

## Website Privacy Test of djs-place.freemyip.com

- ✓ Privacy Policy Review

✓ Tracking Technologies Detection
- ✓ Privacy-Invasive Practices Detection

✓ Cookies & External Content Detection
- Free online tool to test website privacy  
**80,272** privacy security tests performed

HOME

MONITOR

STATISTICS

NEW

API

LATEST TESTS

SCORING

ABOUT

https://djs-place.freemyip.com/

▶

118 tests running

16,186 tests in 24 hours

☐ Hide from Latest Tests

Provided "as is" without any warranty of any kind

Cloud Security Test

Email Security Test

Website Security Test

Mobile App Security Test

Dark Web Exposure Test

SSL Security Test

Summary of djs-place.freemyip.com Website Privacy Test

Your final score:

Tested on: Aug 5th, 2025 23:28:57 GMT-4

Server IP: 71.168.136.174

Location: United States

Input URL: https://djs-place.freemyip.com/

Tested URL: https://djs-place.freemyip.com/

A

B

C

F

A+

Refresh Test

Download Report

Website Policies

FOUND

Tracking Pixels

NO ISSUES FOUND

Cookies Analysis

NO ISSUES FOUND

XHR Requests Analysis

NO ISSUES FOUND

Third-Party Content

NO ISSUES FOUND

The website is accessible via HTTPS protocol, all web traffic between your browser and the website is encrypted. Test the encryption with our [SSL Security Test](#).

Information

Test Certificate

Quality Seal

ImmuniWeb®  
Community Edition

Website Privacy Test  
example.org

A+

Certificate Date

Verify Your Results: <https://www.immunoweb.com/privacy/>



ImmuniWeb® is a registered trademark of ImmuniWeb Inc. All rights reserved.

Register to Download

Aug 25

A+

ImmuniWeb®

WEBSITE PRIVACY TEST

example.org

Register to Install

## Website Policies of djs-place.freemyip.com

Website privacy policy (or privacy notice) is an essential legal document that governs how your personal data is used by website operator. Cookie consent banner allows website visitor to control use of third-party or tracking cookies. Both are required under the majority of privacy laws and regulations.

- Privacy Policy was found on the website

Good configuration
- Cookie Consent Banner was found on the website

Good configuration
- The copyright notice is up-to-date: © Copyright 2025 djs-place - All Rights Reserved

Good configuration

## Tracking Pixels

Pixel tracking, also known as pixel-based tracking or web beacon tracking, is an intrusive method of user tracking in online advertising used to monitor user habits, interests or interactions across different websites and social media platforms for targeted advertising. This technique usually inserts an invisible to human eye tracker (a pixel or web beacon) into a web page code.

- There are no tracking pixels found

Good configuration

## Cookies Analysis of djs-place.freemyip.com

Cookies are small files that websites save on your computer or mobile device to remember your preferences, such as website language or search history. However, cookies, especially third-party cookies, can be used for user tracking across different websites and collection of personal data for targeted advertising.

### First-Party Cookies

- There are no first-party cookies

Good configuration

### Third-Party Cookies

- There are no third-party cookies

Good configuration

## Local Storage Analysis

Local Storage is a persistent key-value based storage in a web browser, which allows storing various information required for better interaction with a website. Local Storage, however, can be misused to store persistent tracking information to trace and profile website visitors in a highly intrusive manner.

- No data has been set in the Local Storage by the website

Information

## XHR Requests Analysis of djs-place.freemyip.com

XHR (XMLHttpRequests) are HTTP requests made to external websites by the website you visit. While XHR technology is important for proper functioning of modern websites, it can also be misused to, among other things, send your personal data to external resources or to inject tracking technologies and monitor your behavior on the website.

- There are no external XHR requests found

Good configuration

## Third-Party Content Analysis

External web content hosted on remote web servers, such as JavaScript or CSS files, are indispensable components of modern websites. However, each time a remote content is loaded, the remote server collects user IP address and some other information that may potentially be misused to track user behavior and collect personal data.

### Iframes

An external iframe is an HTML element used to embed content from a different domain within a web page. It allows web developers to display external content, such as documents, videos, or entire web pages, within the context of their own site.

- There are no external iframes found

Good configuration

### External JavaScript Files

- There are no external JavaScript files found

Good configuration

### External CSS Files

- There are no external CSS files found

Good configuration

### External Images

- There are no external images found

Good configuration

### External Media Files

- There are no external videos found

Good configuration
- There are no external audios found

Good configuration

### External Fonts

- There are no external fonts found

Good configuration

## Web Forms of djs-place.freemyip.com

Web forms allow users to interact with websites in many useful ways. However, before submitting a web form with your personal data or other sensitive information, make sure that the website has a privacy policy that provides you with acceptable level of data protection.

- There are no web forms found submitting data to an external domain

Good configuration

## Need More? Upgrade to ImmuniWeb® AI Platform

Get remediation advice and ensure compliance with ImmuniWeb AI Platform:

API Security Scanning

▶

Web Security Scanning

▶

Cybersecurity Compliance Services

▶

FREE DEMO

ASK A QUESTION

## Why Choosing ImmuniWeb® AI Platform

Feel the difference. Get the results.

### Reduce Complexity

All-in-one platform for 20 synergized use cases

LEARN MORE

### Optimize Costs

All-in-one model & AI automation reduce costs by up to 90%

LEARN MORE

### Validate Compliance

Letter of conformity from law firm confirming your compliance

LEARN MORE



The award-winning ImmuniWeb® AI Platform helps over 1,000 companies from over 50 countries to test, secure and protect their web and mobile applications, APIs and microservices, cloud and networks, to prevent data breaches and reduce third-party risk, and to comply with regulatory requirements.

<b>Use Cases</b> <ul style="list-style-type: none"><li>API Penetration Testing</li><li>API Security Scanning</li><li>Attack Surface Management</li><li>Cloud Penetration Testing</li><li>Cloud Security Posture Management</li><li>Continuous Automated Red Teaming</li><li>Continuous Breach &amp; Attack Simulation</li><li>Continuous Penetration Testing</li><li>Continuous Threat Exposure Management</li><li>Cyber Threat Intelligence</li><li>Dark Web Monitoring</li><li>Mobile Penetration Testing</li><li>Mobile Security Scanning</li><li>Network Security Assessment</li><li>Penetration Testing-as-a-Service</li><li>Phishing Websites Takedown</li><li>Third-Party Risk Management</li><li>Threat-Led Penetration Testing</li><li>Web Penetration Testing</li><li>Web Security Scanning</li></ul>	<b>ImmuniWeb® AI Platform</b> <ul style="list-style-type: none"><li>ImmuniWeb® Discovery</li><li>ImmuniWeb® Neuron</li><li>ImmuniWeb® On-Demand</li><li>ImmuniWeb® MobileSuite</li><li>ImmuniWeb® Continuous</li><li>Customer Success</li><li>Integrations</li></ul> <b>Community Edition</b> <span>Free</span> <ul style="list-style-type: none"><li>Email Security Test</li><li>Website Security Test</li><li>Website Privacy Test</li><li>SSL Security Test</li><li>Mobile App Security Test</li><li>Dark Web Exposure Test</li><li>Third-Party Risk Test</li></ul> <b>Partners</b> <ul style="list-style-type: none"><li>Partner Program</li><li>Partner Directory</li><li>Partner Portal</li></ul>	<b>Resources</b> <ul style="list-style-type: none"><li>Cybersecurity Webinars</li><li>Cybercrime Investigations Weekly</li><li>Application Penetration Testing</li><li>Automated Penetration Testing</li><li>Attack Surface Management</li><li>Dark Web Monitoring</li><li>Ecommerce Security</li><li>CWE Knowledge Base</li><li>Security Advisories</li></ul> <b>OWASP Top 10</b> <ul style="list-style-type: none"><li>Broken Access Control</li><li>Cryptographic Failures</li><li>Injection</li><li>Insecure Design</li><li>Security Misconfiguration</li><li>Vulnerable and Outdated Components</li><li>Identification and Authentication Failures</li><li>Software and Data Integrity Failures</li><li>Security Logging and Monitoring Failures</li><li>Server-Side Request Forgery</li></ul>	<b>Compliance Services</b> <ul style="list-style-type: none"><li> EU &amp; UK GDPR</li><li> Singapore PDPA</li><li> Hong Kong PDPO</li><li> South Africa POPIA</li><li> Brazil LGPD</li><li> HIPAA / HITECH</li><li> NIST SP 800, FISMA, CMMC</li><li> New York SHIELD, NYDFS</li><li> California CCPA, CPRA</li><li> ISO 27001 / ISO 27002</li><li> Singapore MAS</li><li> PCI DSS</li></ul>
---	---	---	---