

Audit Report: A place with a character. In a neighbourhood that has one too. - The Diplomat

Website: <https://thediplomat.ee/>

Date: 2026-07-03

Overall Score: 78 / 100

Status: ☐ **Needs Improvement**

Confidence: high

Audit Coverage: 100% — all sources returned data

Pages Audited (5 of 5):

- <https://thediplomat.ee/>
- <https://thediplomat.ee/contact>
- <https://thediplomat.ee/faq>
- <https://thediplomat.ee/et/kkk>
- <https://thediplomat.ee/for-business-customers>

Summary

Site overall 78 is the mean of 5 pages. Scores range 74 (<https://thediplomat.ee/faq>) → 82 (<https://thediplomat.ee/>). Weakest page: Mobile performance is strong at 88 with excellent TTFB (6 ms), but LCP (3.0 s) exceeds the 2.5 s threshold. Security is the weakest area with a 13/100 header grade and HTTP failing to redirect to HTTPS, which is critical given the site accepts user content. Accessibility has one critical axe violation regarding invalid ARIA values on accordions. SEO is mostly solid but lacks a meta description. Confidence is high as all audit tools returned complete data.

Per-Page Scores

Page	Score	Status	Confidence
https://thediplomat.ee/	82	☐ Needs Improvement	high
https://thediplomat.ee/contact	78	☐ Needs Improvement	high
https://thediplomat.ee/faq	74	☐ Needs Improvement	high

Page	Score	Status	Confidence
https://thediplomat.ee/et/kkk	76	 Needs Improvement	high
https://thediplomat.ee/for-business-customers	78	 Needs Improvement	high

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://thediplomat.ee/	91 / 100	3.16 s / 776 ms	0.012 / 0.000
https://thediplomat.ee/contact	94 / 99	2.75 s / 910 ms	0.010 / 0.000
https://thediplomat.ee/faq	88 / 100	2.96 s / 731 ms	0.000 / 0.000
https://thediplomat.ee/et/kkk	88 / 99	3.05 s / 724 ms	0.000 / 0.001
https://thediplomat.ee/for-business-customers	94 / 99	2.87 s / 873 ms	0.016 / 0.001

Optimization Checklist

4 of 4 passing — 4 pass · 0 warn · 0 fail · 3 n/a

Item	Status	Detail
Page caching plugin / CDN active	Pass	Caching plugin detected (WP Rocket) + CDN Cloudflare/Kinsta
Images lazy-loaded	Pass	All non-hero raster images use loading="lazy" except one.

Item	Status	Detail
Hero image eagerly loaded	Pass	Hero image is eagerly loaded (inferred from DOM order/size — Lighthouse LCP element unavailable).
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.
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 HSTS and Content-Security-Policy headers

- **Impact:** Security Headers Grade, XSS/Clickjacking protection
- **Problem:** Security Headers grade is 13/100; HSTS and CSP are missing despite site signals indicating user-generated content (upload link).
- **Solution:** Add HSTS with preload and a strict CSP:

```
Strict-Transport-Security: max-age=63072000; includeSubDomains;
preload
Content-Security-Policy: default-src 'self'; script-src 'nonce-
{random}' 'strict-dynamic'; object-src 'none'; base-uri 'none';
```

1B. Fix serious color-contrast violation

- **Impact:** WCAG 1.4.3 Compliance, Accessibility Score
- **Problem:** axe-core reports 1 serious violation on `.button--secondary` where background and foreground colors lack sufficient contrast.
- **Solution:** Increase contrast ratio to at least 4.5:1 for the secondary button text. Use a darker text color or lighter background in CSS.

1C. Enforce HTTPS redirect and add HSTS

- **Impact:** Transport security, data integrity

- **Problem:** HTTP does not redirect to HTTPS (<http://thediplomat.ee/contact> stays on HTTP), and HSTS is missing. Security Headers grade is 13/100.
- **Solution:** Configure the web server or CDN (Cloudflare) to redirect all HTTP traffic to HTTPS immediately.

Cloudflare Page Rule:

- URL: `thediplomat.ee/*`
- Setting: `Always Use HTTPS`

Apache/Nginx (Origin):

```
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

Add HSTS Header:

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

1D. Implement Content Security Policy (CSP)

- **Impact:** XSS protection, data exfiltration prevention
- **Problem:** CSP is missing. Site signals indicate User-Generated Content (textarea, upload link), making XSS risk high per the security rubric.
- **Solution:** Deploy a strict CSP with nonces for scripts. Start with a report-only mode to avoid breaking WP Rocket/CDN scripts.

Header:

```
Header always set Content-Security-Policy "default-src 'self';
script-src 'nonce-{RANDOM}' 'strict-dynamic' https;; style-src
'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self'
data: https;; font-src 'self' https://fonts.gstatic.com; form-
action 'self'; frame-ancestors 'self';"
```

Implementation:

- Generate a random nonce per request in PHP/WordPress.
- Add `nonce="{NONCE}"` to all `<script>` tags.
- Monitor `Content-Security-Policy-Report-Only` before enforcing.

1E. Enforce HTTPS and Add Critical Security Headers

- **Impact:** Transport security, XSS protection, clickjacking

- **Problem:** HTTP does not redirect to HTTPS, and HSTS/CSP are missing. Site signals indicate User-Generated Content (textarea/upload), making XSS protection critical.
- **Solution:** Configure server/CDN to redirect all HTTP traffic to HTTPS. Add the following headers:

```
Strict-Transport-Security: max-age=63072000; includeSubDomains;
preload
Content-Security-Policy: default-src 'self'; script-src 'nonce-
{random}' 'strict-dynamic';
X-Frame-Options: SAMEORIGIN
```

1F. Fix Critical ARIA Attribute Values

- **Impact:** Accessibility (WCAG 4.1.2)
- **Problem:** Critical axe violation: `aria-expanded` uses value '1' instead of 'true'/'false' on accordion buttons. W3C validator confirms 4 instances of this error.
- **Solution:** Update accordion buttons to use boolean strings:

```
<button aria-expanded="true" aria-controls="...">
  Toggle Section
</button>
```

1G. Force HTTPS redirect and add HSTS

- **Impact:** Transport security, MITM protection
- **Problem:** HTTP does not redirect to HTTPS (<http://thediplomat.ee/et/kkk> does not redirect) and HSTS is missing, leaving users vulnerable on insecure connections.
- **Solution:** Configure the web server (Nginx/Apache) to return 301 redirects for all HTTP traffic to HTTPS. Add HSTS header:

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

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Optimize Largest Contentful Paint (LCP)

- **Impact:** Performance Score, LCP Metric
- **Problem:** Mobile LCP is 3.2 s (warning zone), flagged by PSI `largest-contentful-paint` and `image-delivery-insight`.
- **Solution:**

- Preload the LCP image resource.
- Ensure hero image uses `fetchpriority="high"` .
- Convert remaining heavy images to WebP/AVIF if not already done.

2B. Fix W3C script type/defer errors

- **Impact:** HTML Validity, Potential JS Execution Issues
- **Problem:** W3C Validator reports 4 errors where `script` elements with non-standard `type` attributes (e.g., `text/rocketlazyloadscript`) incorrectly use the `defer` attribute.
- **Solution:** Update WP Rocket configuration or custom scripts to remove `defer` from non-standard script types, or change `type` to `text/javascript` where appropriate.

2C. Fix W3C Validation Errors (Scripts & ARIA)

- **Impact:** Maintainability, Accessibility compliance
- **Problem:** 19 W3C errors found, including 11 instances of `type="text/rocketlazyloadscript"` with `defer` and 3 invalid `aria-expanded=""` attributes.
- **Solution:**
 1. **Scripts:** Remove `type` attribute from standard JS or use valid MIME types (`text/javascript`). WP Rocket's lazyload script type is non-standard.
 2. **ARIA:** Fix `aria-expanded` to be `true` or `false` (not empty string).
 3. **Hidden Inputs:** Remove `autocomplete` from `type="hidden"` inputs.

Example Fix:

```
<!-- Before -->
<button aria-expanded="" ...>
<!-- After -->
<button aria-expanded="false" ...>
```

2D. Add Meta Description and Structured Data

- **Impact:** SEO, Search Result CTR
- **Problem:** PSI SEO audit fails `metaDescription` and `structuredData` . HTML Inventory confirms Description is not set.
- **Solution:** Add a unique meta description (150-160 chars) in the `<head>` .

```
<meta name="description" content="Contact The Diplomat for
inquiries regarding apartments, payments, and general support."
```

Reach out via our secure form.">

Add JSON-LD for `ContactPage` or `LocalBusiness` :

```
<script type="application/ld+json">
{
  "@context": "https://schema.org",
  "@type": "ContactPage",
  "name": "Contact The Diplomat"
}
</script>
```

2E. Add Meta Description for SEO

- **Impact:** SEO (Search Snippets)
- **Problem:** W3C and PSI report missing meta description. This affects click-through rates in search results.
- **Solution:** Add a concise description (150–160 characters) in the `<head>` :

```
<meta name="description" content="Frequently asked questions about
The Diplomat apartments, payments, and move-in process.">
```

2F. Fix W3C validation errors and ARIA attributes

- **Impact:** Accessibility, Standards compliance
- **Problem:** 19 W3C errors including invalid `aria-expanded="1"` (should be true/false) and invalid script types with `defer` attribute.
- **Solution:**
 - Update `aria-expanded` values to boolean strings (`true / false`).
 - Remove `type="text/rocketlazyloadscript"` or use valid MIME types for scripts.
 - Fix hidden input autocomplete attributes per W3C spec.

2G. Add Meta Description

- **Impact:** SEO, Click-through rate
- **Problem:** SEO audit flags `metaDescription` as missing; document has no description tag.
- **Solution:** Add a concise description (150–160 chars) in the `<head>` :

```
<meta name="description" content="Korduma kippuvad küsimused The
Diplomat'i teenuste kohta. Leia vastused broneerimise, maksete ja
majutuse küsimustele.">
```

2H. Fix W3C HTML Validation Errors

- **Impact:** Maintainability, Compliance
- **Problem:** 15 errors found, including 11 instances of `script` with invalid `type` attributes (WP Rocket) and hidden inputs with `autocomplete`.
- **Solution:**
 - Remove `type` attribute from standard JS scripts (or use valid MIME types).
 - Remove `autocomplete` from `input type="hidden"` elements.
 - Move `meta charset` to the first 1024 bytes of the document.
 - Fix unclosed `<p>` tags.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Ensure lazy loading for below-fold images

- **Impact:** Page Weight, Initial Load Time
- **Problem:** HTML Inventory shows 2 images missing `loading="lazy"` despite being below the fold.
- **Solution:** Add `loading="lazy"` to all `<img>` tags that are not the LCP element or above the fold.

3B. Optimize LCP and Font Loading

- **Impact:** Core Web Vitals (LCP 2.8 s)
- **Problem:** Mobile LCP is 2.8 s (warning zone). PSI suggests 80 ms savings from font-display and 142 KiB from image delivery.
- **Solution:**
 1. **Fonts:** Add `font-display: swap` to CSS or use `display=swap` in Google Fonts URL.
 2. **Images:** Ensure the LCP image (likely the hero) is preloaded or has `fetchpriority="high"` (already present per checklist, verify priority).
 3. **Images:** Convert remaining raster images to WebP/AVIF if not already done.

Google Fonts:

```
<link href="https://fonts.googleapis.com/css?family=Open+Sans&display=swap" rel="stylesheet">
```

3C. Resolve W3C HTML Validation Errors

- **Impact:** Maintainability, Browser Compatibility
- **Problem:** 19 errors found, including invalid script types (`text/rocketlazyloadscript` with `defer`) and hidden inputs with `autocomplete` .
- **Solution:**
 - Remove `defer` from non-JavaScript script types (WP Rocket optimization).
 - Remove `autocomplete` from `type="hidden"` inputs.
 - Move `meta charset` to the first 1024 bytes of the document.

3D. Optimize LCP and Image Delivery

- **Impact:** Performance (LCP 2.9 s)
- **Problem:** LCP is 2.9 s (warning threshold) and PSI suggests 187 KiB savings via image delivery optimization.
- **Solution:**
 - Convert remaining JPEGs to WebP/AVIF.
 - Ensure the LCP image (likely the hero) has `fetchpriority="high"` .
 - Preload the LCP image resource in the `<head>` .