AESIR

PRIVACY COMPLIANCE REPORT

Compliance Findings for Your Website

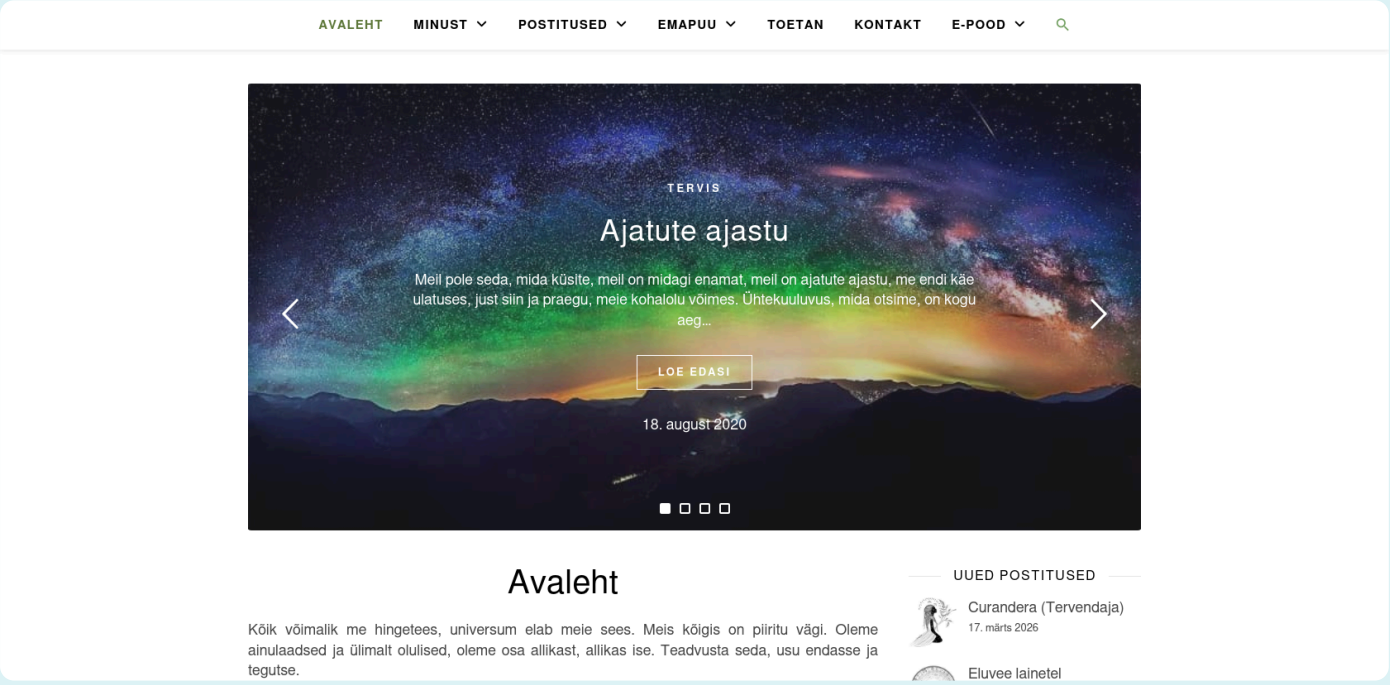
Status: Low Risk

0 Beacons and 0 Cookie Violations Found

Scan Date: 2026-06-22

Subject: Privacy and Compliance Analysis of https://hingetee.ee based on ePrivacy Directive and GDPR

Privacy Scan: https://hingetee.ee



Need Guidance?

Request a follow-up

Leave Your Details

Your Privacy Scan Summary

Subject: Privacy and Compliance Summary Based on GDPR and ePrivacy Directive
Scanned Website: https://hingetee.ee
Scan Date: 2026-06-22

Status: Low Risk

This report assesses https://hingetee.ee privacy compliance concerning third-party data sharing and tracking before consent under the GDPR, ePrivacy Directive (ePD), and CCPA.

Risk Levels:

- **Low Risk:** Complies fully with GDPR, ePD, PECR, CCPA, and global privacy regulations by requiring explicit consent before any tracking and keeping all personal data under first-party control.
- **Medium Risk:** No third-party cookies are set, but image-type beacons load before consent. This partial tracking may lead to compliance issues.
- **High Risk:** Trackers are activated before consent or transfer of personal data, including IP address, to third parties during consent management, risking non-compliance.

1. No Violations Identified

Your scanned URL/s did not trigger any unauthorized tracking technologies during this scan.

This is a good indication that your consent strategy is currently working as intended.

Findings indicate that:

- **0 Beacons (Tracking Pixels) load before consent.**
- **0 Non-Compliant Cookies are set before consent.**

However, privacy compliance isn't static. Third-party plugins, script behaviors, or browser updates can introduce new risks – sometimes without notice. We recommend running scans regularly to keep your site compliant with evolving laws and tech changes.

Important Reminder: If this scan only included your homepage, risks may still exist on subpages like checkout, blog, or video pages. Rescan and add subpages for a fuller view.

Note:

- *This report reflects the status at the time of scanning. While no issues were found, this should not be taken as a permanent guarantee of compliance.*
- *These results are from the EDPS Inspection Tool and EasyPrivacy list – AesirX does not generate this data.*

2. Compliance Risks and Consequences

If regulators investigate, your organization may face the following consequences:

Regulatory Violation	Legal Reference	Risk
Tracking before consent	GDPR Art 5, 6, 7; ePD Art, 5(3)	Fines up to €20 million or 4% turnover.
Misleading cookie classification	GDPR Art 12, 13	Enforcement for deceptive consent practices
Third-party scripts pre-consent	ePD Art 5(3)	Investigations and sanctions by DPAs

3. What You Need to Do

1. Audit and Fix Cookies
Implement a fully compliant Consent Management Platform (CMP).

2. Block Unauthorized Trackers
Use first-party data tools. Data stays under your control and reduces third-party privacy risks.

3. Monitor Privacy Continuously
Automate or do regular manual compliance checks to detect future risks.

How AesirX Can Help

Resolve unauthorized third-party tracking with a fully compliant CMP.

AesirX Consent Management Platform
Prevent Unauthorized Tracking
Automatically detects and blocks ALL trackers before consent for full compliance.

Automate regular compliance checks to detect future risks.

Privacy Monitoring
Continuous Privacy Scans
Automatically detects compliance risks so you stay compliant.

1 Website Evidence Collection

1.1 https://hingetee.ee

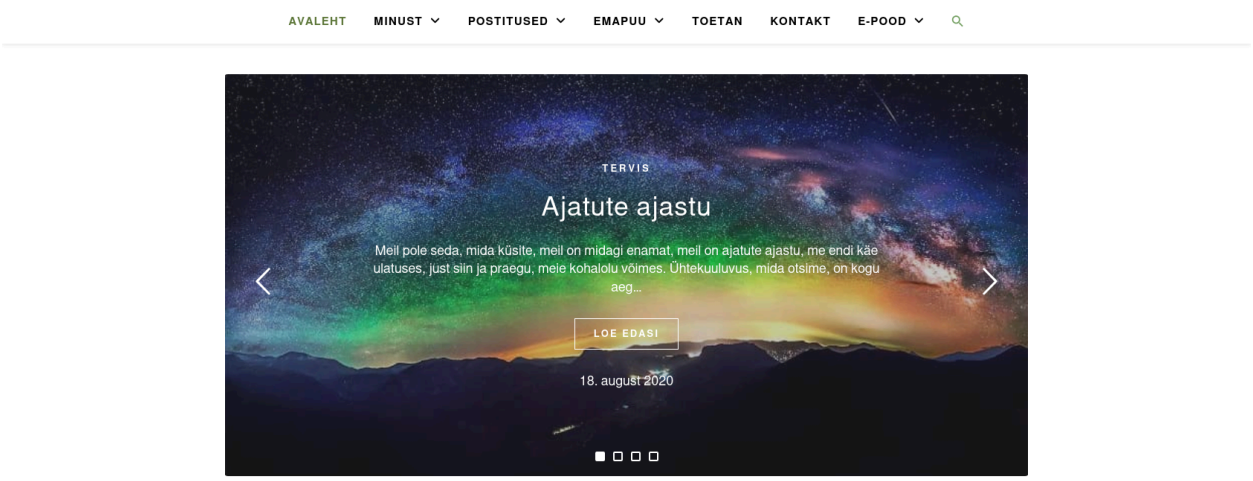
2 Evidence Collection Organisation

Target Web Service	`https://hingetee.ee`
Automated Evidence Collection Start Time	6/22/2026, 10:01:22 PM
Automated Evidence Collection End Time	6/22/2026, 10:01:31 PM
Software Version	2.1.1
Software Host	0d73487eda79

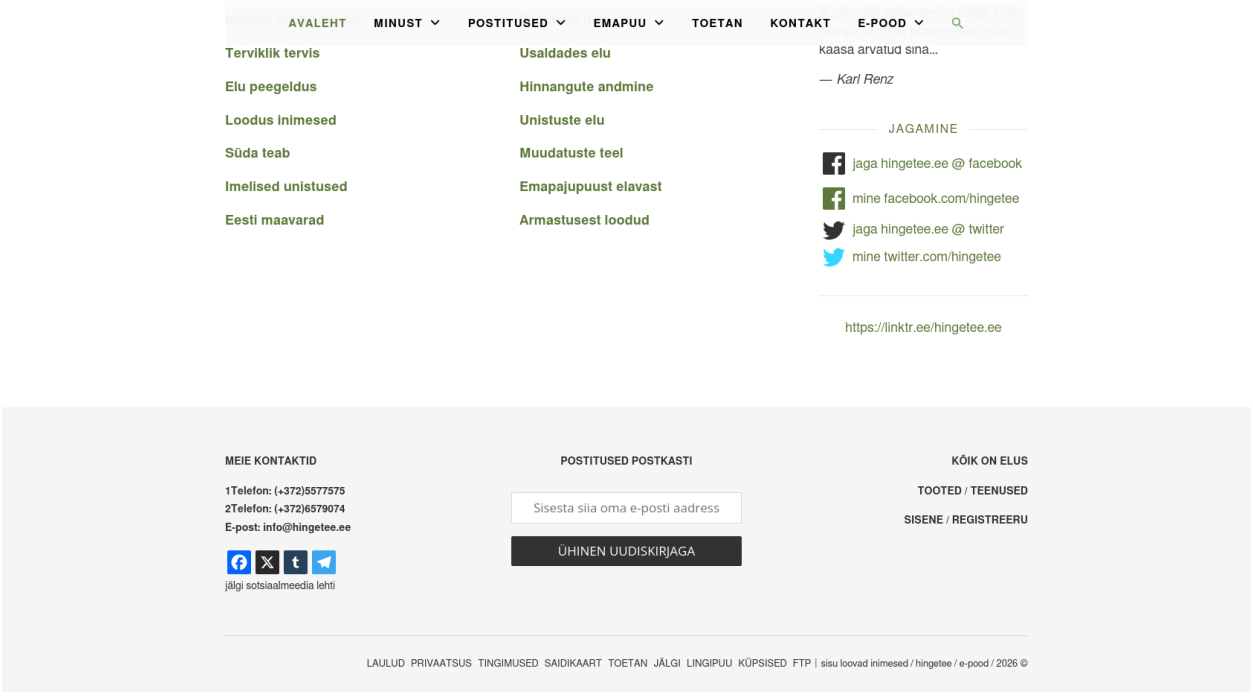
3 Automated Evidence Collection

3.1 Webpage Visit

On 6/22/2026, 10:01:22 PM, the evidence collection tool navigated the browser to https://hingetee.ee. The final location after potential redirects was https://hingetee.ee/. The evidence collection tool took two screenshots to cover the top of the webpage and the bottom.



Webpage Top Screenshot



Webpage Bottom Screenshot

3.2 Use of HTTPS/SSL

The evidence collection tool assessed the redirecting behaviour of hingetee.ee with respect to the use of HTTPS.

allows connection with HTTPS	false
HTTP redirect to HTTPS	false
HTTP redirect location	
Error when connecting with HTTP	ReferenceError: HttpsAgent is not defined

Error when connecting with HTTPS	ReferenceError: HttpsAgent is not defined

3.3 Use of Content Security Policies (CSPs)

Upon browser request of a web page, websites can indicate in the Content Security Policy (CSP) meta data sent along with the requested web page a whitelist of mechanisms, domains and subdomains that browsers must respect when embedding components, such as styles, fonts, beacons, videos, maps, etc.

No CSP meta data was found. Consequently, no restrictions apply.

3.4 Use of Social Media and Collaboration Platforms

Link URL	Link Caption
https://www.facebook.com/sharer/sharer.php?u=http:/...	jaga hingetee.ee @ facebook
https://www.facebook.com/hingetee	mine facebook.com/hingetee
https://twitter.com/intent/tweet?url=http://hingetee.ee/	jaga hingetee.ee @ twitter
https://twitter.com/hingetee	mine twitter.com/hingetee
https://facebook.com/hingetee	
https://www.tumblr.com/hingetee	

Common social media and collaboration platforms linked from https://hingetee.ee/ have been considered.

3.5 Traffic and Persistent Data Analysis

The evidence collection tool simulates a browsing session of the web service to analyse hereafter the recorded traffic between the browser and the Internet as well as the persistent data stored in the browser. First, the browser visited https://hingetee.ee/. The evidence collection took no other web page(s) into account. Generally, predefined pages and a random subset of all first-party link targets (URLs) from the initial web page https://hingetee.ee/ are considered. The exhaustive list of browsed web pages is given in the Annex.

The web page(s) were browsed consecutively between 6/22/2026, 10:01:22 PM and 6/22/2026, 10:01:31 PM.

During the browsing, the HTTP Header Do Not Track was not set.

For the subsequent analysis, the following hosts (with their path) were defined as first-party:

1. hingetee.ee

3.5.1 Traffic Analysis

In the case of a visit of a very simple web page with a given URL, the browser sends a *request* to the web server configured for the domain specified in the URL. The web server, also called *host*, sends then a *response* in the form of e.g. an HTML file that the browser downloads and displays. Most web pages nowadays are more complex and require the browser to send further requests to the same host (*first-party*) or even different hosts (potentially *third-party*) to download e.g. images, videos and fonts and to embed e.g. maps, tweets and comments. Please find more information about hosts and the distinction between first-party and third-party in the glossary in the Annex.

The evidence collection tool extracted lists of distinct first-party, respectively third-party, hosts from the browser requests recorded as part of the traffic. Note that if a specific path is configured to be first-party, than requests to other paths may lead to the first-party host being also listed amongst the third-party hosts.

A number of techniques allow hosts to track the browsing behaviour. The first-party host may instruct the browser to send requests for the (sole) purpose of providing information embedded in the request (e.g. cookies) to a given first-party or third-party host. Often, those requests are then responded with an empty file or with an image of size 1×1 pixel. Such files requested for the purpose of tracking are commonly called *web beacons*.

The evidence collection tool compares all requests to signature lists compiled to detect potential web beacons or otherwise problematic content. The positive matches with the lists EasyPrivacy (`easyprivacy.txt`) and Fanboy's Annoyance (`fanboy-annoyance.txt`) from https://easylist.to are presented in the Annex. The list of *web beacon hosts* contains hosts of those requests that match the signature list EasyPrivacy. Note that the result may include false positives and may be incomplete due to inaccurate, outdated or incomplete signature lists.

Eventually, the evidence collection tool logged all identified web forms that potentially transmit web form data using an unencrypted connection.

First-Party Hosts

1. hingetee.ee

Requests have been made to 1 distinct first-party hosts.

Third-Party Hosts

Requests have been made to 0 distinct third-party hosts.

First-Party Web Beacon Hosts

No first-party web beacons were found.

Third-Party Web Beacon Hosts

No third-party web beacons were found.

Third-Party Content Security Policy Hosts

Upon browser request of a web page, websites can indicate in the Content Security Policy (CSP) meta data sent along with the requested web page a whitelist of mechanisms, domains and subdomains that browsers must respect when embedding components, such as styles, fonts, beacons, videos, maps, etc.

No third-party content security policy hosts were whitelisted.

Web Forms with non-encrypted Transmission

No web forms submitting data without SSL encryption were detected.

3.5.2 Persistent Data Analysis

The evidence collection tool analysed persistent cookies after the browsing session. Web pages can also use the persistent HTML5 *local storage*. The subsequent section lists its content after the browsing.

Cookies linked to First-Party Hosts

No first-party cookies were found.

Cookies linked to Third-Party Hosts

No third-party cookies were found.

Local Storage

The local storage was found to be empty.

Annex

A Browsing History

For the collection of evidence, the browser navigated consecutively to the following 1 webpage(s):

1. https://hingetee.ee/

B All Beacons

The data transmitted by beacons using HTTP GET parameters are decoded for improved readability and displayed beneath the beacon URL.

C Glossary

Filter Lists

Browser extensions commonly referred by *Adblocker* have been developed to block the loading of ads based on filter lists. Later on, filter lists have been extended to also block the loading of web page elements connected to the tracking of web page visitors. For this evidence collection, publicly available tracking filter lists are re-purposed to identify web page elements that may track the web page visitors.

Do Not Track (DNT for short, HTTP)

The Do Not Track header is the proposed HTTP header field DNT that requests that a web service does not track its individual visitors. Note that this request cannot be enforced by technical means on the visitors' side. It is upon the web service to take the DNT header field into account. For this evidence collection, the Do Not Track header is not employed.

First Party

In this document, *first party* is a classification of the resources links, web beacons, and cookies. To be first party, the resource domain must match the domain of the inspected web service or other configured first party domains. Note that the resource path must also be within the path of the web service to be considered first party.

Host (HTTP)

The HTTP *host* is the computer receiving and answering browser requests for web pages.

Redirect (HTTP)

A request for a web page may be answered with a new location (URL) to be requested instead. These HTTP *redirects* can be used to enforce the use of HTTPS. Visitors who requested an HTTP web page are redirected to the corresponding HTTPS web page.

Request (HTTP)

To download and display a web page identified by a URL, browsers send HTTP *requests* with the URL to the host computer specified as part of the URL.

Local Storage (HTML5)

Modern web browsers allow web pages to store data locally in the browser profile. This *local storage* is website-specific and persistent through browser shutdowns. As embedded third-party resources may also have access to the first-party local storage, it is classified both as first- and third-party.

Third Party

Links, web beacons, and cookies that are not *first party* (see above) are classified as *third party*.

Web Beacon

A web beacon is one of various techniques used on web pages to unobtrusively (usually invisibly) allow tracking of web page visitors. A web beacon can be implemented for instance as a 1×1 pixel image, a transparent image, or an empty file that is requested together with other resources when a web page is loaded.

Web Beacon Host

The *host* in the URL of a *request* of a *Web Beacon* is called *Web Beacon host*.

Unsure what to do next?

We can help interpret your results and suggest the next steps.

Request Guidance

Want to stay compliant?
Ready to fix any issues found?

Take control of all tracking technologies – not just cookies – with AesirX CMP. Try it free for 14 days, manage scripts based on real consent, and run a new scan showing no unauthorized cookies or beacons.

Learn More