Audit Report: Tallinn accommodation made easy - Larsen

Website: https://larsen.ee/
Date: 13.10.2026
Audit Coverage: 70% — PageSpeed Insights: mobile: PSI HTTP 400; desktop: PSI HTTP 400; W3C Validator: W3C validator could not fetch the page: Non-XML Content-Type: “application/pdf”.; axe-core: page.goto: Download is starting Call log:

- navigating to "https://larsen.ee/terms-of-service", waiting until "networkidle" ; Browser Runtime: page.goto: Download is starting Call log:
- navigating to "https://larsen.ee/terms-of-service", waiting until "networkidle" ; HTML Inventory: page.goto: Download is starting Call log:
- navigating to "https://larsen.ee/terms-of-service", waiting until "networkidle" ; Optimized-Web Checklist: Requires html and securityHeaders to succeed; axe-core: page.goto: Download is starting Call log:
- navigating to "https://larsen.ee/privacy-policy", waiting until "networkidle" ; Browser Runtime: page.goto: Download is starting Call log:
- navigating to "https://larsen.ee/privacy-policy", waiting until "networkidle" ; HTML Inventory: page.goto: Download is starting Call log:
- navigating to "https://larsen.ee/privacy-policy", waiting until "networkidle"

Confidence: low

Pages Audited (5 of 5):

- https://larsen.ee/
- https://larsen.ee/about
- https://larsen.ee/faq
- https://larsen.ee/terms-of-service
- https://larsen.ee/privacy-policy

Summary of results

Overall Score: 68 / 100
Status: □ □ **Needs Improvement**

Site overall 68 is the mean of 3 pages. Scores range 64 (https://larsen.ee/about) → 70 (https://larsen.ee/faq). Weakest page: PSI mobile 70 vs desktop 89 with a large lab/field gap — lab LCP 5.5 s and FCP 4.06 s on mobile, but CrUX field LCP 1062 ms p75 (fast) and INP 96 ms, so the throttled simulation is likely pessimistic for real users. The dominant drag is image weight: 2.34 MB of the 2.65 MB total page weight is images, 11/17 raster images lack srcset, 11 lack width/height, and the hero (menu-image-11.jpg) is lazy-loaded with no fetchpriority, costing an estimated 363 KiB. Accessibility is close to passing (mobile 87, desktop 91) but axe flags one critical (button-name on .header__search-submit) and one serious (color-contrast on the current nav link). Security basics FAILED — no HTTP→HTTPS redirect, no HSTS, no CSP, no X-Frame-Options, plus readme.html public, installer reachable, and login on the default /wp-login.php path — which caps the score below 90. W3C reports 55 errors, mostly WordPress plugin inline styles outside @scope and invalid attributes, adding a further drag.

Per-page scores

 Needs Improvement · https://larsen.ee/

Score	Performance	Accessibility	Best Practices	SEO	Security
70	91	87	81	85	FAILED

 Needs Improvement · https://larsen.ee/about

Score	Performance	Accessibility	Best Practices	SEO	Security
64	70	87	81	92	FAILED

 Needs Improvement · https://larsen.ee/faq

Score	Performance	Accessibility	Best Practices	SEO	Security
70	89	87	100	92	FAILED

— · https://larsen.ee/terms-of-service

Score	Performance	Accessibility	Best Practices	SEO	Security
—	—	—	—	—	FAILED

— · https://larsen.ee/privacy-policy

Score	Performance	Accessibility	Best Practices	SEO	Security
—	—	—	—	—	FAILED

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://larsen.ee/	**91** / 95	**2.93 s** / 1.28 s	0.001 / **0.012**
https://larsen.ee/about	**70** / 89	**5.55 s** / 2.15 s	**0.004** / 0.001
https://larsen.ee/faq	**89** / 99	**3.02 s** / 809 ms	**0.029** / 0.000

Optimization Checklist

3 of 8 passing — 3 pass · 2 warn · 3 fail

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	**Pass**	All non-hero raster images use loading="lazy" except one.
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".

Item	Status	Detail
Hero is a real (not a CSS background -image)	**Warn**	Hero element uses a CSS background-image (no image-set() variants), so the browser always loads the original asset regardless of viewport — there is no srcset equivalent. Move the hero to a real with srcset/sizes (or) so smaller viewports can fetch a smaller file.
Responsive images (srcset /)	**Fail**	11/17 raster images lack srcset and are not inside .
Reasonable number of image sizes	**Fail**	No raster images use srcset; browsers cannot pick an optimally sized variant.
JS scripts not blocking in	**Warn**	2 render-blocking scripts in . Move to footer or add defer/async.

Fixes

Priority 1: Critical

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

1A. Stop autoloading 98.74 MB of video from storage.googleapis.com

`Performance`

- **Impact:** Page weight, data cost, LCP, FCP on real devices
- **Problem:** Browser runtime shows 6 media requests totalling 98.74 MB from storage.googleapis.com, with three net::ERR_ABORTED video requests (Larsen - Kokkuvõte eng bars.mp4, uus-logota-larsen-video-2.mp4). This dwarfs the 3.11 MB of images and 206 KB of scripts.
- **Solution:**
  - Add `preload="none"` and a poster image to every `<video>`; do not set `autoplay` on below-the-fold players.
  - Gate playback behind a click-to-play button that swaps in the `<source>` on demand.
  - Serve the MP4s from a CDN with range requests and consider HLS/DASH for adaptive bitrate.

```
<video preload="none" poster="/img/poster.webp" controls
playsinline>
  <source src="…mp4" type="video/mp4">
</video>
```

1B. Make the hero a real with eager loading and fetchpriority `Performance`

- **Impact:** LCP, FCP
- **Problem:** The optimized-web checklist fails 'Hero image eagerly loaded' — the hero `<img>` (menu-image-11.jpg) has `loading="lazy"` and no `fetchpriority` — and warns the hero is a CSS background-image on `div.buildings-map__map-overlay` (1200×800 px), so no srcset equivalent exists.
- **Solution:**
  - Replace the CSS background-image hero with a real `<img>` (or `<picture>`) carrying `srcset` / `sizes`.
  - Set `loading="eager"` (or omit) and `fetchpriority="high"` on the LCP image.

```
<img src="/img/hero-1200.webp"
     srcset="/img/hero-800.webp 800w, /img/hero-1200.webp 1200w,
/img/hero-1600.webp 1600w"
     sizes="100vw"
     fetchpriority="high" decoding="async"
     width="1200" height="800" alt="…">
```

1C. Give the header search submit button an accessible name `Accessibility`

- **Impact:** WCAG 4.1.2 (Name, Role, Value); screen reader users cannot identify the control
- **Problem:** axe-core reports a critical `button-name` violation on `.header__search-submit` — the button has no discernible text. PSI's `button-name` audit also scores 0.00 (weight 10).
- **Solution:** Add a visible or visually-hidden label:

```
<button class="header__search-submit" type="submit" aria-
label="Search">
  <svg aria-hidden="true" focusable="false">…</svg>
</button>
```

1D. Add Strict-Transport-Security (HSTS) `Security`

- **Impact:** TLS downgrade / SSL-strip protection
- **Problem:** Security basics marks Strict-Transport-Security as FAILED — the header is missing, so browsers will happily follow an http:// link to this origin.

- **Solution:**

  ```
  Header always set Strict-Transport-Security "max-age=63072000;
  includeSubDomains; preload"
  ```

  Start with a short max-age to verify, then raise it and submit to hstspreload.org.

1E. Add clickjacking protection `Security`

- **Impact:** Framing / UI-redress attacks
- **Problem:** Security basics marks Clickjacking protection as FAILED — neither X-Frame-Options nor CSP frame-ancestors is set, so the page can be framed.
- **Solution:** Prefer CSP frame-ancestors, with X-Frame-Options as a fallback for older browsers:

  ```
  Header always set Content-Security-Policy "frame-ancestors 'self'"
  Header always set X-Frame-Options "SAMEORIGIN"
  ```

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

- **Impact:** LCP, FCP
- **Problem:** The hero image (menu-image-11.jpg) has loading="lazy" and no fetchpriority, and mobile lab LCP is 5.5 s / FCP 4.06 s.
- **Solution:** Mark the hero as eager and give it priority:

  ```
  <img src=".../menu-image-11.jpg" loading="eager"
  fetchpriority="high" width="1600" height="900" alt="…">
  ```

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

1G. Optimize and serve responsive images `Performance`

- **Impact:** LCP, page weight
- **Problem:** Images account for 2.34 MB of the 2.65 MB total page weight; PSI estimates 363 KiB savings and 11/17 raster images lack srcset.
- **Solution:**
  - Convert JPEG/PNG to WebP/AVIF and add `<picture>` fallbacks.
  - Add `srcset` / `sizes` to the 11 images missing them (menu-image-11/22, the two 150×150 PNGs, the GreenKey logo).
  - Re-encode the 342.6 KB menu-image-22.jpg, which is the largest single image request.

1H. Redirect HTTP to HTTPS and enable HSTS `Security`

- **Impact:** Transport security, downgrade attacks
- **Problem:** http://larsen.ee/about does not redirect to HTTPS and the Strict-Transport-Security header is missing.
- **Solution:** Force HTTPS at the edge/origin and send HSTS:

  ```
  Header always set Strict-Transport-Security "max-age=63072000;
  includeSubDomains; preload"
  ```

  Then submit the domain to hstspreload.org.

1I. Give the search submit button an accessible name `Accessibility`

- **Impact:** WCAG 4.1.2 (button-name)
- **Problem:** axe reports a critical button-name violation on `.header__search-submit` — the button has no discernible text.
- **Solution:** Add visible text or an aria-label:

  ```
  <button class="header__search-submit" aria-label="Search">…
  </button>
  ```

1J. Enforce HTTPS redirect and add HSTS `Security`

- **Impact:** Transport security, session hijacking, downgrade attacks
- **Problem:** Security basics FAILED: http://larsen.ee/faq does not redirect to HTTPS and Strict-Transport-Security is missing — both basic-tier checks.
- **Solution:** Redirect all plain HTTP to HTTPS at the edge/origin, then send HSTS:

  ```
  # nginx
  server { listen 80; server_name larsen.ee; return 301
  https://$host$request_uri; }
  add_header Strict-Transport-Security "max-age=63072000;
  includeSubDomains; preload" always;
  ```

  Verify with `curl -I http://larsen.ee/faq` (expect 301) and submit to hstspreload.org once stable.

1K. Give the header search button an accessible name `Accessibility`

- **Impact:** WCAG 4.1.2, screen reader users
- **Problem:** axe critical button-name violation on .header__search-submit; PSI button-name scores 0.00 (weight 10).
- **Solution:** Add an accessible name to the submit button:

```
<button class="header__search-submit" aria-label="Search">
  <svg aria-hidden="true">…</svg>
</button>
```

Or include a visually-hidden `<span class="sr-only">Search</span>` inside the button.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Fix color contrast on the current-page nav link `Accessibility`

- **Impact:** WCAG 1.4.3 (AA); readability
- **Problem:** axe-core reports a serious `color-contrast` violation on `.is-current[aria-current="page"][href$="larsen.ee/"]`; PSI's color-contrast audit also scores 0.00 (weight 7).
- **Solution:**
  - Darken the active nav link color to reach ≥4.5:1 against its background (or ≥3:1 if it qualifies as large text).
  - Verify with the DevTools contrast checker, including hover/focus states.

2B. Enlarge touch targets and label the unlabeled form inputs `Accessibility`

- **Impact:** WCAG 2.5.8 target size; WCAG 1.3.1/4.1.2 form labels
- **Problem:** PSI's `target-size` audit scores 0.00 (weight 7) and `tapTargets` is a failing SEO-modeled audit; HTML inventory also shows Form 2 with two text inputs that have no label.
- **Solution:**
  - Ensure every interactive control is at least 44×44 px with adequate spacing (WCAG 2.5.8).
  - Associate a `<label for>` (or `aria-label`) with each text input in Form 2.

```
<label for="newsletter-email">Email</label>
<input id="newsletter-email" type="email" name="email"
autocomplete="email">
```

2C. Ship responsive, dimensioned images `Performance`

- **Impact:** LCP, CLS, image bytes (est. 251 KiB savings)
- **Problem:** PSI's `image-delivery-insight` estimates 251 KiB of savings; HTML inventory shows 11 of 40 images without explicit width/height and only 29/40 using

srcset, and the checklist flags menu-image-11.jpg and menu-image-22.jpg as non-responsive.

- **Solution:**
  - Add `width` / `height` (or `aspect-ratio` in CSS) to all 11 images missing dimensions to reserve layout space.
  - Extend `srcset` / `sizes` to the remaining 11 raster images; the site already generates 18 widths, so reuse them.
  - Convert the remaining JPEG/PNG assets to WebP/AVIF.

```
<img src="/img/menu-800.webp"
     srcset="/img/menu-400.webp 400w, /img/menu-800.webp 800w,
/img/menu-1200.webp 1200w"
     sizes="(max-width: 800px) 100vw, 800px"
     width="800" height="600" loading="lazy" alt="…">
```

2D. Defer or move the render-blocking scripts `Performance`

- **Impact:** FCP (2.71 s mobile), Speed Index (2.92 s), TBT
- **Problem:** HTML inventory shows 22 scripts with only 1 defer and 2 async, and 6 render-blocking scripts; the checklist flags 2 render-blocking scripts in `<head>` (iframemanager.js and cookieconsent.umd.js from cdn.jsdelivr.net). PSI's `render-blocking-insight` is a medium priority fix.
- **Solution:**
  - Add `defer` to `iframemanager.js` and `cookieconsent.umd.js` (both are safe to defer — they only run on user interaction).
  - Audit the remaining 4 render-blocking scripts and defer or move to the footer where execution order allows.
  - Inline the critical CSS and load the rest with `media="print" onload="this.media='all'"`.

2E. Add a Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is missing (Security basics: advanced FAILED). Site signals show no auth, payments, or user-generated content, but the page does expose a booking flow and a search form, so a baseline CSP is worth deploying.
- **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'
```

Roll it out in Report-Only mode first and watch for violations from GTM, Chatbase and the jsDelivr-hosted consent scripts.

2F. Close WordPress hygiene gaps `Security`

- **Impact:** Attack surface, information disclosure
- **Problem:** Security basics reports readme.html is public and reveals WordPress, /wp-admin/install.php is reachable, and the login form is served on the default /wp-login.php path.
- **Solution:**
  - Delete or block `readme.html`:

```
<Files readme.html>
  Require all denied
</Files>
```

  - Block the installer: `Redirect 403 /wp-admin/install.php`.
  - Move the login form off `/wp-login.php` (e.g. a custom slug) and rate-limit it.
  - Keep the WordPress core, theme and plugins patched — the audit does not test plugin vulnerabilities.

2G. Add a meta description `SEO`

- **Impact:** Search snippet CTR
- **Problem:** HTML inventory shows `Description: not set`, and PSI's `meta-description` audit scores 0.00.
- **Solution:** Add a unique 120–155 character description to the homepage:

```
<meta name="description" content="Furnished apartments and co-
living rooms across Tallinn — instant booking, flexible stays, all-
inclusive rent.">
```

2H. Disambiguate repeated vague link text `SEO`

- **Impact:** Anchor relevance, accessibility of link purpose
- **Problem:** HTML inventory finds "learn more" repeated 6 times plus "home", "locations", "features", "testimonials" and others repeated 3 times each; PSI's `link-text` audit scores 0.00 with 6 links flagged.
- **Solution:**
  - Rewrite anchors to describe the destination, e.g. "Learn more about Sume" instead of "learn more".

    - Where the visual design requires short text, add `aria-label` with the full purpose.

2I. Fix color contrast on the current nav link `Accessibility`

- **Impact:** WCAG 1.4.3 (color-contrast)
- **Problem:** axe reports a serious color-contrast violation on `.is-current[aria-current="page"][href$="about/"]`, and 6 further nodes could not be evaluated.
- **Solution:** Raise the foreground/background contrast ratio to at least 4.5:1 for the active nav state, and manually verify the 6 incomplete nodes (likely alpha/gradient backgrounds axe skips).

2J. Add clickjacking protection `Security`

- **Impact:** Clickjacking
- **Problem:** Neither X-Frame-Options nor CSP frame-ancestors is set, so the page can be framed.
- **Solution:** Prefer CSP frame-ancestors; keep X-Frame-Options as a fallback:

```
Header always set X-Frame-Options "SAMEORIGIN"
Header always set Content-Security-Policy "frame-ancestors 'self'"
```

2K. Deploy a nonce-based Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is missing. The site is WordPress with a reachable /wp-login.php, so an XSS foothold could compromise admin sessions.
- **Solution:** Use 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';
```

  Note the two cross-origin scripts (jsdelivr) will need nonces or SRI hashes.

2L. Add explicit width/height to images `Performance`

- **Impact:** CLS
- **Problem:** 11 of 17 images lack explicit width/height attributes, which can cause layout shifts.
- **Solution:** Add intrinsic dimensions to every `<img>` (and `<source>`), or set `aspect-ratio` in CSS so the browser reserves space before load.

2M. Fix the 55 W3C HTML validation errors `Best Practices`

- **Impact:** Markup correctness, maintainability

- **Problem:** W3C reports 55 errors, led by invalid `src` on `<source>` (×6), `defer` on non-JS script types (×4), and dozens of style rules outside `@scope` in a body `<style>` block.
- **Solution:**
  - Replace `<source src="…">` with `srcset` (or use `<img src>` for the fallback).
  - Remove `defer` / `async` from `type="text/rocketlazyloadscript"` data blocks.
  - Move the inline `<style id="larsen-book-a-tour-styles">` block into `<head>` or wrap its rules in `@scope`.
  - Fix `area-hidden` → `aria-hidden` on the header search form.

2N. Harden the WordPress install `Security`

- **Impact:** Attack surface, information disclosure
- **Problem:** readme.html is public, /wp-admin/install.php is reachable, and the login form is served on the default /wp-login.php path.
- **Solution:**
  - Delete or block `readme.html`.
  - Block `/wp-admin/install.php` in .htaccess or via the WAF.
  - Move or protect the login path (custom login URL plugin, or IP allowlist on /wp-login.php).

2O. Serve responsive images with srcset and modern formats `Performance`

- **Impact:** Page weight, LCP, Speed Index
- **Problem:** 11/11 raster images lack srcset and are not inside ; menu-image-22.jpg alone is 342.6 KB and total image bytes are 919 KB.
- **Solution:** Emit multiple widths and let the browser choose:

```
<img src="hero-800.jpg"
     srcset="hero-400.jpg 400w, hero-800.jpg 800w, hero-1600.jpg
1600w"
     sizes="(max-width: 600px) 100vw, 800px"
     width="800" height="800" alt="…">
```

  Also convert JPEG/PNG to WebP/AVIF with a `<picture>` fallback.

2P. Fix color contrast on current-page links `Accessibility`

- **Impact:** WCAG 1.4.3, readability

- **Problem:** axe serious color-contrast violation on .is-current[aria-current="page"] [href$="faq/"] and the matching footer link; PSI color-contrast scores 0.00 (weight 7).
- **Solution:** Darken the current-page link color to reach ≥4.5:1 against its background (≥3:1 for large text). Verify with the DevTools contrast checker or axe DevTools.

2Q. Fix invalid aria-expanded values on accordion buttons `Accessibility`

- **Impact:** WCAG 4.1.2, ARIA state, screen readers
- **Problem:** W3C reports 53 errors 'Bad value "" for attribute "aria-expanded" on element "button"' (first at line 544); axe flags 53 incomplete aria-valid-attr-value nodes.
- **Solution:** Set a real boolean string on every accordion toggle:

  ```
  <button aria-expanded="false" aria-controls="…">…</button>
  ```

  Update the attribute in JS when the panel opens/closes; never leave it empty.

2R. Enlarge touch targets `Accessibility`

- **Impact:** WCAG 2.5.8, mobile usability
- **Problem:** PSI target-size scores 0.00 (weight 7) and SEO tapTargets is failing.
- **Solution:** Ensure every interactive element is at least 44×44 px with adequate spacing:

  ```
  .header__search-submit, .footer__navigation-link { min-width: 44px; min-height: 44px; }
  ```

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Fix the W3C validation errors `Best Practices`

- **Impact:** Markup correctness, maintainability
- **Problem:** W3C reports 57 errors and 4 warnings, dominated by 12 `srcset`-without-`sizes` errors and a large cluster of style rules in a `<body>` `<style>` element that the validator says must be inside `@scope`.
- **Solution:**
  - Add a `sizes` attribute to every `<img>` that uses width descriptors in `srcset` (12 occurrences).
  - Move the `#larsen-book-a-tour-styles` block out of `<body>` into `<head>`, or wrap its rules in `@scope`.

- Fix the remaining structural errors: `area-hidden` typo on `#header-search` (should be `aria-hidden`), empty `action=""` on two forms, and `src` on `<source>` at line 1370.

3B. Remove deprecated APIs and add SRI to cross-origin scripts `Best Practices`

- **Impact:** Lighthouse Best Practices (81 mobile / 77 desktop)
- **Problem:** PSI's `deprecations` audit scores 0.00 (weight 5) with 1 warning, and Security basics flags 4 of 4 cross-origin scripts lacking an `integrity` attribute.
- **Solution:**
  - Identify the deprecated API via the Lighthouse `deprecations` details and replace it.
  - Add `integrity` + `crossorigin="anonymous"` to the jsDelivr-hosted scripts:

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

3C. Fix the heading outline and structured data `SEO`

- **Impact:** Document outline, rich results eligibility
- **Problem:** HTML inventory shows 2 `<h1>` elements ("Tallinn accommodation made easy" and "Choose your stay") and PSI's `structuredData` audit is failing; the single JSON-LD block is typed "Unknown".
- **Solution:**
  - Keep exactly one `<h1>` per page; demote "Choose your stay" to `<h2>`.
  - Replace the unrecognized JSON-LD with a valid schema.org type (e.g. `LodgingBusiness` / `Organization`) and validate it in the Rich Results Test.

3D. Add the remaining low-cost security headers `Security`

- **Impact:** Referrer leakage, feature abuse, cross-origin isolation
- **Problem:** Security basics reports Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy all missing, and the `server: cloudflare` 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-origin"
Header always set X-Permitted-Cross-Domain-Policies "none"
```

Note: these are hygiene improvements, not a security guarantee — application logic, plugins and dependencies are not tested here.

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

- **Impact:** Privacy, origin isolation
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing.
- **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-origin"
```

3F. Add SRI to cross-origin scripts `Security`

- **Impact:** Supply-chain integrity
- **Problem:** 2 of 2 cross-origin scripts (jsdelivr iframemanager and cookieconsent) lack an `integrity` attribute.
- **Solution:** Add `integrity="sha384-…"` and `crossorigin="anonymous"` to each CDN `<script>` tag, or self-host the libraries.

3G. Increase touch target sizes `Accessibility`

- **Impact:** WCAG 2.5.8 (target-size)
- **Problem:** PSI's `target-size` audit fails on mobile and axe flags touch targets as a manual check.
- **Solution:** Ensure every interactive element is at least 44×44 px with adequate spacing, especially nav links and icon buttons.

3H. Add structured data and disambiguate link text `SEO`

- **Impact:** Rich results, link purpose
- **Problem:** PSI's `structuredData` audit fails (JSON-LD type is Unknown) and repeated vague link text appears ("home" ×3, "locations" ×3, "faq" ×3).
- **Solution:**
  - Emit valid `LocalBusiness` / `Organization` JSON-LD with name, address and contact details.

- Disambiguate repeated nav links with `aria-label` or visually hidden context.

3I. Optimize web fonts `Performance`

- **Impact:** FCP, page weight
- **Problem:** Fonts total 292.9 KB, including a 225.1 KB variable font (inter-tight-variable.woff2); mobile FCP is 2.87 s.
- **Solution:**
  - Subset the variable font to the glyphs actually used (Latin + Estonian).
  - Preload the primary font file:

```
<link rel="preload" href="/…/inter-tight-variable.woff2" as="font"
type="font/woff2" crossorigin>
```

  - Keep `font-display: swap` and drop the redundant Google Fonts request if the self-hosted file covers it.

3J. Add Subresource Integrity to cross-origin scripts `Security`

- **Impact:** Supply-chain integrity
- **Problem:** 2 of 2 cross-origin scripts lack an integrity attribute (jsdelivr CDN: iframemanager.js, cookieconsent.umd.js).
- **Solution:** Pin versions and add SRI hashes:

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

  Better still, self-host these two libraries to remove the third-party dependency.

3K. Add structured data `SEO`

- **Impact:** Rich results eligibility
- **Problem:** PSI structuredData is failing and the single JSON-LD block has type 'Unknown'.
- **Solution:** Add a valid schema.org block matching the page, e.g.:

```
<script type="application/ld+json">
{"@context":"https://schema.org","@type":"FAQPage","mainEntity":
[…]}
</script>
```

  Validate with the Rich Results Test.