dpoffice.net - audit report

dpoffice.net: summary of findings

This report sets out the findings of a forensic privacy audit of dpoffice.net. 3 of its pages were captured from Malta, in the European Union, on 2 November 2026, in a clean browser that did nothing at all: nothing was clicked, nothing was typed and no consent banner was answered. Every event in this report therefore took place before any consent was given.

dpoffice.net is DPOffice, a synthetic test site operated by That Privacy Guy! to demonstrate WebSentinel (section 3.1). It is not one of the 100 websites in the study; its figures are shown against the study's results for context.

Measure	dpoffice.net
Events engaging the law	**870**
Tier 1 - interception, exfiltration, high-entropy fingerprinting	39
Tier 2 - storage on the device and reading device characteristics	476
Tier 3 - protocol mechanisms and passive reads used for tracking	355
Events rated high or critical	110
Cookies set before consent	17, of which 7 on other companies' domains
Servers contacted / of which third-party	15 / 14
Servers on networks registered outside the EEA	12

Key points

- DPOffice is our own synthetic test site, built to deploy every privacy, security and consent-bypass signal WebSentinel detects. Its tracker IDs are fake, but every network call it makes is real, so the capture shows what an ordinary visitor's browser actually does.
- Before any consent, the homepage set cookies on doubleclick.net, linkedin.com, tiktok.com and hubspot.com, and Meta's _fbp identifier on dpoffice.net itself.
- analytics.dpoffice.net is a DNS alias (CNAME) of track.hubspot.com, so HubSpot's tracking server was presented to the browser as DPOffice's own subdomain.
- The site produced 39 tier 1 events - interception, exfiltration and high-entropy fingerprinting - and 110 events rated high or critical, all before any consent was given.

2. Scope

Pages audited, at the address reached after any redirects:

- **Homepage:** https://dpoffice.net/
- **Privacy notice:** https://dpoffice.net/privacy.html
- **Cookie notice:** https://dpoffice.net/cookie-policy.html
- DPOffice is a synthetic test site operated by That Privacy Guy! for WebSentinel development and demonstration. It is not one of the 100 websites in the study; its figures are compared with the study's 100 sites for context only.

3.1 Site selection

DPOffice is a realistic-looking business-to-business software website built by That Privacy Guy! as a test site for WebSentinel. It deploys real third-party tags with fake account identifiers, CNAME-cloaked trackers, fingerprinting, sensor probes and consent-bypass dark patterns, so that every capability of the engine can be exercised and demonstrated - the network calls it makes are real.

Eleven of its pages were captured on 2 November 2026. This report covers the three pages the study audits on every website - the homepage, the privacy notice and the cookie notice - using the same methodology as the study of the 100 most visited English-language content websites. The pages audited are listed in section 2.

3.2 The capture instrument

The capture was made with WebSentinel, a forensic website audit tool for data protection, privacy and security compliance work. It runs as an extension inside an ordinary, visible Google Chrome browser and records what a website does in that browser, at the point where the website's code runs. It observes and records; it does not change what a website is able to do.

WebSentinel records evidence from several independent layers of the browser at once:

- **Instrumented browser interfaces.** Every call a script makes to the interfaces websites use to interact with the device - reading screen, time zone or graphics characteristics, storing data, listening to the mouse and keyboard, sending data to servers - is recorded as an event.
- **The network layer.** Every network request the browser makes, from the browser's own request log and from the Chrome DevTools Protocol, which adds the code that initiated each request, together with a full HTTP archive of requests and responses.
- **Storage state.** The contents of cookies, local storage and session storage as they change.
- **Scripts.** Every script loaded by the page, with its address, a hash of its content, its size and where it was inserted; scripts loaded by other scripts from a different origin are recorded with the script that loaded them.
- **Page state.** A copy of the rendered page, full-page screenshots, the text of the legal notices the page links to, and an inventory of software libraries.

Attribution. Every fingerprinting, storage and tracking event carries the full call stack at the moment it happened - the script, the function, and the line and column in the code - so every behaviour can be traced to the code, and the company, that caused it.

Severity. Each event is assigned a severity (info, low, medium, high or critical) by the engine's rules for the technique. Severity describes how intrusive a technique is; it does not decide whether an event breaches the law (section 4.0).

Version. dpoffice.net was captured with WebSentinel engine 2.1.5.

3.3 Capture protocol

- **Location.** The capture was made from Malta, in the European Union, through a Maltese broadband connection (GO p.l.c.), whose exit address was checked before the capture. The website saw an ordinary visitor from the EU.
- **Browser.** A visible Google Chrome browser (version 153), 1920 by 1080 pixels, with background Google services switched off - background networking, component updates, synchronisation and the download of on-device AI models - so that the only traffic captured was caused by the website.
- **No interaction, no consent.** The browser opened each page and did nothing else. Nothing was clicked, nothing was typed, no banner was answered. Every event took place before any consent was given - the position of every person who arrives on a website.
- **A clean profile.** Before the website was captured, the browser profile was reset to a fixed, verified baseline with no cookies, no website storage, no history and no cache, and the capture software confirmed that no cookies were present before the first page was opened. Within the website, storage was kept from page to page in the order the eleven pages were captured, beginning with the homepage; the privacy notice was the seventh page and the cookie notice the eighth. A snapshot of the whole profile was committed to version control after every page.
- **One page at a time.** Only one page was open at any time, and the capture software confirmed that before each page.
- **Dwell time.** Each page was kept open for five minutes, capturing activity that starts after loading - timers, delayed scripts, periodic beacons and lazily loaded advertising.
- **Acceptance.** The capture of a website was accepted only when, after the browser had closed and all records had arrived, there was exactly one recorded session for each page, every session corresponded to one of the website's pages, and every session's record chain verified as complete and unbroken (section 3.4).

3.4 Evidence integrity

The evidence was captured so that anyone given it can verify that it is complete and has not been altered since capture.

1. **Hash-chained records.** Evidence is sent in a sequence of records while each page is open; each record carries a SHA-256 hash of its content and the hash of the record before it. Removing, reordering or altering any record breaks the chain detectably.
2. **Hardware-backed signatures.** Each record is signed on receipt with ECDSA on the P-256 curve with SHA-256, using a key held by a Secure Enclave. Each signature can be checked against the published public key.
3. **Trusted timestamps.** Each record's hash is timestamped by an independent RFC 3161 time-stamping authority, FreeTSA (freetsa.org).
4. **Bitcoin anchoring.** Each record's hash is submitted to two independent OpenTimestamps calendars (a.pool.opentimestamps.org and alice.btc.calendar.opentimestamps.org), which commit it to the Bitcoin blockchain.
5. **Chain verification.** Every session's chain was verified after capture; only complete, unbroken chains with no flags were accepted.

All of dpoffice.net's sessions passed on the first capture.

The sessions and records for dpoffice.net are listed in section 5.

3.5 Limitations

- **One location.** The capture was made from Malta and shows what a visitor in the EU receives. Claims under the California Invasion of Privacy Act rest on that evidence: a website may be configured differently for Californian visitors, but such configuration normally reaches only the consent platform and the tag manager, and dpoffice.net produced 110 events rated high or critical before any consent was given.
- **One visit, no interaction.** Each page was opened once, by a first-time visitor who did nothing. Interaction, returning visits and consent decisions may produce different activity; the figures show what happens before any choice is made.
- **Desktop Chrome, five minutes per page.** Other browsers and mobile devices may receive different code; activity starting after five minutes is not captured.
- **Built-in AI interfaces.** The version of WebSentinel used did not record calls to the browser's built-in AI interfaces. The full source of every script delivered to the pages was searched for code using them instead (section 4B); that shows code delivered, not code that ran.
- **Events, not intent.** WebSentinel records what code did, not why. Where this report describes the purpose of a technique, it describes what the technique is capable of and how it is generally used.
- **Exclusions.** Event types the engine derives by matching addresses against lists of known tracking domains are excluded from every count, as is the engine's record of scripts inserted into the page (which includes the website's own inline code); scripts loaded by other scripts are counted instead.
- **Cookies sent to aliased subdomains.** The HTTP archive records request headers before the browser adds its cookies, so it does not show which cookies were sent with each request.
- **Notice text.** Where a notice page loads its text after the page or holds it in collapsed sections, the captured page may not contain the full text; this is stated where it affects a finding.

4.00 Who is responsible: joint controllership

Much of the activity in this report was carried out by code that the website operator did not write: advertising libraries, analytics tags, consent tools, video players, fonts, bot detection. A common response from website operators is that this is someone else's code and someone else's responsibility.

The Court of Justice of the European Union has rejected that position.

The case law

In **Fashion ID** (C-40/17, judgment of 29 July 2019, ECLI:EU:C:2019:629), a retailer embedded Facebook's "Like" button on its website. The button caused visitors' browsers to send personal data to Facebook as soon as the page loaded, whether or not the visitor was a Facebook user and whether or not they clicked the button. The Court held that the website operator is a **joint controller** with the third party for the collection of the data and its transmission to the third party, because by embedding the code it determines, together with the third party, the purposes and means of that processing. It does not need to have access to the data to be a controller.

Fashion ID built on two earlier Grand Chamber judgments: **Wirtschaftsakademie** (C-210/16, 5 June 2018, ECLI:EU:C:2018:388), in which the administrator of a Facebook fan page was held to be a joint controller with Facebook for the processing of visitors' data, and **Jehovan todistajat** (C-25/17, 10 July 2018, ECLI:EU:C:2018:551), which confirmed that joint control does not require each party to have access to the data or an equal share of responsibility.

What it means for this website

Every third-party script that the website loaded was loaded because the website operator chose to put it, or the code that loads it, on the page. For every collection of data by that script, and every transmission of data from the visitor's device to its operator, **the website operator is a joint controller** under Article 26 GDPR, alongside the company that supplied the script.

That has three consequences for the findings that follow:

1. **The website operator answers for every event on its pages**, including those carried out by third-party code, at least for the collection and transmission of the data.
2. **The obligations of Articles 5, 6, 7, 12 to 14, 25 and 32 GDPR rest on the website operator** for that processing - including the obligation to obtain valid consent before it takes place, and to tell visitors about it.
3. **Sideloading does not move responsibility elsewhere.** Where a script the operator loaded goes on to load further scripts from other companies (section 4.3), those scripts are on the page because of the operator's choice.

Article 5(3) of the ePrivacy Directive points the same way: it prohibits storing information on, or gaining access to information in, the user's device without consent, whoever's code does it. The website is the means by which that code reaches the device.

Third parties on dpoffice.net's pages

Third-party servers contacted by dpoffice.net's audited pages before consent (14):

Server	Operator of the network	Pages
analytics-ipv6.tiktokw.us	AKAMAI-ASN1	homepage
analytics.tiktok.com	AKAMAI-ASN1	homepage
cdn.jsdelivr.net	FASTLY	homepage
connect.facebook.net	FACEBOOK	homepage

Server	Operator of the network	Pages
fonts.gstatic.com	GOOGLE	homepage
px.ads.linkedin.com	CLOUDFLARENET	homepage
region1.google-analytics.com	GOOGLE	homepage, privacy notice
script.hotjar.com	AMAZON-02	homepage
securepubads.g.doubleclick.net	GOOGLE	homepage
snap.licdn.com	AKAMAI-ASN1	homepage
static.hotjar.com	AMAZON-02	homepage
track.hubspot.com	CLOUDFLARENET	homepage
www.clarity.ms	MICROSOFT-CORP-MSN-AS-BLOCK	homepage
www.google-analytics.com	GOOGLE	homepage, privacy notice

4.0 How to read this report

Every event in this report happened **before any consent was given**. The browser opened each page and did nothing else (section 3.3).

This report is organised by the kind of thing the website did to the visitor's device. Each section explains what the technique is and why it matters, sets out what we found, and maps it to the provisions of EU and California law it engages.

How we count

Every event that engages a legal provision is counted. Each time a script reads a characteristic of the device, stores an identifier on it or sends data off it, that is a separate access to the visitor's terminal equipment and a separate act of processing - and a separate breach of the law. A script that reads the screen width fifty times has accessed the device fifty times, and every one of those accesses is counted.

	Events
dpoffice.net	**870**
Tier 1 - interception, exfiltration and high-entropy fingerprinting	39
Tier 2 - storage on the device and reading device characteristics	476
Tier 3 - protocol mechanisms and passive reads that can be used for tracking	355

By page: 595 on the homepage, 164 on the privacy notice, 95 on the cookie notice, plus 16 sideloaded script loads (16 on the homepage).

Tiers

The tiers express how serious a technique is. They do not decide whether it counts: every tier counts. Tier 3 covers mechanisms such as ETags and HSTS, which have legitimate functions and are also used to track people across visits; the reasons they still engage the law are set out in section 4.10.

What is not counted

Three kinds of event are excluded from every count:

- the detection of consent management platforms and banners, which we use only to show that a consent mechanism was present while everything else happened;
- two event types the capture engine derives by matching addresses against lists of known tracking domains - every figure in this report rests on observed behaviour, not on lists;
- the insertion of scripts into the page, which includes each site's own inline code; scripts loaded by other scripts from a different origin are counted instead (section 4.3).

The legal provisions

Short form	Provision
ePD 5(1)	Directive 2002/58/EC, Article 5(1): confidentiality of communications - no listening, tapping, storage or other interception or surveillance without consent
ePD 5(3)	Directive 2002/58/EC, Article 5(3): storing information, or gaining access to information already stored, in the terminal equipment of a user, only with consent unless strictly necessary for a service the user explicitly requested
GDPR 5	Regulation (EU) 2016/679, Article 5(1): lawfulness, fairness and transparency; purpose limitation; data minimisation
GDPR 6	Article 6(1): lawful basis

Short form	Provision
GDPR 7	Article 7: conditions for consent - consent must be given before processing and be freely given, specific, informed and unambiguous
GDPR 9	Article 9: special categories of personal data
GDPR 12-14	Articles 12 to 14: transparency and information duties
GDPR 22	Article 22: decisions based solely on automated processing producing legal or similarly significant effects
GDPR 25	Article 25: data protection by design and by default
GDPR 26	Article 26: joint controllers
GDPR 32	Article 32: security of processing
GDPR Chapter V	Articles 44 to 50: transfers to third countries
Dir 2013/40	Directive 2013/40/EU on attacks against information systems: Article 3 illegal access, Article 4 illegal system interference, Article 5 illegal data interference, Article 6 illegal interception, as transposed in each Member State (for example Article 337C of the Maltese Criminal Code)
Budapest	Council of Europe Convention on Cybercrime: Article 2 illegal access, Article 3 illegal interception, Article 4 data interference, Article 5 system interference
CIPA 631	California Penal Code section 631: reading or attempting to learn the contents of a communication in transit without the consent of all parties
CIPA 638.51	California Penal Code section 638.51: pen registers and trap and trace devices - capturing dialling, routing, addressing or signalling information
PC 502	California Penal Code section 502: knowingly accessing a computer, computer system or data without permission

Article 5(3) of the ePrivacy Directive applies whether or not the information concerned is personal data (CJEU, Planet49, C-673/17, ECLI:EU:C:2019:801). Where it is, the GDPR applies as well.

Where this report says a provision is **engaged**, it means the observed conduct falls within the provision's scope. Whether any exemption could apply - such as the strict necessity exemption in Article 5(3) - is addressed in each section. None of the conduct was preceded by consent, because none was given.

4.1 Device fingerprinting

What it is

Fingerprinting identifies a device by reading its characteristics instead of storing an identifier on it. Each characteristic on its own - the screen size, the time zone, the number of processor cores, the list of graphics extensions, the way the device draws a hidden image - says little. Read together, they are distinctive enough to recognise the same device again, across websites and across visits, without a cookie and without the person being able to see it, block it or delete it.

Fingerprinting works by script: code on the page asks the browser for information about the device and sends the results to a server. Every one of those requests is a script gaining access to information stored in the visitor's device.

We group the techniques by how much they reveal:

- **High-entropy techniques (Tier 1)** read characteristics that vary widely between devices and are used specifically to tell devices apart: drawing to a hidden canvas and reading the pixels back, querying the graphics hardware through WebGL and WebGPU, generating audio signals, measuring installed fonts, setting up WebRTC connections that expose network addresses, reading the battery state, the keyboard layout, the installed speech voices, connected media devices and motion sensors, and probing for browser extensions.
- **Device characteristics (Tier 2)** are the standard components of a fingerprint: user agent, platform, language, screen dimensions and colour depth, time zone, processor cores, device memory, network connection type and the browser's client hints.
- **Environmental reads (Tier 3)** report the state of the page and the device - whether the page is visible or in focus, layout and timing measurements. Individually they carry little identifying information; combined with the above, they add to a fingerprint and they are used to measure attention.

What we found on dpoffice.net

Measure	Figure
Events	**119**
Where	98 on the homepage, 16 on the privacy notice, 5 on the cookie notice

Techniques

Technique	Events
navigator.userAgent	17
visibility.listen.pagehide	9
visibility.listen.visibilitychange	8
screen.width	4
screen.height	4
clientHints.getHighEntropyValues	4
visibility.listen.pageshow	4
sharedArrayBuffer.available	3
visibility.listen.beforeunload	3
focus.hasFocus	3
visibility.listen.focus	3

Technique	Events
visibility.listen.blur	3
document.visibilityState	3
webgl.getParameter	2
navigator.cookieEnabled	2
navigator.doNotTrack	2
navigator.language	2
canvas.toDataURL	1
webgl.getExtension	1
navigator.platform	1

Scripts and servers responsible

Script or server	Events
dpoffice.net	53
www.googletagmanager.com	24
snap.licdn.com	9
securepubads.g.doubleclick.net	9
analytics.tiktok.com	9
connect.facebook.net	6
script.hotjar.com	5
unattributed	3
static.hotjar.com	1

"server:" denotes an event caused by a server response with no script involved; "unattributed" denotes an event with no usable call stack.

The law

ePrivacy Directive, Article 5(3). Reading a characteristic of the device is gaining access to information stored in the terminal equipment. It requires consent unless it is strictly necessary to provide a service the visitor explicitly requested. Reading the graphics hardware, the battery, the installed voices or the keyboard layout of someone who has asked to read a news article is not necessary to show them that article. The provision applies whether or not the information is personal data (Planet49).

Bot detection deserves a specific word, because the largest single source of fingerprinting was a bot challenge. A security purpose does not remove the need for consent. The exemption covers only what is strictly necessary for the service the visitor requested, and only to the extent necessary. Covert collection of dozens of device characteristics from every visitor, on every page including the privacy notice, is difficult to describe as strictly necessary for reading a page.

GDPR, Articles 5, 6, 7 and 25. A fingerprint is a means of singling out a device, and through it a person; it is personal data. Collecting it before consent has no lawful basis where consent is required, fails the conditions of Article 7 because consent was never asked for, collects far more than any purpose requires (Article 5(1)(c)), and is the opposite of data protection by design and by default (Article 25). Because fingerprinting is invisible and cannot be cleared by the user, it also fails the fairness and transparency principle in Article 5(1)(a).

Criminal law. Accessing a computer system without right is illegal access under Article 3 of Directive 2013/40/EU and Article 2 of the Budapest Convention, as transposed in each Member State. Scripts that interrogate the hardware, software and configuration of a visitor's device, without the visitor's knowledge or consent, are accessing that system without right. In California, knowingly accessing a computer or its data without permission engages Penal Code section 502.

Section 4B sets out how the availability of the browser's built-in AI interfaces was itself used as one input to a fingerprint.

4.2 CNAME cloaking

What it is

Browsers treat a website's own subdomains as part of the website. A request to `metrics.example.com` from a page on `example.com` is a first-party request: the browser sends it the cookies set for `example.com`, lets it set cookies of its own, and does not apply the protections it applies to third parties.

CNAME cloaking exploits this. The website points one of its own subdomains, through a DNS alias (a CNAME record), at a server run by another company - typically an analytics or advertising provider. To the browser, and to the visitor, the third party now looks like the website itself. Tracking that browsers and privacy tools would otherwise block or limit as third-party goes through under the website's own name.

How we measured it

The capture engine includes a CNAME detection, but it works by matching addresses against a list of known tracking domains. Every figure in this report rests on observed behaviour, so we did not use it. Instead we resolved the DNS records of every subdomain of each website that the audited pages contacted, and followed each chain of aliases to its end.

This resolution was done on 7 October 2026, after the capture. DNS records can change; the results show how each subdomain was configured on that date.

What we found on dpoffice.net

Subdomain	Alias resolves to	Requests before consent
analytics.dpoffice.net	track.hubspot.com	1

The law

ePrivacy Directive, Article 5(3). Requests and cookies handled through an alias are storage on, and access to, the visitor's device in the same way as any other. The alias changes nothing about the need for consent.

GDPR, Article 5(1)(a), Article 25 and Article 26. Disguising a third party's data collection as the website's own is the opposite of fairness and transparency. A visitor, a browser or a privacy tool looking at the requests sees the website's name, not the company receiving the data. Designing a system so that a third party's tracking escapes the protections the visitor's browser applies to third parties is the opposite of data protection by design. The website operator, which created the alias, is at least a joint controller for the collection and transmission (section 4.00).

GDPR, Articles 12 to 14. A visitor can only be told who receives their data if the notice names the company behind each aliased subdomain. Whether the website's notice does so is set out in section 4A; nothing in the request itself tells the visitor.

4.3 Sideloaded scripts

What it is

A website chooses which scripts to put on its pages. Many of those scripts then load further scripts of their own, from other companies, which the website never named. A tag manager loads a dozen analytics and advertising tags; an advertising library loads bidders; a consent tool loads its own components. We call these **sideloaded scripts**: scripts loaded by another script from a different origin.

Every one of these scripts is code downloaded to the visitor's device and run there. It is stored in the browser, executed with access to the page and to the browser's interfaces, and can do everything described in the rest of this report. The visitor did not ask for any of it, and in most cases neither did the website operator by name.

How we measured it

The capture engine records every script that is loaded by another script from a different origin, together with the script that loaded it. These records are the basis of this section.

The engine's definition is technical, so it includes some scripts that a company loads from its own content domains - x.com loading code from twimg.com, for example. We therefore give two figures: all sideloaded scripts as the engine defines them, and the subset loaded from a different registrable domain from the website's own.

The engine also records every script inserted into a page. Those records include each site's own inline code, so they are not counted here.

What we found on dpoffice.net

Measure	Figure
Sideloaded script loads	**16**
Where	16 on the homepage

Every sideloaded script, with the script that loaded it, is listed in Appendix D.

The law

ePrivacy Directive, Article 5(3). A script downloaded to the device and run there is information stored in the terminal equipment, and the access it then has to the device's interfaces is access to information stored there. Loading third-party code onto a visitor's device without consent engages Article 5(3), before the code does anything else. It is not strictly necessary to load an advertiser's bidding script to show someone a news article.

GDPR, Articles 25, 26, 28 and 32. A website operator that lets loaded scripts load further scripts it has not chosen cannot know what code runs on its visitors' devices, which processors and third parties receive their data, or whether that code is secure. That is incompatible with data protection by design (Article 25), with the requirement to engage processors only under contracts that bind them (Article 28), and with security of processing (Article 32). Under Fashion ID, the operator is a joint controller for the collection and transmission that this code carries out (section 4.00, Article 26).

GDPR, Articles 12 to 14. A visitor cannot be told who receives their data when the website itself does not know which scripts its pages will load.

4.4 Cookies

What it is

A cookie is a small piece of data a website stores in the visitor's browser and receives back with later requests. Cookies can hold settings and session state; they can also hold an identifier that recognises the same browser across pages, visits and websites. Advertising and analytics cookies are surveillance technology: their purpose is to keep state that lets a company follow behaviour over time.

Cookies are set in two ways - by a server, in its response (a Set-Cookie header), and by a script on the page, through `document.cookie`. Scripts can also read the cookies set for a site, and the browser sends a site's cookies back with every request to it.

What we found on dpoffice.net

Measure	Figure
Events	**170**
Where	104 on the homepage, 45 on the privacy notice, 21 on the cookie notice

Techniques

Technique	Events
cookies.sent	117
document.cookie.write	29
document.cookie.read	13
cookies.set	11

Scripts and servers responsible

Script or server	Events
server:dpoffice.net	101
dpoffice.net	27
server:.dpoffice.net	16
www.googletagmanager.com	7
server:.linkedin.com	6
script.hotjar.com	5
server:linkedin.com	2
snap.licdn.com	1
securepubads.g.doubleclick.net	1
server:tiktok.com	1
server:.doubleclick.net	1
analytics.tiktok.com	1

"server:" denotes an event caused by a server response with no script involved; "unattributed" denotes an event with no usable call stack.

Cookies set before consent (17)

Name	Domain	Expires	Third-party	Set on
test_cookie	doubleclick.net	Mon, 02-Nov-2026 14:06:49 GMT	yes	homepage
__cf_bm	hubspot.com	Mon, 02 Nov 2026 14:21:50 GMT	yes	homepage
__cf_bm	linkedin.com	Mon, 02 Nov 2026 14:21:50 GMT	yes	homepage
bcookie	linkedin.com	Tue, 02-Nov-2027 13:51:50 GMT	yes	homepage
li_gc	linkedin.com	Sat, 01 May 2027 13:51:50 GMT	yes	homepage
lidc	linkedin.com	Tue, 03 Nov 2026 13:51:50 GMT	yes	homepage
_ttp	tiktok.com	session	yes	homepage
OptanonConsent	dpoffice.net	session	no	cookie notice
_dpo_first_visit	dpoffice.net	session	no	cookie notice
_dpo_legacy	dpoffice.net	session	no	cookie notice
_dpo_uid	dpoffice.net	session	no	cookie notice
_fbp	dpoffice.net	session	no	cookie notice
_ga	dpoffice.net	session	no	cookie notice
_ga_DPOTESTFAKE	dpoffice.net	session	no	privacy notice
_gcl_au	dpoffice.net	session	no	cookie notice
auth_token	dpoffice.net	session	no	cookie notice
sessionid	dpoffice.net	session	no	cookie notice

The law

ePrivacy Directive, Article 5(3). Setting a cookie is storing information in the terminal equipment; reading it, by script or with a request, is gaining access to information already stored there. Both require consent unless strictly necessary for a service the visitor explicitly requested. A cookie that keeps an identifier for months is not strictly necessary to display a page.

ePrivacy Directive, Article 5(1). Cookies that hold an identifier used to follow behaviour across visits and websites are instruments of surveillance. Surveillance of a person's communications - here, the pages they request and read - without their consent is prohibited by Article 5(1), in addition to Article 5(3).

GDPR, Articles 5, 6 and 7. An identifier in a cookie is personal data. Processing it before consent, where consent is required, has no lawful basis; consent that was never asked for cannot meet Article 7.

Criminal law. Writing data to a visitor's device and reading it back, without the visitor's knowledge or consent, is access to an information system without right (Directive 2013/40/EU, Article 3; Budapest Convention, Article 2) and alteration of data on it (Directive 2013/40/EU, Article 5; Budapest Convention, Article 4). This is not storage of mundane data: it is storage of a tracking mechanism. In California, knowingly accessing a computer or its data without permission engages Penal Code section 502, and identifiers sent to third parties that capture addressing and signalling information engage section 638.51.

4.5 Local storage, session storage and other browser storage

What it is

Browsers give websites several places to store data on the visitor's device besides cookies: local storage, which persists until it is deleted; session storage, which lasts until the tab is closed; IndexedDB, a database in the browser; the cache storage and service workers used by web applications; and `window.name`, a value that survives navigation from one site to another. These stores are not sent to servers automatically, but scripts can read them at any time and send what they contain. They are widely used to keep identifiers, consent state and behavioural data, including by companies that want an identifier that survives the deletion of cookies.

What we found on dpoffice.net

Measure	Figure
Events	**66**
Where	29 on the homepage, 19 on the privacy notice, 18 on the cookie notice

Techniques

Technique	Events
localStorage.setItem	16
sessionStorage.setItem	8
localStorage.getItem	7
indexedDB.put	6
sessionStorage.getItem	5
indexedDB.open	3
cacheStorage.open	3
broadcastChannels.BroadcastChannel	3
serviceWorkers.register	3
cacheStorage.add	3
cacheStorage.put	3
windowName.read	3
localStorage.removeItem	1
sessionStorage.removeItem	1
cacheStorage.match	1

Scripts and servers responsible

Script or server	Events
dpoffice.net	53
script.hotjar.com	6
www.googletagmanager.com	3

Script or server	Events
analytics.tiktok.com	2
securepubads.g.doubleclick.net	1
snap.licdn.com	1

"server:" denotes an event caused by a server response with no script involved; "unattributed" denotes an event with no usable call stack.

The law

ePrivacy Directive, Article 5(3). Writing to any of these stores is storing information in the terminal equipment, and reading from them is gaining access to it. Article 5(3) is not limited to cookies; it applies to every technology that stores or accesses information on the device.

ePrivacy Directive, Article 5(1). Where the stored data is an identifier or behavioural record used to follow the visitor, it is a surveillance mechanism (section 4.4).

GDPR, Articles 5, 6 and 7. Identifiers and behavioural data held in browser storage are personal data, processed here without any consent having been sought.

Criminal law. As with cookies, writing to and reading from the device's storage without right is illegal access and data interference (Directive 2013/40/EU, Articles 3 and 5; Budapest Convention, Articles 2 and 4), and engages California Penal Code section 502. Registering a service worker - code that keeps running in the browser after the page is closed - adds interference with the functioning of the system (Directive 2013/40/EU, Article 4; Budapest Convention, Article 5).

4.6 Beacons, keep-alive requests, tracking pixels and link decoration

What it is

These are the techniques used to get data off the visitor's device.

- **Beacons** (`navigator.sendBeacon`) send data to a server in the background. They are designed to be delivered even as the page closes, so that nothing is lost when the visitor leaves.
- **Keep-alive requests** (`fetch` with `keepalive`) do the same with an ordinary request.
- **Tracking pixels** are invisible images whose address carries data to the server that serves them.
- **Link decoration** adds identifiers to the addresses of requests or links so that the receiving server can recognise the visitor.

What we found on dpoffice.net

Measure	Figure
Events	**11**
Where	8 on the homepage, 3 on the privacy notice

Techniques

Technique	Events
fetch.keepalive	7
sendBeacon.sendBeacon	3
img.trackingPixel	1

Scripts and servers responsible

Script or server	Events
dpoffice.net	5
www.googletagmanager.com	3
unattributed	1
analytics.tiktok.com	1
snap.licdn.com	1

"server:" denotes an event caused by a server response with no script involved; "unattributed" denotes an event with no usable call stack.

The law

ePrivacy Directive, Article 5(3). Collecting data from the device and sending it to a server is gaining access to information stored in the terminal equipment.

GDPR, Articles 5, 6 and 7. This is the moment personal data leaves the visitor's control. Doing it before consent has no lawful basis.

GDPR, Chapter V. Section 4.11 sets out where the servers receiving the data are registered and located.

Criminal law and CIPA. Taking data from a visitor's device without permission engages California Penal Code section 502. Beacons and pixels that report the pages a visitor is reading, and identifiers attached to those reports, capture addressing and signalling information and engage section 638.51.

4.7 Referrer leakage

What it is

When a page loads a resource from another company's server - a script, a font, an image - the browser normally tells that server which page asked for it, in the Referer header. Depending on the website's settings, that is either just the website's address or the full address of the page, including the article or search being viewed.

Each such request tells a third party that this browser is on this website at this moment. On a health or adult website, the mere fact of the visit is sensitive (section 4.12).

What we found on dpoffice.net

Measure	Figure
Events	**32**
Where	26 on the homepage, 4 on the privacy notice, 2 on the cookie notice

Techniques

Technique	Events
referer.crossOrigin	32

Scripts and servers responsible

Script or server	Events
server:analytics.tiktok.com	5
server:www.google-analytics.com	3
server:fonts.gstatic.com	3
server:cdn.jsdelivr.net	3
server:region1.google-analytics.com	3
server:px.ads.linkedin.com	2
server:securepubads.g.doubleclick.net	2
server:connect.facebook.net	1
server:static.hotjar.com	1
server:www.clarity.ms	1
server:snap.licdn.com	1
server:insecure-pixel.example.com	1

"server:" denotes an event caused by a server response with no script involved; "unattributed" denotes an event with no usable call stack.

Domains told of the visit

Receiving domain	Requests
google-analytics.com	6

Receiving domain	Requests
tiktok.com	5
gstatic.com	3
jsdelivr.net	3
hotjar.com	2
dpoffice.net	2
linkedin.com	2
doubleclick.net	2
facebook.net	1
clarity.ms	1
licdn.com	1
example.com	1
hubspot.com	1
eloqua.com	1
tiktokw.us	1

The law

GDPR, Articles 5, 6 and 32. A request that reveals a visitor's presence on a website, with their IP address, is personal data disclosed to a third party. Disclosing it without a lawful basis, and configuring pages so that third parties receive more than they need, breaches the principles of lawfulness and data minimisation and the duty of security.

GDPR, Chapter V. Section 4.11 sets out where the receiving servers are registered and located.

CIPA, section 638.51. Capturing the addressing information of the pages a person visits is the function of a pen register or trap and trace device.

4.8 Cross-origin messaging, tracking frames and other browser mechanisms

What it is

Browsers keep the code of different websites apart. Several mechanisms exist to let them talk to each other, and they are used to move data between the website and third parties inside the browser, out of sight of the network:

- **postMessage** sends data from one window or frame to another. With a target of `*` (a wildcard), the data can be received by any origin.
- **MessageChannel** and **BroadcastChannel** open channels between frames and between tabs.
- **Hidden third-party frames** embed another company's page invisibly, giving it its own access to the browser.
- **History rewriting** (`history.replaceState`) changes the address shown in the browser without a new page load.
- **Content Security Policy violation listeners**, **Web Locks** and the **Topics** interface can be used to coordinate between scripts or, in the case of Topics, to request the browser's own profile of the visitor's interests.

What we found on dpoffice.net

Measure	Figure
Events	**10**
Where	6 on the homepage, 2 on the privacy notice, 2 on the cookie notice

Techniques

Technique	Events
broadcastChannelCovert.BroadcastChannel	3
topics.browsingTopics	3
postMessage.wildcard	3
iframe.crossOrigin	1

Scripts and servers responsible

Script or server	Events
dpoffice.net	7
	1
unattributed	1
connect.facebook.net	1

"server:" denotes an event caused by a server response with no script involved; "unattributed" denotes an event with no usable call stack.

The law

ePrivacy Directive, Article 5(3). Each of these mechanisms is used by scripts that are running on the visitor's device and moving information obtained there.

GDPR, Articles 5, 6, 7, 25 and 32. Sending data to any origin that is listening (wildcard postMessage) is a security failure as well as a disclosure; embedding hidden third-party frames hands third parties their own presence in the visitor's browser. Neither is compatible with data protection by design or with security of processing. Requesting the browser's interest profile is processing of personal data about the visitor's interests, without any basis.

4.9 Event listeners, form reads and clipboard monitoring

What it is

Scripts can listen to what a visitor does - every movement of the mouse, every scroll, every touch, every key - and read what is typed into forms, including before it is submitted. Recorded together and sent to a server, this is how "session replay" tools reconstruct a visit, and how behavioural analysis and bot-detection products profile a visitor by the way they move. Scripts can also watch the clipboard as content is copied, cut or pasted.

The visitor's interaction with a page is a communication between the visitor and the website. Recording it for a third party is interception.

What we found on dpoffice.net

Measure	Figure
Events	**3**
Where	3 on the homepage

Techniques

Technique	Events
behavioural.scroll	2
behavioural.mousemove	1

Scripts and servers responsible

Script or server	Events
script.hotjar.com	2
analytics.tiktok.com	1

"server:" denotes an event caused by a server response with no script involved; "unattributed" denotes an event with no usable call stack.

The law

ePrivacy Directive, Article 5(1). Listening to, recording or otherwise intercepting a communication without consent is prohibited. A visitor's interaction with a page is part of their communication with the website; capturing it for a third party is interception, and the systematic recording of behaviour is surveillance.

ePrivacy Directive, Article 5(3). Reading form values and registering listeners on the device is access to information in the terminal equipment.

GDPR, Articles 5, 6, 7, 25 and 32. Behavioural data and form contents are personal data and can include anything a visitor types.

Criminal law. Interception of non-public transmissions of computer data is an offence under Article 6 of Directive 2013/40/EU and Article 3 of the Budapest Convention. In California, reading or attempting to learn the contents of a communication in transit, without the consent of all parties, engages Penal Code section 631 - the provision on which session-replay claims in California are based.

4.10 Client hints, ETags, HSTS, Alt-Svc and pre-emptive connections

What it is

These mechanisms work at the level of the web's protocols, not through scripts. Each has a legitimate function. Each can also be used to recognise a visitor, and some are documented ways of doing so when cookies are blocked or deleted. We count them in Tier 3, with that caveat.

- **Client hints.** A server can instruct the browser (with an Accept-CH header) to send detailed information about the device - platform, model, architecture, version - with every subsequent request.
- **ETags.** A server attaches a tag to a resource; the browser stores it in its cache and sends it back the next time it requests the resource. A unique ETag works as an identifier that survives the deletion of cookies.
- **HSTS.** A server tells the browser to use secure connections in future; the browser stores that instruction per host. The pattern of stored instructions across many hosts can be used as a "supercookie".
- **Alt-Svc.** A server tells the browser about alternative ways to connect to it, which the browser stores and can reuse to recognise the same browser.
- **Pre-emptive connections and background workers.** Pages instruct the browser to resolve, connect to or fetch from third-party servers before anything is needed, and start workers and WebSockets that keep connections open.

What we found on dpoffice.net

Measure	Figure
Events	**274**
Where	175 on the homepage, 60 on the privacy notice, 39 on the cookie notice

Techniques

Technique	Events
altSvc.set	114
hsts.set	72
clientHints.request	66
etag.set	15
fetch.reject	3
resourceHint.preconnect	2
fetch.error	2

Scripts and servers responsible

Script or server	Events
unattributed	121
server:dpoffice.net	87
server:cdn.jsdelivr.net	13
server:securepubads.g.doubleclick.net	6

Script or server	Events
server:analytics.tiktok.com	5
server:px.ads.linkedin.com	4
server:fonts.googleapis.com	3
server:www.google-analytics.com	3
server:static.hotjar.com	3
server:fonts.gstatic.com	3
server:script.hotjar.com	3
server:www.googletagmanager.com	3

"server:" denotes an event caused by a server response with no script involved; "unattributed" denotes an event with no usable call stack.

The law

ePrivacy Directive, Article 5(3). An ETag is stored in the browser's cache and returned on the next request; HSTS and Alt-Svc state is stored by the browser; a client hints instruction makes the browser hand over information about the device with every request. Each is storage in, or access to information from, the terminal equipment.

GDPR, Articles 5, 6 and 7. Where these mechanisms are used to recognise a visitor, the data they carry is personal data, and server-side tracking needs a lawful basis just as browser-side tracking does. That the tracking happens on a server does not make it lawful.

4.11 International transfers

What it is

Chapter V of the GDPR (Articles 44 to 50) allows personal data to be transferred to a country outside the European Economic Area only on one of the bases it sets out - an adequacy decision, appropriate safeguards such as standard contractual clauses, or one of the narrow derogations. Every request a visitor's browser makes to a server carries at least their IP address, and usually much more, so every request to a server outside the EEA is a candidate transfer.

How we measured it

The capture records the IP address of every server each page connected to. For each server address the website's pages contacted we first obtained the network it belongs to, the organisation that operates that network, and the country in which the address block is registered, from the Team Cymru IP-to-ASN mapping service, on 7 October 2026.

This is registry data, not physical geolocation. It identifies the jurisdiction of the organisation operating the receiving network. It does not prove where a particular request was processed. Content delivery networks, in particular, answer from servers close to the visitor, so many requests to US-registered networks will have been served from inside the EEA. That does not remove them from the scope of this section: the operator receiving the data is subject to the law of the country where it is established, which is the concern the Court of Justice addressed in Schrems II.

What we found on dpoffice.net

Measure	Figure
Servers contacted	15
Of which third-party	14
On networks registered outside the EEA	12
Located outside the EEA, where the location could be determined	4

Server	Third-party	Operator	Registry country	Geolocation
analytics-ipv6.tiktokw.us	yes	AKAMAI-ASN1	US	FR
analytics.tiktok.com	yes	AKAMAI-ASN1	US	FR
cdn.jsdelivr.net	yes	FASTLY	US	indeterminate (anycast)
connect.facebook.net	yes	FACEBOOK	IE	FR
fonts.gstatic.com	yes	GOOGLE	US	US
px.ads.linkedin.com	yes	CLOUDFLARENET	US	indeterminate (anycast)
region1.google-analytics.com	yes	GOOGLE	US	US
script.hotjar.com	yes	AMAZON-02	US	FR
securepubads.g.doubleclick.net	yes	GOOGLE	US	DE
snap.licdn.com	yes	AKAMAI-ASN1	NL	IT
static.hotjar.com	yes	AMAZON-02	US	FR
track.hubspot.com	yes	CLOUDFLARENET	US	indeterminate (anycast)
www.clarity.ms	yes	MICROSOFT-CORP-MSN-AS-BLOCK	US	CH
www.google-analytics.com	yes	GOOGLE	US	CA, US

Server	Third-party	Operator	Registry country	Geolocation
dpoffice.net	no	DATASTREAM-NET	MT	MT

Geolocation: DB-IP IP to Country Lite, October 2026 (IP geolocation by DB-IP, licensed under CC BY 4.0). Cloudflare and Fastly answer from shared anycast addresses and are treated as indeterminate.

The law

No transfer mechanism can cure processing that has no lawful basis. Every transfer counted here happened before any consent was given. Where consent was required for the processing in the first place (sections 4.1 to 4.10), there was no lawful basis under Article 6, and the question of which Chapter V mechanism applies does not arise.

The United States. Transfers to US organisations certified under the EU-US Data Privacy Framework rely on Commission Implementing Decision (EU) 2023/1795. The General Court dismissed a challenge to that decision in Latombe v Commission (T-553/23, judgment of 3 September 2025, ECLI:EU:T:2025:831); an appeal to the Court of Justice was lodged on 31 October 2025 (C-703/25 P) and was pending when this report was written. Its predecessor, the Privacy Shield, was annulled by the Court of Justice in Schrems II (C-311/18, judgment of 16 July 2020, ECLI:EU:C:2020:559) because of the access US intelligence agencies have to data held by US companies. Whether each receiving organisation is certified under the Framework, and for which data, is something each website must be able to show; certification of a content delivery network does not extend to the advertising and analytics companies whose servers the data reaches.

Transparency. Articles 13(1)(f) and 14(1)(f) require a privacy notice to state the intention to transfer and the mechanism relied on. Section 4A sets out how many notices do.

4.12 Special categories of data

This report does not make findings under Article 9 GDPR on the basis of dpoffice.net's subject matter. The provisions in sections 4.1 to 4.11 apply irrespective of the content of the pages visited.

4A. Disclosures: privacy and cookie notices

What is required

Readability

- **Privacy notice** (https://dpoffice.net/privacy.html): 1,043 words - about 4 minutes to read at an average adult reading speed of 238 words a minute (Brysbaert, 2019); Flesch Reading Ease 33.5 (below 50 is difficult, below 30 very difficult); Flesch-Kincaid grade 13.6, a reading age of about 18.6.
- **Cookie notice** (https://dpoffice.net/cookie-policy.html): 337 words - about 1 minutes to read at an average adult reading speed of 238 words a minute (Brysbaert, 2019); Flesch Reading Ease 37.7 (below 50 is difficult, below 30 very difficult); Flesch-Kincaid grade 11.8, a reading age of about 16.8.

What the notices say compared with what the website did

[To be completed after reading the notices in full.]

The law

GDPR, Article 12(1). Information must be concise, transparent, intelligible and easily accessible, in clear and plain language.

GDPR, Articles 13 and 14. Each item in the table above is mandatory. A notice that does not name the cookies a website sets, the fingerprinting it carries out or the companies that receive the data cannot inform a decision about any of them.

GDPR, Article 5(1)(a), and ePrivacy Article 5(3). Consent must be informed. Where the notice does not describe what the website does, no consent obtained against it could be valid; and here, no consent was obtained at all. A notice that says something will happen only with consent, on a website that does it before consent is asked for, is not a transparency failure alone: it misdescribes the processing.

4B. Built-in AI interfaces

What they are

How we measured it

The version of WebSentinel used for this research did not record calls to these interfaces (section 3.5). Instead, we searched the full source of every script delivered to every audited page for code that uses them, and read the code around every match. In addition, the on-device model was switched off in the audit browser, so any attempt to use it could only have found it unavailable.

These findings therefore show **code delivered to visitors' devices**, before any consent, that is written to use the built-in AI interfaces. They do not show that the code ran.

What we found on dpoffice.net

No code using the browser's built-in AI interfaces was found in the scripts delivered to this website's audited pages.

5. Evidence

Page	Session	Records	Chain valid	Flags
homepage	sess_ffc5f6c2-51ed-4fa0-abdb-be08cdca5c7d	7	True	none
privacy notice	sess_4156bc57-52c7-41c2-ab3a-5ba3c3ce961e	2	True	none
cookie notice	sess_0ebb93e1-5b65-4993-917f-5036174a5ee8	2	True	none

Each record is SHA-256 hash-chained, signed with ECDSA P-256 using a key held by a Secure Enclave, timestamped by FreeTSA under RFC 3161, and submitted to two OpenTimestamps calendars for anchoring in the Bitcoin blockchain (section 3.4). The evidence for dpoffice.net can be provided for independent verification; the verification steps are in Appendix E.

6. Scale

One visit to dpoffice.net's homepage, before any consent, produced 611 events that engage the law. A person who visits the homepage once a day is subject to about 223,015 such events a year from it; once a week, about 31,772; once a month, about 7,332.

DPOffice is a test site with no real visitors, so no figure for its impact on people in the EU applies.

7. Next steps

- [Record of contact with dpoffice.net: dates, participants and outcome.]

Appendix B. Cookies set before consent

Name	Domain	Expires	Third-party	Set on	Set by
test_cookie	doubleclick.net	Mon, 02-Nov-2026 14:06:49 GMT	yes	homepage	server:.doubleclick.net
__cf_bm	hubspot.com	Mon, 02 Nov 2026 14:21:50 GMT	yes	homepage	server:hubspot.com
__cf_bm	linkedin.com	Mon, 02 Nov 2026 14:21:50 GMT	yes	homepage	server:linkedin.com
bcookie	linkedin.com	Tue, 02-Nov-2027 13:51:50 GMT	yes	homepage	server:.linkedin.com
li_gc	linkedin.com	Sat, 01 May 2027 13:51:50 GMT	yes	homepage	server:.linkedin.com
lidc	linkedin.com	Tue, 03 Nov 2026 13:51:50 GMT	yes	homepage	server:.linkedin.com
_ttp	tiktok.com	session	yes	homepage	server:tiktok.com
OptanonConsent	dpoffice.net	session	no	cookie notice	dpoffice.net
_dpo_first_visit	dpoffice.net	session	no	cookie notice	dpoffice.net
_dpo_legacy	dpoffice.net	session	no	cookie notice	dpoffice.net
_dpo_uid	dpoffice.net	session	no	cookie notice	dpoffice.net
_fbp	dpoffice.net	session	no	cookie notice	dpoffice.net
_ga	dpoffice.net	session	no	cookie notice	dpoffice.net
_ga_DPOTESTFAKE	dpoffice.net	session	no	privacy notice	www.googletagmanager.com
_gcl_au	dpoffice.net	session	no	cookie notice	dpoffice.net
auth_token	dpoffice.net	session	no	cookie notice	dpoffice.net
sessionid	dpoffice.net	session	no	cookie notice	dpoffice.net

Appendix E. Verifying the evidence

[To be completed: the exact commands for verifying each record's SHA-256 hash, ECDSA signature, RFC 3161 timestamp token and OpenTimestamps proofs, each tested against dpoffice.net's records before this report is issued.]

Appendix D. Sideloaded scripts

Script	Loaded by	Page
https://www.googletagmanager.com/gtag/js	https://dpoffice.net/	homepage
https://securepubads.g.doubleclick.net/tag/js/gpt.js	https://dpoffice.net/	homepage
https://code.jquery.com/jquery-3.6.0.min.js	https://dpoffice.net/	homepage
https://cdnjs.cloudflare.com/ajax/libs/lodash.js/4.17.21/lodash.min.js	https://dpoffice.net/	homepage
https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/js/bootstrap.bundle.min.js	https://dpoffice.net/	homepage
https://connect.facebook.net/en_US/fbevents.js	https://dpoffice.net/	homepage
https://analytics.tiktok.com/i18n/pixel/events.js	https://dpoffice.net/	homepage
https://static.hotjar.com/c/hotjar-0.js	https://dpoffice.net/	homepage
https://www.clarity.ms/tag/fakedpodemo	https://dpoffice.net/	homepage
https://snap.licdn.com/li.lms-analytics/insight.min.js	https://dpoffice.net/	homepage
https://cdn.jsdelivr.net/npm/vanilla-cookieconsent@3.0.1/dist/cookieconsent.umd.js	https://dpoffice.net/	homepage
https://track.hubspot.com/__ptq.js	https://dpoffice.net/	homepage
https://script.hotjar.com/modules.e85a87e594b0aace33cf.js	https://dpoffice.net/	homepage
https://securepubads.g.doubleclick.net/pagead/managed/js/gpt/m202610260101/pubads_impl.js	https://dpoffice.net/	homepage
https://analytics.tiktok.com/i18n/pixel/static/main.MTJjYzk1MmQ1MA.js	https://dpoffice.net/	homepage
https://analytics.tiktok.com/i18n/pixel/static/identify_9fbdaf50.js	https://dpoffice.net/	homepage

Appendix A. Every event type recorded

Section	Technique	Events
beacons	fetch.keepalive	7
beacons	sendBeacon.sendBeacon	3
beacons	img.trackingPixel	1
cookies	cookies.sent	117
cookies	document.cookie.write	29
cookies	document.cookie.read	13
cookies	cookies.set	11
fingerprinting	navigator.userAgent	17
fingerprinting	visibility.listen.pagehide	9
fingerprinting	visibility.listen.visibilitychange	8
fingerprinting	screen.width	4
fingerprinting	screen.height	4
fingerprinting	clientHints.getHighEntropyValues	4
fingerprinting	visibility.listen.pageshow	4
fingerprinting	sharedArrayBuffer.available	3
fingerprinting	visibility.listen.beforeunload	3
fingerprinting	focus.hasFocus	3
fingerprinting	visibility.listen.focus	3
fingerprinting	visibility.listen.blur	3
fingerprinting	document.visibilityState	3
fingerprinting	webgl.getParameter	2
fingerprinting	navigator.cookieEnabled	2
fingerprinting	navigator.doNotTrack	2
fingerprinting	navigator.language	2
fingerprinting	canvas.toDataURL	1
fingerprinting	webgl.getExtension	1
fingerprinting	navigator.platform	1
fingerprinting	navigator.languages	1
fingerprinting	navigator.hardwareConcurrency	1
fingerprinting	navigator.deviceMemory	1
fingerprinting	navigator.maxTouchPoints	1
fingerprinting	navigator.vendor	1
fingerprinting	navigator.plugins	1
fingerprinting	navigator.mimeTypes	1

Section	Technique	Events
fingerprinting	navigator.pdfViewerEnabled	1
fingerprinting	screen.colorDepth	1
fingerprinting	screen.pixelDepth	1
fingerprinting	screen.availWidth	1
fingerprinting	screen.availHeight	1
fingerprinting	screen.orientation	1
fingerprinting	screenOrientation.type	1
fingerprinting	timezone.resolvedOptions	1
fingerprinting	webrtc.RTCPeerConnection	1
fingerprinting	webrtc.createDataChannel	1
fingerprinting	webrtc.createOffer	1
fingerprinting	networkInfo.effectiveType	1
fingerprinting	networkInfo.downlink	1
fingerprinting	networkInfo.rtt	1
fingerprinting	networkInfo.saveData	1
fingerprinting	storageEstimate.estimate	1
fingerprinting	speech.getVoices	1
fingerprinting	keyboard.getLayoutMap	1
fingerprinting	deviceSensor.listen.devicemotion	1
fingerprinting	deviceSensor.listen.deviceorientation	1
fingerprinting	battery.getBattery	1
fingerprinting	credentials.get	1
fingerprinting	idleDetection.requestPermission	1
fingerprinting	sensors.Accelerometer	1
fingerprinting	sensors.Gyroscope	1
fingerprinting	webrtc.setLocalDescription	1
fingerprinting	trustedTypes.createPolicy	1
fingerprinting	timing.getEntriesByType	1
fingerprinting	requestIdleCallback	1
fingerprinting	performanceObserver.PerformanceObserver	1
fingerprinting	timing.PerformanceObserver	1
fingerprinting	paintTiming.largest-contentful-paint	1
fingerprinting	performanceObserver.observe	1
headers	altSvc.set	114
headers	hsts.set	72
headers	clientHints.request	66

Section	Technique	Events
headers	etag.set	15
headers	fetch.reject	3
headers	resourceHint.preconnect	2
headers	fetch.error	2
listeners	behavioural.scroll	2
listeners	behavioural.mousemove	1
messaging	broadcastChannelCovert.BroadcastChannel	3
messaging	topics.browsingTopics	3
messaging	postMessage.wildcard	3
messaging	iframe.crossOrigin	1
referrer	referer.crossOrigin	32
storage	localStorage.setItem	16
storage	sessionStorage.setItem	8
storage	localStorage.getItem	7
storage	indexedDB.put	6
storage	sessionStorage.getItem	5
storage	indexedDB.open	3
storage	cacheStorage.open	3
storage	broadcastChannels.BroadcastChannel	3
storage	serviceWorkers.register	3
storage	cacheStorage.add	3
storage	cacheStorage.put	3
storage	windowName.read	3
storage	localStorage.removeItem	1
storage	sessionStorage.removeItem	1
storage	cacheStorage.match	1

Appendix C. Servers contacted before consent

Server	Third-party	Operator	Registry country	Geolocation	Pages
analytics-ipv6.tiktokw.us	yes	AKAMAI-ASN1	US	FR	homepage
analytics.tiktok.com	yes	AKAMAI-ASN1	US	FR	homepage
cdn.jsdelivr.net	yes	FASTLY	US	indeterminate (anycast)	homepage
connect.facebook.net	yes	FACEBOOK	IE	FR	homepage
fonts.gstatic.com	yes	GOOGLE	US	US	homepage
px.ads.linkedin.com	yes	CLOUDFLARENET	US	indeterminate (anycast)	homepage
region1.google-analytics.com	yes	GOOGLE	US	US	homepage, privacy notice
script.hotjar.com	yes	AMAZON-02	US	FR	homepage
securepubads.g.doubleclick.net	yes	GOOGLE	US	DE	homepage
snap.licdn.com	yes	AKAMAI-ASN1	NL	IT	homepage
static.hotjar.com	yes	AMAZON-02	US	FR	homepage
track.hubspot.com	yes	CLOUDFLARENET	US	indeterminate (anycast)	homepage
www.clarity.ms	yes	MICROSOFT-CORP-MSN-AS-BLOCK	US	CH	homepage
www.google-analytics.com	yes	GOOGLE	US	CA, US	homepage, privacy notice
dpoffice.net	no	DATASTREAM-NET	MT	MT	cookie notice, homepage, privacy notice