



网站隐私与跨境数据流合规检测报告

https://***



国内网站



深度检测 (含大模型分析)



耗时 225.74秒



电子商务/零售

⚠ 不合规 — 8 项风险



3

跨境数据流合规风险

检测到数据流向海外

国内网站集成 6 个海外SDK，存在数...

检测到 3 个海外埋点，存在数据出境



5

网站隐私合规风险

缺少Cookie政策链接

Cookie安全标志配置建议 (2 项)

检测到多项高风险个人信息采集 (7项)

隐私政策未充分披露实际采集的个人信...



跨境数据流合规风险



网站数据流向可视化

3 个数据出境目标国

美国 53 日本 24 欧洲 18



HIGH 检测到数据流向海外

国内网站流量流向以下海外地区: 美国, 日本, 欧洲

根据《个人信息保护法》第三十八条, 向境外提供个人信息应通过安全评估或标准合同。

⚠️ 风险影响: 个人数据一旦出境, 将脱离中国法律直接保护, 面临被境外机构滥用、泄露的风险。企业可能在不知情的情况下违反数据出境安全评估要求, 面临最高五千万或年营业额5%的罚款。

📖 法规要求原文

中国《个人信息保护法》

《个人信息保护法》第三十八条: 确需向境外提供个人信息的, 应当具备下列条件之一:

- (一) 通过国家网信部门组织的安全评估;
- (二) 经专业机构进行个人信息保护认证;
- (三) 按照标准合同与境外接收方订立合同。

《数据出境安全评估办法》第四条: 处理100万人以上个人信息或累计向境外提供10万人个人信息的数据处理者, 应当申报数据出境安全评估。

CRITICAL 国内网站集成 6 个海外SDK, 存在数据出境风险

国内网站 https://*** 集成了 6 个海外SDK (Microsoft Clarity、Google Analytics 等), 所属公司为 Hotjar Ltd、Microsoft Corporation 等5家公司。这些SDK可能将用户浏览数据、设备信息等传输至境外服务器, 需通过数据出境安全评估后方可传输。查看完整SDK清单与公司详情请升级正式版。

《个人信息保护法》第38条: 向境外提供个人信息须通过安全评估或认证。《数据出境安全评估办法》: 数据处理者向境外提供数据前应申报安全评估。

⚠️ 风险影响：海外SDK在运行时会自动将用户数据（设备信息、IP地址、行为数据等）发送至境外服务器。企业作为数据控制者，对SDK的数据处理行为负有监督义务，未履行者承担连带责任。

法规要求原文

中国《个人信息保护法》

《个人信息保护法》第二十一条：委托处理个人信息的，应当与受托方约定处理目的、方式、种类、保护措施及双方权利义务，并对受托方进行监督。

第二十三条：向其他个人信息处理者提供个人信息的，应当告知接收方信息并取得单独同意。

涉及的海外SDK：[Microsoft Clarity](#) [Google Analytics](#) 等6个

MEDIUM 检测到 3 个海外埋点，存在数据出境

网站集成了 3 个向境外发送数据的埋点（Facebook Pixel 事件上报、Microsoft Clarity 数据收集、Google Analytics 数据收集等），用户行为数据被实时发送至境外服务器。建议评估每个埋点的必要性并完成数据出境合规手续。

《个人信息保护法》第38-40条、《数据出境安全评估办法》

⚠️ 风险影响：埋点数据虽然看似零散，但聚合后可还原用户完整行为画像，同样构成个人信息出境。

法规要求原文

中国《个人信息保护法》

《个人信息保护法》第二十一条：委托处理个人信息的，应当与受托方约定处理目的、方式、种类、保护措施及双方权利义务，并对受托方进行监督。

第二十三条：向其他个人信息处理者提供个人信息的，应当告知接收方信息并取得单独同意。

第三方SDK & 埋点

SDK共 8 个：[海外 6](#) / [国内 2](#) | 埋点共 6 个：[跨境 3](#) / [国内 2](#)

SDK分析

SDK名称	所属公司	数据流向	分类
-------	------	------	----

Microsoft Clarity	Microsoft Corporation	美国 △数据出境风险	用户行为分析
-------------------	-----------------------	-------------------------	--------

神策数据 (Sensors Data)	神策网络科技 (北京) 有限公司	中国	数据分析
---------------------	------------------	----	------

埋点分析

埋点名称	目标服务器	数据流向	请求次数
------	-------	------	------

百度统计上报	hm.baidu.com	中国	2
--------	--------------	----	---

Google Analytics 数据收集	www.google-analytics.com	美国 △数据出境风险	6
-----------------------	--------------------------	-------------------------	---

 还有 6 个SDK详情需付费查看 (当前展示20%概览)
升级正式版解锁全部SDK完整分析与证据代码

 还有 4 个埋点详情需付费查看 (当前展示20%概览)
升级正式版解锁全部埋点目标服务器、数据流向与请求次数详情

流量分析

总请求: 410 | 第一方: 188 | 第三方: 222

流量流向: 中国:121 美国:53 日本:24 欧洲:18 Unknown:6



 域名详情与IP地址需付费解锁
正式版可查看第三方域名列表、IP地址、请求次数详情

网站隐私合规风险

个人信息采集

检测到表单采集 13 项 + SDK/埋点采集 35 项 = 合计 48 项个人信息 (12 种类型 + 35 种 SDK采集)

账号凭证

CRITICAL

分类: credential · 检测到 2 处

姓名

MEDIUM

分类: PII · 检测到 1 处

联系方式

HIGH

分类: contact · 检测到 1 处

 还有 9 类个人信息采集的完整证据需付费查看（当前展示20%概览）

正式版可查看全部类型及每项的检测证据（表单字段名、脚本URL、代码片段），方便研发定位整改。

 请联系管理员升级套餐

第三方SDK/埋点采集的个人信息:

页面浏览记录

浏览器信息

浏览器指纹

等 35 类 · 完整清单需付费

HIGH

缺少Cookie政策链接 AI增强

网站使用了 36 个Cookie（包含营销/分析类Cookie），但首页底部未找到Cookie政策相关的可阅读超链接。

《个人信息保护法》要求涉及Cookie收集个人信息时，需在隐私政策中明确告知Cookie的收集目的、方式、类型和用途。

 **风险影响：**用户无法了解网站使用了哪些Cookie及其用途，特别是涉及用户行为追踪的营销和分析类Cookie。监管部门对Cookie合规日益重视，缺少Cookie政策是常见处罚项。

法规要求原文

中国《个人信息保护法》

《个人信息保护法》第十七条：通过Cookie等方式收集个人信息的，应当在隐私政策中明确告知Cookie的收集目的、方式、类型和用途。第二十四条规定利用个人信息进行自动化决策的，应当保证决策的透明度和结果公平。

 **AI深度分析补充：** 首页未检测到Cookie政策链接，全站遍历也未发现Cookie政策页面，用户无法清晰了解Cookie的具体用途和管理方式。... [完整分析需付费]

MEDIUM

Cookie安全标志配置建议 (2 项)

AI增强

以下 2 项Cookie安全配置可优化：23 个Cookie未设置 Secure 标志；33 个Cookie未设置 HttpOnly 标志。共涉及 33 个Cookie。

⚠️ 风险影响：Cookie安全标志缺失可能导致用户会话被劫持、Cookie被恶意脚本窃取、跨站请求伪造等安全风险，间接导致用户个人信息泄露。监管检查中对Cookie安全性也日益关注。

📖 法规要求原文

中国《个人信息保护法》

《个人信息保护法》第九条：个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。第五十一条要求采取加密、去标识化等安全技术措施。

💡 AI深度分析补充: 部分Cookie可能未配置Secure、HttpOnly、SameSite等安全属性，存在被窃取或在跨站请求中被滥用的风险。... [完整分析需付费]

▶ 展开详情 (2项)

HIGH

检测到多项高风险个人信息采集 (7项)

网站采集了 12 种个人信息类型，其中高风险项包括：账号凭证、联系方式、身份证号码、地址信息、银行账号。根据《个人信息保护法》的数据最小化原则，不应超范围收集与业务无关的个人信息。

《个人信息保护法》第6条：收集个人信息应当限于实现处理目的的最小范围，不得过度收集。

⚠️ 风险影响：过度收集个人信息是最常见的违规行为之一，监管机构对此类违规的打击力度持续加大。企业可能面临责令整改、罚款等处罚，严重者可被吊销营业执照。

📖 法规要求原文

中国《个人信息保护法》

《个人信息保护法》第六条：收集个人信息应当限于实现处理目的的最小范围，不得过度收集个人信息。

第二十八条：敏感个人信息包括生物识别、医疗健康、金融账户、行踪轨迹等，处理敏感个人信息应当取得个人的单独同意。

HIGH

隐私政策未充分披露实际采集的个人信息（1 项未披露）

AI增强

网站通过表单实际采集了以下个人信息，但在隐私政策中未找到对应的披露声明：账号凭证。根据《个人信息保护法》，处理个人信息前应以显著方式告知用户处理目的、方式和种类。未在隐私政策中披露的数据采集行为构成违规，用户无法充分了解其个人信息被如何使用。

《个人信息保护法》第17条：个人信息处理者应以显著方式、清晰易懂的语言告知个人信息处理目的、方式、种类及保存期限。

⚠️ 风险影响：未在隐私政策中披露的数据采集行为属于违规收集个人信息，监管机构可责令整改、处以罚款，情节严重的可被吊销营业执照。

📖 法规要求原文

中国《个人信息保护法》

《个人信息保护法》第六条：收集个人信息应当限于实现处理目的的最小范围，不得过度收集个人信息。

第二十八条：敏感个人信息包括生物识别、医疗健康、金融账户、行踪轨迹等，处理敏感个人信息应当取得个人的单独同意。

💡 AI深度分析补充: 页面实测表单实际采集账号凭证，但隐私政策中未明确列明账号凭证（如用户名、密码）的采集目的、处理方式和保存期限，违反《个人信息保护法》关于告知处理规则的要求。 隐... [\[完整分析需付费\]](#)

MEDIUM

存在大量未分类Cookie

AI发现

36个Cookie中有18个未分类，无法判断其用途是否涉及追踪、画像或广告，可能包含未声明的数据处理行为。

🍪 Cookie分析

共 36 个Cookie | 隐私风险Cookie: 17 个

分类: 必要Cookie — 网站正常运行所必需，通常无需用户同意:1 未分类Cookie — 未能自动分类的Cookie:18 营销Cookie — 追踪用户以投放定向广告:4 分析/统计Cookie — 收集访问统计数据，帮助改进网站:13

名称	域名	Same Site	Secure	HttpOnly	分类
_gcl_au	.shoplazz a.cn	Lax	✗	✗	营销Cookie — 追踪用户以投放定向广告
HMACCOUNT_BFESS	.hm.baid u.com	None	✓	✗	分析/统计Cookie — 收集访问统计数据，帮助改进网站

名称	域名	Same Site	Secure	HttpOnly	分类
Hm_lvt_8ab5714d3af45fabd9	.shoplazz a.cn	Lax	✗	✗	分析/统计Cookie — 收集访问统计数据，帮助改进网站
Hm_lpvt_8ab5714d3af45fabd	.shoplazz a.cn	Lax	✗	✗	分析/统计Cookie — 收集访问统计数据，帮助改进网站
HMACCOUNT	.shoplazz a.cn	Lax	✗	✗	分析/统计Cookie — 收集访问统计数据，帮助改进网站

 还有 31 个Cookie的完整详情需付费查看（当前展示约20%）

正式版可查看全部Cookie名称、域名、安全标志及分类详情

 请联系管理员升级套餐

一键生成合规政策

基于本次检测结果，AI自动生成针对性隐私政策、Cookie政策

 一键生成政策为付费功能

基于检测结果自动生成针对性隐私政策与Cookie政策，仅正式版可用

 请联系管理员升级套餐

 修订

对生成的政策内容不满意？点击修订，AI将根据您的要求修改政策文本

大模型深度分析

 大模型深度分析为付费功能

综合风险等级评估、Cookie合规分析、SDK风险详情、数据跨境评估、改进建议等AI深度分析内容仅对付费用户开放。基础检测的风险情报对所有用户可见。

 请联系管理员升级套餐

本报告为自动化检测产出的自查材料，检测结果仅供企业内部排查风险使用；如对外提交，建议结合人工核验。

