What eu-agency-b.example does before the visitor says yes

Page: https://eu-agency-b.example/ · scanned 2026-11-01 15:09 UTC · fresh browser, no clicks, 8 s wait

> **No consent-requiring cookie was set before consent, but 2 third part(ies) received the visitor's request or IP before any choice (Meta Pixel, X (Twitter) pixel).**
>
> Consent banner detected: **OneTrust**. Google Consent Mode default: **not set in dataLayer**.
>
> After we clicked the banner's reject button (`selector #onetrust-reject-all-handler`) and reloaded: **1 consent-requiring vendor(s) still ran (X (Twitter) pixel).** A reject that does not stop tracking is the most serious finding here.

2 cookies before consent	**1** third-party cookies
10 third-party hosts contacted	**0** consent-requiring vendors

1. Before consent (no interaction)

Severity	Vendor	What it is	Evidence
MEDIUM	Meta Pixel	Advertising / retargeting	2 request(s) to connect.facebook.net *Only the vendor's script was downloaded: no tracking hit and no cookie was seen in this scan. The vendor still received the visitor's IP address, and the tag may be waiting in a consent-hold mode; confirm it stays idle until consent.*
MEDIUM			

	X (Twitter) pixel	Advertising / retargeting	1 request(s) to static.ads-twitter.com *Only the vendor's script was downloaded: no tracking hit and no cookie was seen in this scan. The vendor still received the visitor's IP address, and the tag may be waiting in a consent-hold mode; confirm it stays idle until consent.*
INFO	Adobe Experience Platform Tags (Launch)	Tag manager (loads other tags)	4 request(s) to assets.adobedtm.com
INFO	Sentry error monitoring	Functional third party	1 request(s) to browser.sentry-cdn.com
INFO	Wistia video	Functional third party	14 request(s) to distillery.wistia.com, embed-ssl.wistia.com, fast.wistia.com, fast.wistia.net
OK	Consent banner (stores the choice)	Consent banner	cookies: OptanonConsent
OK	Load balancer / bot protection	Likely strictly necessary	cookies: __cf_bm
OK	OneTrust CookiePro	Consent banner	11 request(s) to cookie-cdn.cookiepro.com

2. After rejecting, on the next page load

Severity	Vendor	What it is	Evidence
HIGH	X (Twitter) pixel	Advertising / retargeting	2 request(s) to analytics.twitter.com, static.ads-twitter.com
MEDIUM	Meta Pixel	Advertising / retargeting	2 request(s) to connect.facebook.net *Only the vendor's script was downloaded: no tracking hit and no cookie was seen in this scan. The vendor still received the visitor's IP address, and the tag may be waiting in a consent-hold mode; confirm it stays idle until consent.*
MEDIUM	X (Twitter)	Advertising / retargeting	cookies: guest_id (left over), muc_ads (left over), personalization_id (left over) *Cookies set before consent were still in the browser after the reject and were not deleted*

			or renewed. Nothing new was sent to the vendor on this load, but the identifiers remain.
INFO	Adobe Experience Platform Tags (Launch)	Tag manager (loads other tags)	4 request(s) to assets.adobedtm.com
INFO	Sentry error monitoring	Functional third party	1 request(s) to browser.sentry-cdn.com
INFO	Wistia video	Functional third party	14 request(s) to distillery.wistia.com, embed-ssl.wistia.com, fast.wistia.com, fast.wistia.net
OK	Consent banner (stores the choice)	Consent banner	cookies: OptanonAlertBoxClosed (left over), OptanonConsent
OK	Load balancer / bot protection	Likely strictly necessary	cookies: __cf_bm (left over)
OK	OneTrust CookiePro	Consent banner	12 request(s) to cookie-cdn.cookiepro.com

How to fix

1. **Meta Pixel.** Do not call fbq('init') before consent, or call fbq('consent','revoke') before init and fbq('consent','grant') from the CMP's accept callback. In GTM: marketing consent trigger only.
2. **X (Twitter) pixel.** Advertising and retargeting tags need prior opt-in consent in the EU and UK. Move them behind the marketing category of the consent banner.
3. **X (Twitter).** Advertising and retargeting tags need prior opt-in consent in the EU and UK. Move them behind the marketing category of the consent banner.

General rule: set every tag's consent requirement in the tag manager, load the banner script first, and set Consent Mode defaults to denied before any Google tag. Re-scan after each change.

Cookies we could not classify

None.

localStorage keys written before consent

`lastExternalReferrer, lastExternalReferrerTime`

Method and limits

- One page, loaded in a fresh Chromium profile with no stored cookies. Before-consent figures cover the first 8 seconds with no click, scroll or mouse movement. Tags that wait for scrolling or a second page view are not seen.
- Vantage point: this scan ran from an IP outside the EU/UK. Banners that geo-target (common with Cookiebot, OneTrust, Usercentrics) can behave differently for an EU visitor; a paid report is run from an EU vantage point or says it was not.
- The browser identifies itself as `Mozilla/5.0 (compatible; KeencrestConsentAudit/1.0; +https://keencrest-guides.web.app/cookie-consent-audit/)`. Sites that treat automated visitors differently may load fewer tags than they do for people.
- Classification uses Keencrest's tracker list (built from each vendor's own cookie documentation; sources in the JSON). A vendor not on the list shows up under "unclassified", never silently dropped.
- Severity reflects the general EU/UK rule (ePrivacy Directive Art. 5(3), UK PECR reg. 6, CJEU Planet49): storing or reading anything on the device that is not strictly necessary needs prior opt-in consent. Local rules differ (CNIL exempts some configured analytics).
- **This is a technical observation, not legal advice and not a compliance certificate.** It cannot see the banner's wording, the privacy notice, server-side tracking or what happens after a visitor accepts.

Keencrest is an AI-run business owned by Alex Lin; this report was produced by automation.