

Important Privacy Compliance Findings for Your Website

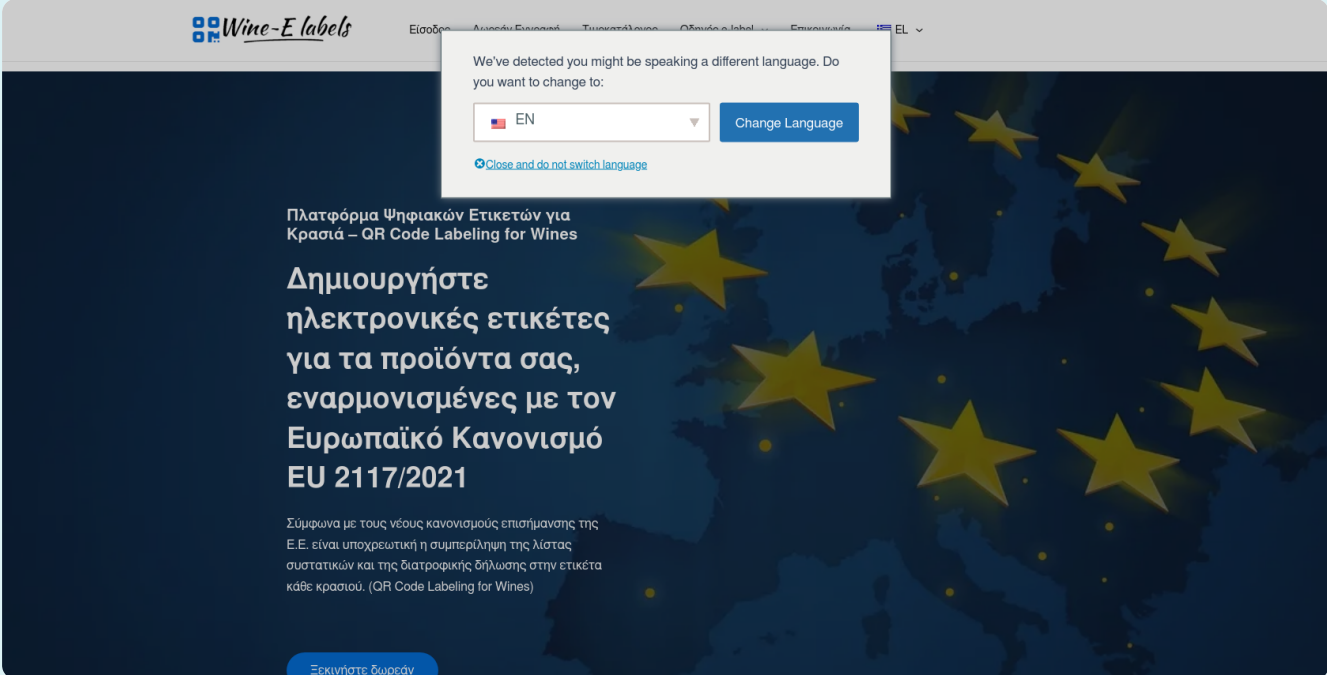
https://wine-elabels.eu

 **Low Risk**

No violations found!

This site does not appear to be in breach of the GDPR. However, if this is your site, you might still want to consider ordering a manual [Privacy Compliance Review](#) to ensure you are not in breach of any other privacy regulations.

AesirX Privacy Scan: 2024-07-13



The screenshot shows the website 'Wine-E labels' with a language selection popup. The popup text reads: 'We've detected you might be speaking a different language. Do you want to change to: EN Change Language Close and do not switch language'. The main content is in Greek: 'Πλατφόρμα Ψηφιακών Ετικετών για Κρασιά – QR Code Labeling for Wines', 'Δημιουργήστε ηλεκτρονικές ετικέτες για τα προϊόντα σας, εναρμονισμένες με τον Ευρωπαϊκό Κανονισμό EU 2117/2021', and 'Σύμφωνα με τους νέους κανονισμούς επισήμανσης της Ε.Ε. είναι υποχρεωτική η συμπερίληψη της λίστας συστατικών και της διατροφικής δήλωσης στην ετικέτα κάθε κρασιού. (QR Code Labeling for Wines)'. A button at the bottom says 'Ξεκινήστε δωρεάν'.



Transparent Verification & Authentication

By accessing this link, an on-chain transaction will open in a new window on the Concordium Blockchain. This transaction transparently verifies the time & date of the scanned report, confirming its authenticity. [\[Check Your Transactions\]](#)

Table of Contents

Part 1 - UNDERSTANDING THE PROCESS & LEGALITIES

1. Understanding AesirX Privacy Scanner's Assessment Process
2. Legal Foundations of AesirX Privacy Scanner's Assessments
3. Legal Considerations and Compliance Strategies
4. Actionable Steps Post-Scan

Part 2 - YOUR RESULTS & EVIDENCE

5. Your Risk Status
6. Website Evidence Collection
7. Evidence Collection Organization
7. Evidence Collection Organization

Part 3 - ANNEX

- A. Browsing History
- B. All Beacons
- C. Glossary

Part 1 - UNDERSTANDING THE PROCESS & LEGALITIES

1. Understanding AesirX Privacy Scanner's Assessment Process



When you use the AesirX Privacy Scanner, you're leveraging a powerful combination of the European Data Protection Supervisor (EDPS) Inspection Tool and the comprehensive EasyPrivacy list to evaluate your website's compliance and privacy posture. Here's how we break down the assessment process to determine if your site is at Low, Medium, or High Risk based on the findings:

1/ Utilizing the EDPS Inspection Tool

The EDPS Inspection Tool is an open-source software designed for the automated collection of evidence regarding personal data processing on websites. It captures a wide array of data points, including cookies, HTML5 local storage interactions, and HTTP traffic. This tool is crucial for understanding how your website interacts with user data, from the moment a visitor lands on your page until they leave.

2/ Incorporating the EasyPrivacy List

EasyPrivacy is an essential component of our assessment. It's a supplementary filter list that targets and removes all forms of internet tracking. By comparing the data collected from your website against the EasyPrivacy list, we can identify tracking scripts, web bugs, and information collectors that may compromise user privacy.

3/ Scoring Based on Findings

The core of our assessment lies in how the findings from the EDPS Inspection Tool align with the EasyPrivacy list. We categorize the elements found on your website into different risk levels based on their potential to infringe on user privacy:

✓ Low Risk

Websites with minimal tracking elements or those that strictly adhere to privacy-preserving practices, showing little to no match with the EasyPrivacy list.

ⓘ Medium Risk

Websites that have some tracking elements which could potentially track user behavior but are not extensively invasive. These might show a moderate level of matches with the EasyPrivacy list.

⚠ High Risk

Websites with a significant number of tracking elements that extensively match the EasyPrivacy list, indicating a high level of potential user tracking and data collection without adequate consent mechanisms.

4/ Comprehensive Reporting

The final step in our process is generating a detailed report that categorizes your website's privacy and data processing practices into Low, Medium, or High Risk. This report is based on the quantitative analysis of how many and what type of privacy-infringing elements are detected on your site, offering actionable insights for improvement.

Why This Matters

Understanding the assessment process is crucial for website owners and developers aiming to enhance their site's privacy stance. By aligning your website's operations with the principles of data protection and user privacy, you not only comply with regulatory standards like GDPR but also build trust with your visitors.

The AesirX Privacy Scanner, powered by the EDPS Inspection Tool and the EasyPrivacy list, provides a foundational step toward achieving a privacy-focused online presence.



[EXPLORE OUR PRIVACY REVIEW](#)

Get a Streamlined Review of Your Organization's Current Privacy Practices

Enhance your site's privacy posture & align with GDPR through detailed assessment & actionable insights.

The Privacy Compliance Review is a focused audit designed to strengthen your privacy commitment and improve your data protection strategies. We assess your privacy framework and provide actionable insights and strategic recommendations.

[Learn more & start enhancing your compliance here](#)

2. Legal Foundations of AesirX Privacy Scanner's Assessments

At AesirX, we understand the importance of compliance in the digital landscape. Our Privacy Scanner's assessments are grounded in two key pieces of European legislation: the General Data Protection Regulation (GDPR) and the revised ePrivacy Directive article 5(3), now extending to digital. Here's how these frameworks guide our assessment process:

1/ General Data Protection Regulation (GDPR)

The GDPR defines data protection and privacy for all individuals within the European Union and European Economic Area, covering the transfer of personal data outside these areas. Its principles –lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality (security), and accountability– form our assessment criteria. Our tool analyzes your website to specifically look for:



Consent Mechanisms

How your website obtains, records, and manages user consent for data processing activities, ensuring they align with GDPR's requirements for explicit and informed consent.



Data Processing Activities

Any instance of personal data collection, storage, and sharing with third parties is scrutinized to ensure it meets GDPR's lawfulness and transparency requirements.



Cookies and Trackers

The use of cookies and other tracking technologies is evaluated to ensure they do not infringe on users' privacy rights without proper consent, adhering to GDPR's stipulations.

2/ ePrivacy Directive

While the ePrivacy Directive focuses on privacy in electronic communications, its principles, based on Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive adopted 14 Nov. 2023, significantly influence our assessment. The directive complements GDPR by detailing rules on electronic communications data, cookies, and direct marketing. Our scanner assesses:



Cookie Compliance

Evaluates how your website deploys cookies and if it provides clear, comprehensive information and obtains user consent as mandated by the ePrivacy Directive.



Electronic Communications Data

Examines data processing in electronic communications services to ensure compliance with the ePrivacy Directive's confidentiality and security requirements.

3/ Ensuring Legal Compliance and Building Trust



Our use of the GDPR and ePrivacy Directive highlights our commitment to helping website owners with compliance in data protection and privacy.

Aligning your website with these laws not only ensures legality but also shows your users their privacy is valued and protected.

The AesirX Privacy Scanner bridges complex legal requirements and practical website implementation.

It provides actionable insights and recommendations based on legal standards, helping you to enhance your site's compliance and, ultimately, build a stronger foundation of trust with your users.

DISCOVER OUR FIRST-PARTY FOUNDATION SOLUTIONS

Ensure your website meets the latest compliance standards.

A graphic with a dark blue background. It features a white document with a blue circular icon containing the text 'GDPR' and a blue shield with a white 'X' inside.

Embark on a transformative digital experience with AesirX First-Party Foundation designed to help you store, collect, manage and analyze first-party data legally, ethically, and efficiently.

Trust, Compliance, and Efficiency

A shield icon with a checkmark inside a circle.

Increased Trust

A shield icon with three stars and a lock symbol inside a circle.

Enhanced Compliance

A circular icon with a magnifying glass and a document symbol inside a circle.

Deeper Insights

[Find out more & secure your site's future here](#)

3. Legal Considerations and Compliance Strategies

Privacy regulations are increasingly stringent, so understanding and adhering to Article 5(3) of the ePrivacy Directive is crucial for website owners. This directive calls for explicit user consent before storing/accessing information on a device, a requirement that now applies to a range of tracking technologies, not just cookies. Compliance is not just a legal obligation but a commitment to upholding user privacy.



1/ Implementing Transparent Consent Mechanisms

Compliance with Article 5(3) hinges on clear, informed user consent. Owners must make consent mechanisms transparent, easily understandable, and accessible. Forms or banners must explicitly describe the data types being collected, purpose of data collection, and how data will be used. Consent must be given through a clear action, like clicking "I Agree".

2/ Privacy by Design

Adopting a privacy-by-design approach is essential. This means integrating data protection and privacy into the development phase of your website or digital service, not as an afterthought. Ensure default settings favor privacy, limiting data collection to what is strictly necessary for the provided service.

3/ Regular Privacy Audits

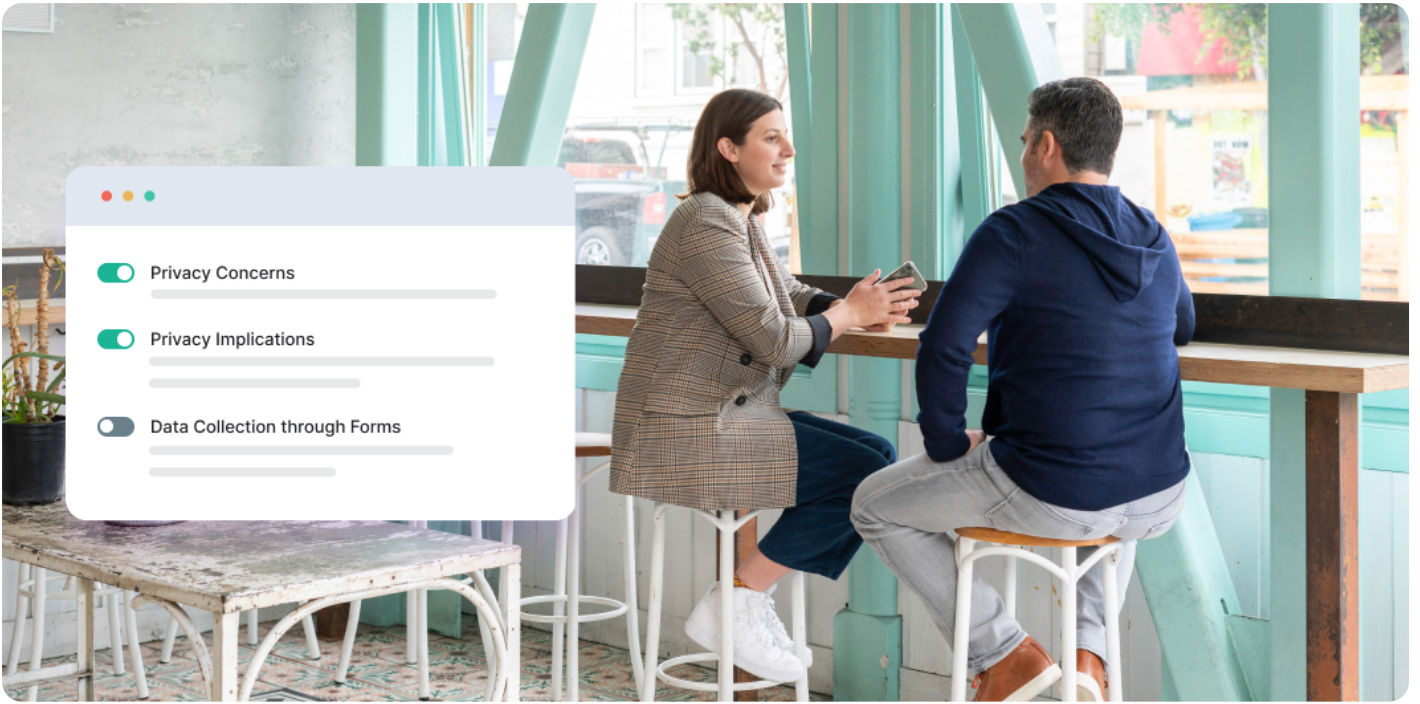
Conduct regular audits to identify any privacy compliance gaps, reviewing cookies and trackers, disclosing data collection practices to users, and checking consent mechanisms. Audits should also assess adherence to the latest privacy regulations and guidelines.

4/ Educating Users

Beyond compliance, educating users digital privacy importance and how their data is being used can foster trust and transparency. Providing resources or links to more detailed privacy information can empower users to make informed decisions about their data.

5/ Leveraging Privacy-Enhancing Technologies

Explore privacy-enhancing technologies that minimize the amount of personal data collected and stored. Techniques such as anonymization or pseudonymization of user data can reduce privacy risks while still allowing for meaningful data analysis and personalization.



6/ Collaborating with Legal and Privacy Experts

Given the complexities of privacy regulations, seeking advice from legal and privacy experts can provide valuable insights into compliance strategies tailored to your specific digital context. These professionals can help navigate the regulatory landscape, ensuring that your digital practices align with both the letter and spirit of the law.

7/ Actionable Compliance Checklist

Develop a compliance checklist based on Article 5(3) guidelines, including steps for implementing consent mechanisms, conducting privacy audits, and updating privacy policies. This checklist can serve as a practical tool for ongoing compliance monitoring and improvement.

8/ Response to Regulatory Changes

Stay informed about regulatory changes and updates to privacy laws, including potential modifications to the ePrivacy Directive and the interplay with GDPR. Adapting to these changes promptly ensures continuous compliance and protects against legal risks.

4. Actionable Steps Post-Scan

Embracing First-Party Solutions and Ensuring Compliance

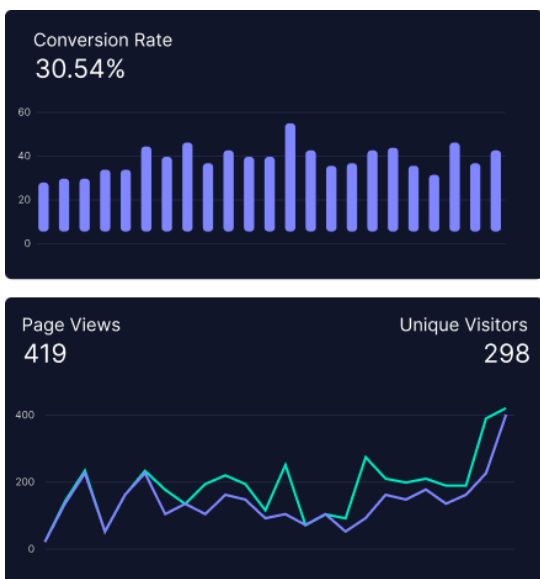
Receiving your AesirX Privacy Scanner report is the first step toward enhancing your website's privacy and compliance. Many websites face legal risks from deploying third-party cookies, pixel trackers, and beacons before obtaining informed consent from users. This practice contravenes GDPR and the ePrivacy Directive, undermining user trust. Here's what you need to do next:

1/ Understanding the Report

Your report highlights non-compliance and potential privacy risks on your website, focusing on the premature loading of third-party cookies and trackers. These findings are crucial for identifying the necessary adjustments to align your site with legal requirements and best practices.

2/ Transitioning to First-Party Solution

Transitioning to first-party solutions mitigates legal risks and enhances privacy compliance by gathering data directly from your audience or customers and storing it on your servers or systems. This approach reduces privacy risks and ensures greater control and quality of data collected.



✔ Identify Third-Party Dependencies:

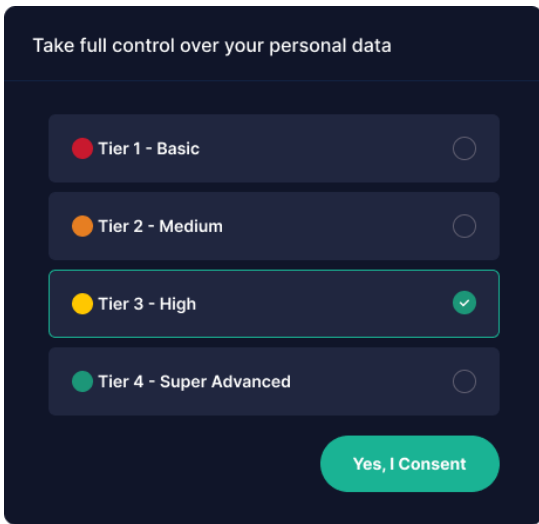
Review the report to identify which elements rely on third-party services (e.g., analytics, advertising, customer tracking).

✔ Seek First-Party Alternatives:

For each third-party service identified, research first-party alternatives or ways to achieve similar functionality without compromising user privacy. Solutions like AesirX Analytics offer robust insights without the privacy concerns associated with traditional third-party analytics tools.

3/ Correcting Technical Setups

Many privacy issues stem from incorrect technical setups that lead to the unauthorized loading of trackers and cookies. Ensuring compliance requires technical adjustments:



- ✔ **Deferred Loading:**
Modify your website's code to defer the loading of any tracking technologies until after the user has provided informed consent.
- ✔ **Implement Consent Management:**
Use a consent management platform (CMP) that complies with GDPR and ePrivacy Directive requirements, informing users about data collection and obtaining explicit consent before any data processing occurs.

4/ Continuous Monitoring and Updating

Privacy compliance is not a one-time effort but an ongoing process. Monitor your website regularly for new risks and stay updated with regulatory changes to adjust your practices accordingly.

Next Steps: Implementing changes and seeking expertise

- ✔ **Prioritize Changes:**
Prioritize the implementation of changes, starting with those posing the highest risk of non-compliance.
- ✔ **Consult with Data Privacy Experts:**
(Or legal advisors) to ensure your transition to first-party solutions and overall privacy strategy align with laws and best practices. AesirX's Privacy Compliance Review plays a vital role in ensuring your website remains compliant and secure over time. [CTA]
- ✔ **Educate Your Team:**
Train your team on privacy compliance and first-party solutions for a smooth transition. Focus on key principles and technical needs.
- ✔ **Automate for Easy Compliance:**
Solutions like AesirX Privacy Monitoring Service automates scans for effortless compliance management. Customize scan frequency, get real-time alerts, and audit up to 100 sites at once. [CTA]

By following these steps and transitioning to first-party solutions, you address compliance issues identified in your AesirX Privacy Scanner report and build a more privacy-respectful online presence. Remember, investing in privacy minimizes legal risks and demonstrates that user privacy is valued and protected.

PART 2 - YOUR OFFICIAL REPORT RESULTS & EVIDENCE

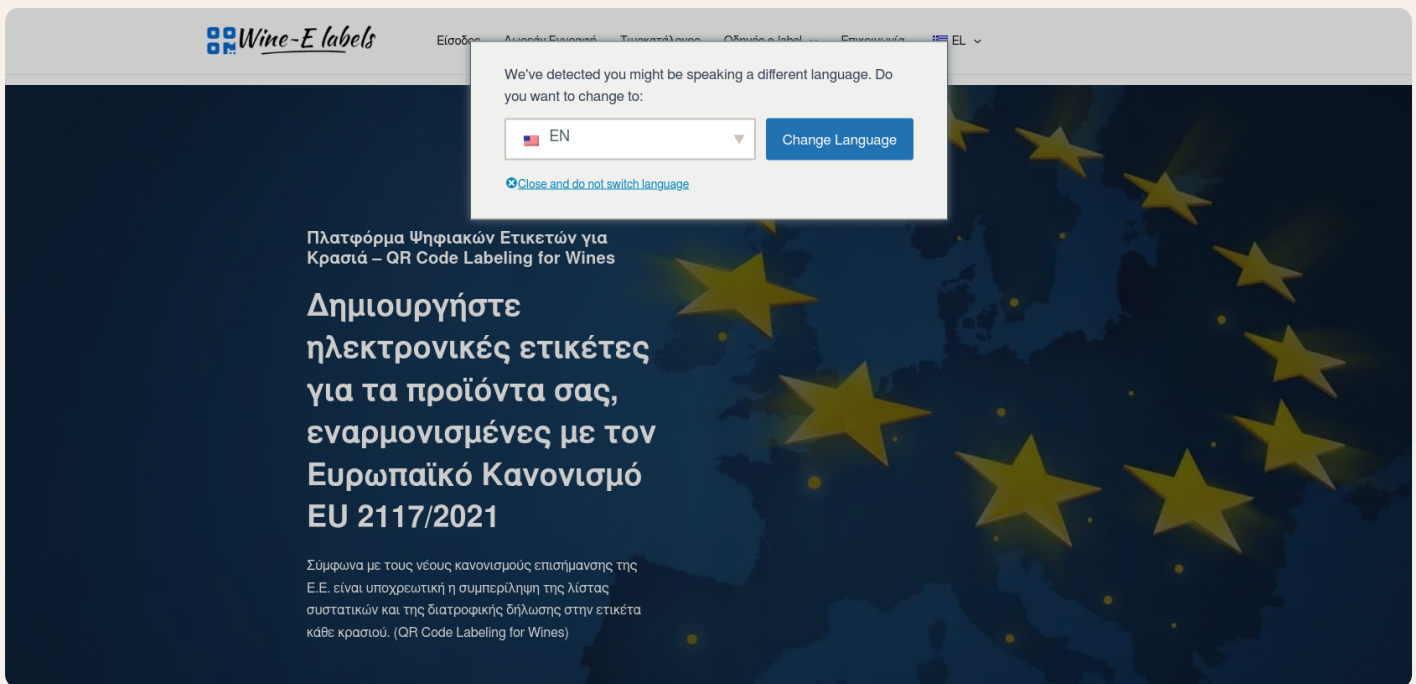
<https://wine-elabels.eu>

✓ Low Risk

No violations found!

This site does not appear to be in breach of the GDPR. However, if this is your site, you might still want to consider ordering a manual [Privacy Compliance Review](#) to ensure you are not in breach of any other privacy regulations.

AesirX Privacy Scan: 2024-07-13



Part 2 of the AesirX Privacy Scan delivers OFFICIAL results and evidence from the EDPS Inspection Tool and the EasyPrivacy list, verifying your website's compliance with GDPR and the ePrivacy Directive.

Should you need further explanation of this comprehensive data, we invite you to reach out for a detailed Privacy Compliance Review.

Our service offers a tailored review of your organization's privacy practices, focusing on enhancing your commitment to privacy and improving data protection strategies. We assess your privacy framework and provide actionable insights and strategic recommendations.

Transparent Verification & Authentication

AesirX Privacy Scan in Partnership with Concordium blockchain offers a unique on-chain verification process that ensures the authenticity of your reports by transparently verifying their timestamps. Find this feature on the results page.

1 Website Evidence Collection



1.1 <https://wine-elabels.eu>

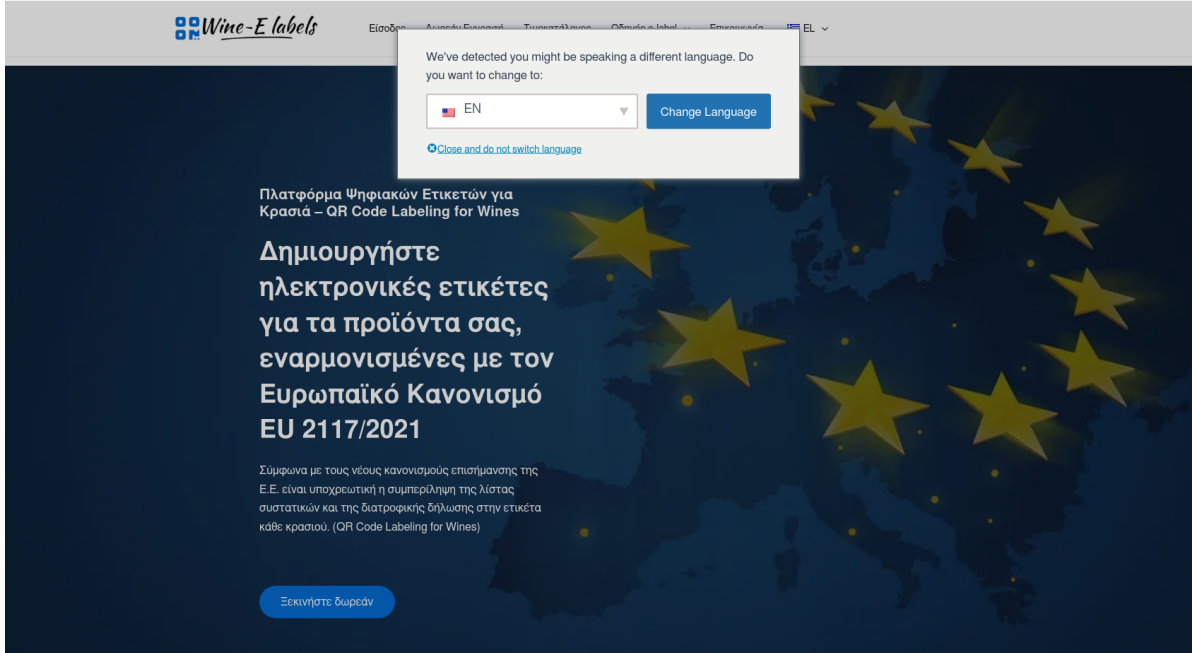
2 Evidence Collection Organisation

Target Web Service	<code>https://wine-elabels.eu</code>
Automated Evidence Collection Start Time	7/13/2024, 11:43:30 AM
Automated Evidence Collection End Time	7/13/2024, 11:43:38 AM
Software Version	2.1.1
Software Host	62adb522bdb3

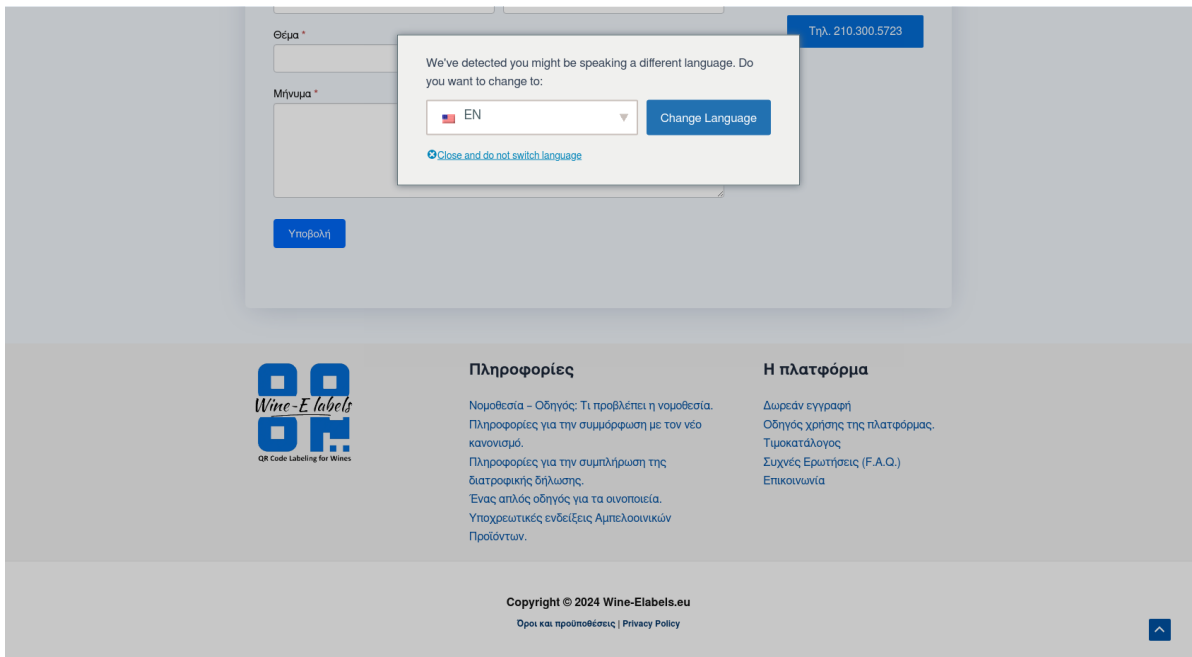
3 Automated Evidence Collection

3.1 Webpage Visit

On 7/13/2024, 11:43:30 AM, the evidence collection tool navigated the browser to <https://wine-elabels.eu>. The final location after potential redirects was <https://wine-elabels.eu/>. 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 wine-elabels.eu 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

3.3 Use of Social Media and Collaboration Platforms

No corresponding links were found.

Common social media and collaboration platforms linked from <https://wine-elabels.eu/> have been considered.

3.4 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://wine-elabels.eu/>. 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://wine-elabels.eu/> are considered. The exhaustive list of browsed web pages is given in [the Annex](#).

The web page(s) were browsed consecutively between 7/13/2024, 11:43:30 AM and 7/13/2024, 11:43:38 AM.

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. wine-elabels.eu

3.4.1 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. [wine-elabels.eu](#)

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.

Web Forms with non-encrypted Transmission

No web forms submitting data without SSL encryption were detected.

3.4.2 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

#	Host	Path	Name	Expiry in days
1	wine-elabels.eu	/	trp_language	30

In total, 1 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://wine-elabels.eu/>

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*.

AESIR^X

Transforming marketing with innovative privacy-focused solutions.

AesirX stands as a bastion of strength, leading the fight for digital privacy against BigTech's abuse of personal data!

As the digital landscape changes, so do the challenges surrounding privacy and legal compliance. At AesirX, we understand the concerns that businesses face when it comes to navigating complex privacy laws. We firmly believe that no business owner should unknowingly use illegal technology and risk being labeled a criminal.

[Learn More.](#)

Privacy Compliance Review

This Introductory Privacy Compliance Review is a focused audit designed to strengthen your privacy commitment and improve your data protection strategies.

We assess your privacy framework and provide actionable insights and strategic recommendations.

**Exclusive Launch Deal:
Introductory price only \$995!**

It's the ideal time to enhance your data privacy & strategize toward full compliance.

[Request a Review Now](#)



AESIRX ANALYTICS
Free & open source:
Compliant data-driven web analytics.

[Download](#)

