload the two woff2 files (56 KB + 58 KB) actually used above the fold; consider dropping the third font file.
  - Do not lazy-load the hero image (it is currently `loading="eager"` — keep that, but add `fetchpriority`).

1B. Fix the broken cross-origin SVG sprite (32 console errors, 32 failed requests)

`Best Practices`

- **Impact:** Console errors, icon rendering, PSI Best Practices
- **Problem:** The runtime capture logged 32 identical errors: "Unsafe attempt to load URL

https://27c41eda.delivery.rocketcdn.me/.../svg/global.f0c272df5a4f94d0b14a.svg from frame with URL https://estply.com/. Domains, protocols and ports must match." — the same file also appears 32 times in failed requests, so the icon sprite is not loading.

- **Solution:**
  - Serve the sprite from the same origin (`https://estply.com/...`) instead of the RocketCDN host, or
  - If it must stay on the CDN, add `crossorigin="anonymous"` on the `<use>` /fetch and return `Access-Control-Allow-Origin: https://estply.com` from the CDN.
  - Simplest robust fix: inline the sprite into the document or bundle it with the theme CSS.

1C. Eliminate the footer layout shift driving CLS 0.491 `Performance`

- **Impact:** CLS, mobile Performance score
- **Problem:** Lighthouse attributes 0.481 of the 0.491 mobile CLS to `div#page > div.main > div.main__footer > footer.footer` , with a second 0.010 shift on the same element.
- **Solution:**
  - Reserve space for the footer before it renders: give `footer.footer` an explicit `min-height` matching its final height.
  - Check the cookie banner (`cookieyes` / RocketLazyLoad) — a banner injected above the footer after load is the classic cause of a 0.48 shift. Render it in a fixed-position overlay, not in document flow.
  - Avoid inserting late-loading widgets, ads, or lazy images above the footer without a reserved placeholder.
  - Re-run Lighthouse mobile after each change; target CLS ≤ 0.1.

1D. Load the hero image eagerly with high fetch priority `Performance`

- **Impact:** LCP (3.8 s mobile), Speed Index (5.41 s)
- **Problem:** The Optimized-Web checklist fails 'Hero image eagerly loaded': the first raster image (`6c041c12…png`) has `loading="lazy"` and no `fetchpriority` , while mobile LCP is 3.8 s.
- **Solution:**

```
<img src="/wp-content/uploads/2026/08/6c041c12….png"
     alt="…"
     width="251" height="134"
     loading="eager"
```

```
      fetchpriority="high"
      decoding="async">
```

Also add a `<link rel="preload" as="image" fetchpriority="high">` for the LCP image in `<head>`.

1E. Give every button an accessible name `Accessibility`

- **Impact:** WCAG 4.1.2, mobile Accessibility score (91)
- **Problem:** Lighthouse `button-name` scores 0.00 at weight 10 on mobile — buttons render with no text or ARIA label.
- **Solution:**
  - Add visible text, or `aria-label` / `aria-labelledby` to each icon-only button:

```
<button type="button" aria-label="Open search">
  <svg aria-hidden="true">…</svg>
</button>
```

  - Never rely on a background-image or icon font alone for the accessible name.

1F. Add a single H1 and a real heading hierarchy `Accessibility`

- **Impact:** WCAG 1.3.1 / 2.4.6, document outline, SEO
- **Problem:** The HTML inventory reports h1 ×0, h2 ×0, h3 ×0, h4 ×0, h5 ×0, h6 ×0 — the page has no headings at all — and axe flags `page-has-heading-one` (moderate).
- **Solution:**
  - Wrap the article title in exactly one `<h1>`.
  - Use `<h2>` for major sections and `<h3>` for subsections; do not skip levels.
  - Keep the visual styling via CSS classes rather than choosing tags by appearance.

1G. Cut mobile LCP (4.4 s) and FCP (3.17 s) on the critical render path `Performance`

- **Impact:** LCP, FCP, Speed Index, document latency
- **Problem:** Mobile LCP is 4.4 s vs 1.0 s on desktop and FCP is 3.17 s; Lighthouse flags `document-latency-insight` (610 ms est. savings) and `font-display-insight` (110 ms est. savings) as high-priority.
- **Solution:**
  - Preload the LCP image and the primary font in `<head>`:

```
<link rel="preload" as="image" href="/wp-
content/uploads/2026/08/6c041c12fb0c531933532c08c2749a1a836d595a.pn
g" fetchpriority="high">
<link rel="preload" as="font" type="font/woff2"
href="/fonts/opensans.woff2" crossorigin>
```

- Add `font-display: swap` (or `optional`) to the Open Sans `@font-face` rules.
- Self-host the 4 Google Fonts files (96.2 KB from fonts.gstatic.com) to remove the third-party DNS/TLS hop.
- Flatten the network dependency tree: the 21 requests chain through fonts.googleapis.com → fonts.gstatic.com → cdn.jsdelivr.net before first paint.

1H. Give buttons accessible names and enlarge touch targets `Accessibility`

- **Impact:** WCAG 4.1.2 Name/Role/Value, 2.5.8 Target Size
- **Problem:** Lighthouse mobile accessibility is 91 with `button-name` (score 0.00, weight 10) and `target-size` (score 0.00, weight 7) both failing, even though axe reported 0 violations.
- **Solution:**
  - Add `aria-label` (or visible text) to every icon-only `<button>`, e.g. `<button aria-label="Close cookie banner">`.
  - Ensure interactive targets are at least 44×44 px with adequate spacing (WCAG 2.5.8).
  - Manually verify the 7 nodes axe marked 'incomplete' for color contrast — axe skips gradients and alpha transparency.

1I. Eager-load the LCP hero image with high fetch priority `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** The hero image (uploads/2026/08/6c041c12…png) carries loading="lazy" and no fetchpriority, and mobile LCP is 4.4 s versus 0.9 s on desktop.
- **Solution:**
  - Remove `loading="lazy"` from the hero and add `fetchpriority="high"`:

```
<img src="/wp-content/uploads/2026/08/6c041c12….png"
     alt="…" width="251" height="134"
     fetchpriority="high" decoding="async">
```

  - Add a preload hint in `<head>` so the browser discovers it before CSS/JS:

```
<link rel="preload" as="image" href="/wp-
content/uploads/2026/08/6c041c12….png" fetchpriority="high">
```

- In WP Rocket, exclude this image from LazyLoad (Settings → Media → Excluded images).

1J. Eliminate the document redirect hop and shorten the critical request chain `Performance`

- **Impact:** LCP, FCP, TTFB, document latency
- **Problem:** The runtime capture shows two document requests — /kupsiste-poliitika (493 ms, 0 B) redirecting to /kupsiste-poliitika/ (1.39 s) — and Lighthouse's document-latency-insight estimates 590 ms of savings.
- **Solution:**
  - Link internally to the canonical trailing-slash URL (`https://estply.com/kupsiste-poliitika/`) so no request pays the redirect.
  - Ensure the canonical tag and all nav/footer links match the final URL exactly.
  - Keep WP Rocket page caching warm for the canonical URL so the first visitor does not pay the cold-start cost.

1K. Load the hero image eagerly to fix the 4.3 s mobile LCP `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** Mobile LCP is 4.3 s (desktop 1.0 s) and the optimized-web checklist fails "Hero image eagerly loaded": the hero `/wp-content/uploads/2026/10/cz5i9178-100x100.webp` has `loading="lazy"` and no `fetchpriority` .
- **Solution:**
  - Remove `loading="lazy"` from the above-the-fold hero and add `fetchpriority="high"` :

```
<img src="/wp-content/uploads/2026/10/cz5i9178.webp"
     srcset="... 400w, ... 800w, ... 1600w"
     sizes="100vw"
     width="1600" height="900"
     fetchpriority="high"
     alt="...">
```

  - Add a `<link rel="preload" as="image" fetchpriority="high" imagesrcset="..." imagesizes="100vw">` in `<head>` .
  - Exclude the hero from WP Rocket's lazy-load exclusion list so the plugin does not re-add `loading="lazy"` .

1L. Give icon buttons accessible names and enlarge touch targets `Accessibility`

- **Impact:** Lighthouse accessibility (92 mobile), WCAG 4.1.2, 2.5.8
- **Problem:** Lighthouse reports `button-name` (weight 10) and `target-size` (weight 7) both at score 0, and the SEO `tapTargets` audit also fails.
- **Solution:**
  - Add an accessible name to every icon-only button:

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

  - Ensure interactive targets are at least 44×44 px with adequate spacing:

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

  - Re-run Lighthouse after the change to confirm both audits pass.

1M. Replace the frame-ancestors-only CSP with a nonce-based policy `Security`

- **Impact:** XSS defense-in-depth, CSP strictness
- **Problem:** The only CSP directive is `frame-ancestors 'self'` — no `default-src`, no `object-src 'none'`, so no script or resource restrictions apply. The page contains a `<textarea>` (user-content signal), which raises the value of a real CSP.
- **Solution:** Deploy a nonce + `'strict-dynamic'` 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'; form-action 'self'
```

  - In WordPress, generate the nonce per request and add it to every enqueued script tag.
  - Roll out in `Content-Security-Policy-Report-Only` first and watch the reports before enforcing.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Name icon buttons and enlarge touch targets `Accessibility`

- **Impact:** WCAG 4.1.2, 2.5.8; PSI accessibility 91

- **Problem:** PSI accessibility is 91 on mobile with `button-name` (score 0, weight 10) and `target-size` (score 0, weight 7) both failing; axe-core reported 0 violations but left 17 color-contrast nodes undetermined.
- **Solution:**
  - Give every icon-only `<button>` an accessible name: `<button aria-label="Close menu"><svg aria-hidden="true">…</svg></button>`.
  - Ensure interactive targets are at least 44×44 px with adequate spacing (WCAG 2.5.8).
  - Manually verify the 17 undetermined contrast nodes (gradients/alpha backgrounds) with a contrast checker.

2B. Add a meta description and valid structured data `SEO`

- **Impact:** SEO score (92), SERP snippet, rich results
- **Problem:** The document has no meta description (`metaDescription` failing in PSI) and `structuredData` fails — the single JSON-LD block is typed "Unknown".
- **Solution:**
  - Add a 140–160 character description in Estonian (and a matching one for `/en/`):

```
<meta name="description" content="ESTPLY tootab kvaliteetset
kasevineeri Jõgevamaa kaasaegses vineeritehases – usaldusväärne
partner sinu ärile.">
```

  - Replace the untyped JSON-LD block with a valid `Organization` (and `WebSite`) schema including `name`, `url`, `logo`, `sameAs`.

2C. Strengthen the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** The CSP is only `frame-ancestors 'self'` — no `default-src`, no `object-src 'none'`, no script/resource restrictions; the security checklist marks "CSP is strict" as FAILED.
- **Solution:** Deploy a nonce-based 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'; upgrade-insecure-requests
```

  Roll it out in report-only mode first, then enforce. Note the site has no auth or payment surface, so this is defense-in-depth rather than an urgent exposure.

2D. Fix invalid srcset/sizes markup so responsive images actually apply `Performance`

- **Impact:** Image bytes, LCP
- **Problem:** W3C reports 8 errors, including 2 `srcset` candidates with no width descriptor and one `sizes` value starting with "auto" on an eagerly loaded image — browsers discard such srcsets and download the full-size file.
- **Solution:**
  - Every candidate in a `srcset` needs a width (or density) descriptor:

```
<img src=".../6c041c12....png"
     srcset=".../6c041c12-251x134.png 251w, .../6c041c12-
502x268.png 502w"
     sizes="(max-width: 600px) 251px, 502px" width="251"
height="134" alt="">
```

  - Remove `auto` from `sizes` on the eager image at line 297, or add `loading="lazy"` if it is genuinely below the fold.

2E. Shrink the 531 KB HTML document `Performance`

- **Impact:** TTFB, FCP, parse time
- **Problem:** HTML bytes are 531,748 (21.6 KB gzipped) and the document request took 2.38 s in the runtime capture — the largest single request in the waterfall.
- **Solution:**
  - Move the 9.6 KB of inline CSS and inline scripts into cacheable external files.
  - Trim the DOM and remove unused markup/whitespace from the page builder output.
  - Verify WP Rocket's "Remove unused CSS" / delay-JS options are not inflating the inline payload.

2F. Enlarge touch targets to at least 44×44 px `Accessibility`

- **Impact:** WCAG 2.5.8, mobile usability, SEO tap-targets audit
- **Problem:** Lighthouse `target-size` scores 0.00 (weight 7) and the SEO `tapTargets` audit fails on mobile.
- **Solution:**
  - Give icon links and nav items a minimum 44×44 px hit area via padding or `min-width` / `min-height`.
  - Add at least 8 px spacing between adjacent targets.

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

2G. Stop serving the HTML with cache-control: max-age=0 `Performance`

- **Impact:** Repeat-visit TTFB, FCP, LCP
- **Problem:** The document response sends `cache-control: max-age=0` with an `Expires` equal to the request time, so the 66.6 KB HTML is re-downloaded on every navigation despite WP Rocket being active.
- **Solution:**
  - Let WP Rocket manage the document cache, or set a short browser TTL with revalidation:

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

  - Keep `Vary: Accept-Encoding` (already present).
  - Verify the canonical URL is warmed after deploy so the first visitor does not pay the cold-start cost.

2H. Fix the 5 invalid rocketlazyloadscript + defer combinations `Best Practices`

- **Impact:** W3C validity (7 errors), HTML correctness
- **Problem:** 5 of the 7 W3C errors are `<script type="text/rocketlazyloadscript" … defer>` — a data-block script type must not carry `defer` (first at line 21, the cookieyes banner).
- **Solution:**
  - Remove `defer` from the `text/rocketlazyloadscript` tags, or switch to a real JS type:

```
<script type="text/javascript" defer src="…"></script>
```

  - If the tag is a data block for WP Rocket's lazy loader, drop `defer` and let the loader handle timing.
  - Also remove the redundant `type="text/javascript"` flagged as a warning at line 272.

2I. Add width descriptors to the two srcset attributes `Best Practices`

- **Impact:** W3C validity, responsive image selection
- **Problem:** 2 W3C errors: `srcset` on the two PNGs (lines 391 and 411) lists a candidate with no width while `sizes` is present, so browsers cannot pick a source.

- **Solution:**

```
<img src="…251w.png"
     srcset="…251w.png 251w, …502w.png 502w"
     sizes="(max-width: 600px) 100vw, 251px"
     width="251" height="134" alt="">
```

  Every candidate in `srcset` must carry a `w` or `x` descriptor when `sizes` is used.

2J. Add valid structured data `SEO`

- **Impact:** Rich results eligibility, PSI SEO audit
- **Problem:** PSI's `structuredData` audit fails on mobile, and the single JSON-LD block on the page is reported with type `Unknown`.
- **Solution:**
  - Emit an `Article` (or `BlogPosting`) block with `headline`, `datePublished`, `author`, `image` and `mainEntityOfPage`.
  - Validate with the Rich Results Test and Schema Markup Validator after deploying.

2K. Add a meta description `SEO`

- **Impact:** SEO score, SERP snippet
- **Problem:** `meta-description` scores 0.00 and the HTML inventory confirms `Description: not set`; SEO is 85 on both mobile and desktop.
- **Solution:**

```
<meta name="description" content="Estply cookie policy — how we
collect, use and retain personal data, and how to exercise your
GDPR rights.">
```

  Keep it 120–155 characters and unique per language variant (en / et).

2L. Harden the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is only `frame-ancestors 'self'` — `default-src` is missing and `object-src` is not `'none'`, so there are no script or resource restrictions at all.
- **Solution:** Deploy a nonce-based policy rather than a flat allowlist:

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

```
  style-src 'self' 'unsafe-inline'; img-src 'self' data:; frame-
ancestors 'self'
```

Note: this is a WordPress site with an admin login at `/wp-login.php`, so a stolen admin session is a real risk even though the audited page has no auth surface.

2M. Complete the missing/weak security headers `Security`

- **Impact:** Transport security, referrer leakage, feature exposure
- **Problem:** HSTS lacks the `preload` directive, and Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing.
- **Solution:**

```
Strict-Transport-Security: max-age=31536000; includeSubDomains;
preload
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: camera=(), microphone=(), geolocation=()
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
X-Permitted-Cross-Domain-Policies: none
```

Then submit the domain at hstspreload.org once the preload directive is live.

2N. Fix the 7 W3C validation errors `Best Practices`

- **Impact:** HTML validity, lazy-load behavior
- **Problem:** W3C reports 7 errors: 5× a `script` with `type="text/rocketlazyloadscript"` also carrying `defer`, and 2× `srcset` candidates with no width descriptor while `sizes` is present.
- **Solution:**
  - WP Rocket's `text/rocketlazyloadscript` data blocks must not carry `defer`; exclude those scripts from Delay JS execution or let WP Rocket rewrite them without `defer`.
  - Add width descriptors to every `srcset` candidate:

```
<img src="…png" srcset="…-251x134.png 251w, …-502x268.png 502w"
sizes="(max-width: 600px) 251px, 502px" width="251" height="134"
alt="">
```

2O. Use a single h1 and disambiguate vague link text `Accessibility`

- **Impact:** Document outline, link purpose (WCAG 2.4.4)
- **Problem:** The heading outline shows h1 ×2 ('Küpsiste poliitika' and 'Privacy Policy'), and Lighthouse `link-text` fails with 2 links; the inventory also lists 'here'

×2 and 'about us' ×2.

- **Solution:**
  - Demote the second `<h1>` to `<h2>` so the page has exactly one top-level heading.
  - Replace 'here' with descriptive text, or add `aria-label`, e.g. `<a href="…" aria-label="Read the full cookie policy">`.

2P. Stop sending cache-control: max-age=0 on the document `Performance`

- **Impact:** Repeat-visit TTFB, LCP
- **Problem:** The document response carries `cache-control: max-age=0` even though WP Rocket 3.23.5.1 is active, forcing revalidation on every visit to a static policy page.
- **Solution:**
  - In WP Rocket → Cache, enable browser caching for HTML with a short TTL (e.g. `max-age=600`) and keep `Vary: Accept-Encoding`.
  - Alternatively set it at the server:

```
<FilesMatch "\.html$">
  Header set Cache-Control "public, max-age=600"
</FilesMatch>
```

2Q. Enlarge touch targets to at least 24×24 px (44×44 recommended) `Accessibility`

- **Impact:** WCAG 2.5.8 Target Size; mobile usability
- **Problem:** Lighthouse fails `target-size` with score 0.00 and weight 7 — interactive elements are too small or too close together on mobile.
- **Solution:**
  - Add padding to icon links and small nav items so the hit area is ≥44×44 px:

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

  - Use `gap` on flex/grid nav containers instead of margins so spacing counts toward the target-size rule.

2R. Self-host and preload the Open Sans webfonts `Performance`

- **Impact:** FCP, LCP, render-blocking chain
- **Problem:** 4 font files totalling 96.2 KB load from fonts.gstatic.com (the largest single resource type on the page), and Lighthouse's font-display-insight estimates 150 ms of savings.
- **Solution:**
  - Self-host the two used weights as WOFF2 and drop the fonts.googleapis.com/gstatic.com round trips.
  - Declare `font-display: swap` (or `optional`) in `@font-face`:

```
@font-face {
  font-family: 'Open Sans';
  src: url('/fonts/opensans-var.woff2') format('woff2-variations');
  font-display: swap;
  font-weight: 300 800;
}
```

  - Preload only the single font file used above the fold:

```
<link rel="preload" as="font" type="font/woff2"
href="/fonts/opensans-var.woff2" crossorigin>
```

2S. Fix heading structure, vague link text and language tagging `SEO`

- **Impact:** Document outline, screen-reader navigation, SEO
- **Problem:** The page has 2 `<h1>` elements ("Küpsiste poliitika" and "Privacy Policy"), repeated vague link text ("here" ×2, "meist" ×2, "kontakt" ×2), and W3C warns the document reads as English while `<html lang="et">`.
- **Solution:**
  - Keep exactly one `<h1>`; demote the second to `<h2>` or split the English policy onto the `/en/` hreflang variant.
  - Replace "here" links with descriptive text: `<a href="…">Loe meie privaatsuspoliitikat</a>`.
  - If the body is genuinely English, set `lang="en"` on the wrapping element:

```
<div lang="en"> … English policy text … </div>
```

2T. Resolve the 7 W3C validation errors `Best Practices`

- **Impact:** HTML validity, lazy-load correctness, responsive images
- **Problem:** W3C reports 7 errors: 5× `script type="text/rocketlazyloadscript"` carrying a `defer` attribute (invalid for a

data block), and 2× `srcset` candidates with no width descriptor while `sizes` is present.

- **Solution:**
  - For the RocketLazyload scripts, drop `defer` from the data-block script tags (WP Rocket re-adds it at execution time), or exclude those specific scripts from Delay JavaScript Execution.
  - Add width descriptors to every `srcset` candidate:

```
<img src="…6c041c12….png"
     srcset="…6c041c12-251x134.png 251w, …6c041c12-502x268.png
502w"
     sizes="(max-width: 600px) 100vw, 251px"
     width="251" height="134" alt="">
```

2U. Allow browser caching of the HTML document `Performance`

- **Impact:** Repeat-visit TTFB, LCP
- **Problem:** The document response sends `cache-control: max-age=0` with an `expires` value equal to the request time, forcing revalidation on every navigation despite WP Rocket being active.
- **Solution:**
  - For a static policy page, serve a short but non-zero browser TTL and let the CDN handle freshness:

```
Cache-Control: public, max-age=600, s-maxage=86400, stale-while-
revalidate=60
```

  - Keep `max-age=0, must-revalidate` only for pages that must never be stale (cart, account).

2V. Cut image bytes and self-host the web font `Performance`

- **Impact:** LCP, page weight, FCP
- **Problem:** Images account for 611 KB of the 740 KB total page weight across 16 requests, Lighthouse estimates 51 KiB of image-delivery savings, and 47.2 KB of Open Sans is fetched from fonts.gstatic.com with a `font-display-insight` saving of 40 ms.
- **Solution:**
  - Serve the hero and gallery images at the exact rendered size; the srcset currently exposes 20 distinct widths up to 2561 px, so cap the largest candidate.

- Re-encode remaining JPEG/PNG sources to WebP/AVIF (the site already uses WebP for most thumbnails).
- Self-host Open Sans as woff2 with `font-display: swap` and `<link rel="preload" as="font" crossorigin>` to remove the fonts.gstatic.com / fonts.googleapis.com round trips.

2W. Fix the 17 W3C validation errors `Best Practices`

- **Impact:** HTML validity, image rendering, script execution
- **Problem:** W3C reports 17 errors: 12× `script type="text/rocketlazyloadscript"` combined with `defer`, 2× `srcset` candidates missing a width descriptor, 1× `charset` meta after the first 1024 bytes, and 2× hidden inputs with `autocomplete`.
- **Solution:**
  - Move `<meta charset="utf-8">` to the very first element inside `<head>`.
  - Add width descriptors to the two offending srcset entries:

```
<img src="…6c041c12….png" srcset="…6c041c12….png 800w" sizes="(max-width: 800px) 100vw, 800px" alt="">
```

  - Remove `autocomplete` from `<input type="hidden">` fields (Gravity Forms).
  - Ask WP Rocket support about the `text/rocketlazyloadscript` + `defer` combination, or disable the "Delay JS execution" option for these scripts.

2X. Add Referrer-Policy, Permissions-Policy, COOP and CORP `Security`

- **Impact:** Privacy leakage, cross-origin isolation
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing from the response headers.
- **Solution:**

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

2Y. Emit valid, typed structured data `SEO`

- **Impact:** Rich results eligibility, SEO score
- **Problem:** The single JSON-LD block is reported with type `Unknown` and Lighthouse's `structuredData` audit fails.

- **Solution:**
  - Replace the untyped block with a schema.org `Organization` / `LocalBusiness` graph including `name`, `url`, `logo`, `address`, `telephone` and `contactPoint`.
  - Validate with the Rich Results Test and Schema Markup Validator after the change.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Add Referrer-Policy, Permissions-Policy, COOP, CORP, HSTS preload and SRI `Security`

- **Impact:** Privacy, origin isolation, supply-chain integrity
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing; HSTS lacks `preload`; 2 of 2 cross-origin scripts lack an `integrity` attribute; the `Server: Apache / ZoneOS` header discloses the stack.
- **Solution:**

```
Header always set Referrer-Policy "strict-origin-when-cross-origin"
Header always set Permissions-Policy "geolocation=(), microphone=
(), camera=()"
Header always set Cross-Origin-Opener-Policy "same-origin"
Header always set Cross-Origin-Resource-Policy "same-site"
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains; preload"
Header always unset Server
```

  - Add `integrity` + `crossorigin="anonymous"` to the jsDelivr `iframemanager.js` and other cross-origin scripts.

3B. Harden WordPress entry points `Security`

- **Impact:** Attack surface
- **Problem:** The security checklist warns that `/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 move it behind HTTP basic auth / a custom login slug.
- Keep the existing protections (xmlrpc blocked, no version disclosure, no user enumeration) in place.

3C. Disambiguate repeated vague link text `Accessibility`

- **Impact:** WCAG 2.4.4 link purpose
- **Problem:** The HTML inventory flags repeated vague anchors: "meist" ×2, "tooted" ×2, "kontakt" ×2, "ressursid" ×2, "liitu meiega" ×2, "käitumiskoodeks" ×3, "tehase külastaja meelespea" ×2.
- **Solution:**
  - Add distinguishing context or `aria-label`, e.g. `<a href="/et/tooted" aria-label="Tooted – vineeritooted">tooted</a>`.
  - Where the same label appears in header and footer, differentiate with `aria-label="Tooted (päis)"` / `"Tooted (jalus)"`.

3D. Allow browser caching of the HTML document `Performance`

- **Impact:** Repeat-visit TTFB
- **Problem:** The document response sends `cache-control: max-age=0` with an `expires` timestamp equal to the request time, so every navigation revalidates.
- **Solution:**
  - Keep `max-age=0` only if the page is genuinely dynamic; otherwise use a short shared cache with stale-while-revalidate:

```
Cache-Control: public, max-age=0, s-maxage=600, stale-while-revalidate=86400
```

  - Confirm WP Rocket's page cache is warmed for the canonical URL after each deploy.

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

- **Impact:** XSS defense-in-depth
- **Problem:** The CSP is `frame-ancestors 'self'` only — no `default-src`, no `object-src 'none'`, so no script or resource restrictions apply. Site signals show no auth, payments, or user content, so this is a hardening item rather than an urgent one.
- **Solution:** Deploy a nonce-based policy 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'
```

Roll it out in report-only mode first and watch for violations from the jsdelivr iframemanager script.

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

- **Impact:** Privacy, origin isolation, cross-origin read protection
- **Problem:** All four headers are missing from the response: `referrer-policy`, `permissions-policy`, `cross-origin-opener-policy`, `cross-origin-resource-policy`.
- **Solution:**

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

3G. Add SRI to the jsdelivr script and finish HSTS preload `Security`

- **Impact:** Supply-chain integrity, HSTS coverage
- **Problem:** 1 of 1 cross-origin scripts (`iframemanager.js` from cdn.jsdelivr.net) lacks an `integrity` attribute, and HSTS is `max-age=31536000; includeSubDomains` without `preload`.
- **Solution:**
  - Add `integrity="sha384-…"` and `crossorigin="anonymous"` to the jsdelivr `<script>` and `<link>` tags, or self-host the file.
  - Append `; preload` to HSTS once you are ready to submit at hstspreload.org.

3H. Reduce WordPress attack surface and tech disclosure `Security`

- **Impact:** Brute-force exposure, information disclosure
- **Problem:** The security basics table warns that `/wp-admin/install.php` is reachable, the login form is on the default `/wp-login.php` path, and the `Server: Apache / ZoneOS` header discloses the stack.
- **Solution:**
  - Block the installer in `.htaccess`:

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

- Move or protect the login path (custom login slug, or IP allowlist / basic auth on `/wp-login.php`).
- Strip the version banner: `ServerTokens Prod` and `Header unset Server`.

3I. Disambiguate repeated link text `SEO`

- **Impact:** Anchor-text clarity, screen-reader navigation
- **Problem:** The HTML inventory flags vague repeated anchors: "code of conduct" ×3, "factory visitor reminder" ×2, "about us" ×2, "products" ×2, "resources" ×2, "timber purchasing" ×2, "contact" ×2.
- **Solution:**
  - Make each anchor's text unique in context, or add `aria-label`:

```
<a href="/en/about/" aria-label="About estply">about us</a>
```

  - Ensure the surrounding heading or list item provides the disambiguating context.

3J. Add Subresource Integrity to the jsDelivr script `Security`

- **Impact:** Supply-chain tampering risk
- **Problem:** Security basics reports 1 of 1 cross-origin scripts lacking an `integrity` attribute — `iframemanager.js` is loaded from cdn.jsdelivr.net.
- **Solution:**

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

  Better still, self-host the 3.0 KB file.

3K. Harden the WordPress install paths `Security`

- **Impact:** Attack surface
- **Problem:** Security basics warns that `/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>
```

- Move or protect the login path (custom login slug, IP allowlist, or HTTP basic auth in front of `/wp-login.php`).
- Also strip the `Server: Apache / ZoneOS` header via `ServerTokens Prod` / `ServerSignature Off`.

3L. Add valid structured data `SEO`

- **Impact:** Rich results eligibility
- **Problem:** Lighthouse `structuredData` fails and the single JSON-LD block is typed 'Unknown', so no Organization/WebPage schema is being recognised.
- **Solution:** Emit a typed graph, e.g.:

```
{"@context":"https://schema.org","@type":"WebPage","name":"Küpsiste poliitika","inLanguage":"en","url":"https://estply.com/en/kupsiste-poliitika/"}
```

  Validate with the Rich Results Test after deployment.

3M. Add Referrer-Policy, Permissions-Policy, COOP/CORP and HSTS preload `Security`

- **Impact:** Privacy leakage, feature abuse, origin isolation
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing, HSTS lacks `preload`, and 1 of 1 cross-origin scripts (cdn.jsdelivr.net) has no `integrity` attribute.
- **Solution:**

```
Header always set Referrer-Policy "strict-origin-when-cross-origin"
Header always set Permissions-Policy "camera=(), microphone=(), geolocation=()"
Header always set Cross-Origin-Opener-Policy "same-origin"
Header always set Cross-Origin-Resource-Policy "same-site"
Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains; preload"
```

  - Add SRI to the jsDelivr script: `<script src="…iframemanager.js" integrity="sha384-…" crossorigin="anonymous" defer>`.
  - Submit the domain at hstspreload.org once the preload directive is live.

3N. Close WordPress hardening gaps and stop disclosing the server `Security`

- **Impact:** Attack surface, information disclosure
- **Problem:** `/wp-admin/install.php` is reachable, the login form is on the default `/wp-login.php` path, and the `Server: Apache / ZoneOS` header discloses the stack.

- **Solution:**
  - Block the installer in `.htaccess`:

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

  - Move or protect the login path (a login-rename plugin or an IP/2FA gate on `/wp-login.php`).
  - Strip the version banner: `Header always unset Server` and `ServerTokens Prod` in the Apache config.

3O. Manually verify contrast on the 8 undetermined nodes `Accessibility`

- **Impact:** WCAG 1.4.3 Contrast
- **Problem:** axe-core returned 0 violations but flagged 8 nodes as incomplete for color-contrast — it cannot evaluate text over gradients or with alpha transparency.
- **Solution:**
  - Inspect the 8 flagged nodes in DevTools and confirm ≥4.5:1 for body text and ≥3:1 for large text.
  - Where text sits over an image or gradient, add a solid scrim behind it rather than relying on the image's average luminance.

3P. Harden remaining WordPress and header hygiene `Security`

- **Impact:** Attack surface, information disclosure
- **Problem:** HSTS lacks `preload`, the `Server: Apache / ZoneOS` header discloses the stack, `/wp-admin/install.php` is reachable, the login form sits on the default `/wp-login.php`, and 1 of 1 cross-origin scripts lacks an `integrity` attribute.
- **Solution:**
  - Add `preload` to HSTS once you are ready to submit to hstspreload.org.
  - Strip the `Server` header: `Header unset Server` / `ServerTokens Prod`.
  - Block the installer: `Redirect 404 /wp-admin/install.php`.
  - Move the login form off `/wp-login.php` (e.g. a security plugin's custom login URL).
  - Add SRI to the jsDelivr iframemanager script, or self-host it.

3Q. Stop sending `cache-control: max-age=0` **on the HTML document** `Performance`

- **Impact:** Repeat-visit TTFB, back/forward navigation
- **Problem:** The document response carries `cache-control: max-age=0` with an `expires` value only seconds ahead, so every navigation revalidates the HTML despite WP Rocket being active.
- **Solution:**
  - Let WP Rocket serve the cached HTML with a short browser TTL, e.g. `Cache-Control: public, max-age=600, stale-while-revalidate=60`.
  - Keep `max-age=0` only for logged-in or personalized responses.

3R. Manually verify the 109 undetermined contrast nodes `Accessibility`

- **Impact:** WCAG 1.4.3 color contrast
- **Problem:** axe-core returned 0 violations but could not determine contrast for 109 nodes (alpha transparency, gradients or overlapping backgrounds).
- **Solution:**
  - Run a contrast check in DevTools on the flagged nodes, especially text over the photographic hero and any semi-transparent overlays.
  - Target ≥4.5:1 for body text and ≥3:1 for large text (≥24 px or ≥18.66 px bold).