

Scan**RGPD**

The pixel you installed is on **your** invoice

Why GDPR exposure follows the agency that built the site, and how to turn it into a line item instead of a liability.

WHAT CHANGED

A client in dispute no longer looks for a bug.

Late delivery, a design disagreement, a drop in traffic. The fastest way to hold an invoice is no longer to open the browser console. It is to have the site scanned for GDPR failures, and to point at whoever configured it.

WHAT A SCAN FINDS ON A SITE YOU DELIVERED

Six failures, all of them yours to explain.

01 Trackers before consent Analytics and advertising pixels firing from page load. Art. 5 & 7 GDPR	02 No symmetric refusal Accepting is one click, refusing takes three, or is impossible. Art. 7(3) GDPR	03 Server-side tracking GTM-SS containers and CAPI relays that bypass the banner entirely. Art. 5(1)(a) GDPR
04 Consent Mode v2 misconfigured Missing gcd and gcs parameters, conversions silently rejected. DMA 2024	05 Third-country transfers Captcha and session replay services outside the EEA, no valid mechanism. Chapter V GDPR	06 Embedded third-party content Video players, maps and social widgets loading cookies on arrival. Art. 5(3) ePrivacy

THE PART MOST AGENCIES GET WRONG

You are not a bystander. You are a processor.

“A processor shall be liable for the damage caused by processing **only where it has not complied with obligations** of this Regulation specifically directed to processors, or where it has acted outside or contrary to lawful instructions of the controller.”

Article 82(2) GDPR

Building, hosting or maintaining a client site means processing personal data on their behalf. That makes you a processor under Article 28, with obligations of your own, and liability of your own. The contract that names you does not move that liability, it records it.

COURT OF JUSTICE OF THE EUROPEAN UNION

Embedding a third-party widget creates joint controllership.

THE RULING**Fashion ID, C-40/17**

The operator of a website that embeds a third-party social plugin is a joint controller with that third party for the collection and transmission of the visitor's data, even if the operator has no access to it.

Judgment of 29 July 2019

WHAT IT MEANS FOR YOU**You chose the embed**

The YouTube player, the Meta Pixel, the map, the chat widget: each one you added put your client into joint controllership. When the complaint arrives, the question is who configured it, and the answer is on your invoice.

Applies across the EEA

THE MONEY HAS MOVED

Most of the fines ever issued under the GDPR are recent.

Thirty supervisory authorities apply the same regulation. The volume changed sharply after 2023.

€7.1bn¹

in GDPR fines issued across the EEA
since 2018

2,685²

documented enforcement cases
as of March 2026

€1.2bn¹

issued in 2025 alone

60%+¹

of all fine value imposed since
January 2023

YOUR CLIENTS ARE ON THE LIST THIS YEAR

In 2026, EU authorities are checking exactly what you configured.

2025 Right to erasure 32 authorities took part, 764 controllers answered. Findings adopted 10 February 2026.³	2026 · RUNNING NOW Transparency and information, Art. 12-14 25 authorities are contacting controllers across sectors this year.⁴	What it covers The pages you wrote Privacy notice, information at the point of collection, and whether the banner matches the browser's actual behaviour.
--	---	---

When a client is contacted, they will forward the letter to whoever built the site. You will either answer for free, under warranty, or you will have sold the audit as a deliverable before it was needed.

THE TURN

From liability to line item.

The exposure exists whether or not you bill for it. The only variable is whether it appears on a quote or on a complaint.

FOUR EFFECTS, ONE TOOL

The weak point becomes the entry point.

A deliverable you can quote A 20 to 30 page report under your own brand, with four pre-filled legal documents. Sold as work, not absorbed as overhead.	A reason to reopen old accounts Every site you delivered in the last three years is a call you can justify making, with a finding to show.
A defence, documented A timestamped record of what was checked and when, on the day the client asks why nobody flagged it.	Capacity without hiring A hundred and fifty sites a year, each audited in under ten minutes instead of half a day.

BUY IN VOLUME, RESELL AT YOUR RATE

Thirty-three euros in. Four hundred and ninety out.

Agency Pro Pack, 150 audits per year	€4,990
Cost per audit	€33.27
Suggested resale price	€490
Margin per audit	€456.73
Annual margin if all 150 are sold	€68,509

Eleven audits cover the annual fee. The remaining hundred and thirty-nine are margin.
And the report carries your logo: ScanRGPD appears nowhere.

FOUR STEPS, ZERO INSTALLATION

Nothing to deploy on the client's site.

01

Paste the URL

No tag, no plugin, no access to the client's systems or hosting.

02

Argus runs the scan

A real browser loads the page, refuses consent, and records what still leaves.

03

Report in under 10 minutes

Your logo, your details, your rate. Four legal documents included.

04

Re-scan after fixes

Unlimited iterations, so the client sees the score move.

WHAT THE ENGINE CHECKS

The twelve-point technical checklist.

- ❑ **Consent Bypass Test** — trackers still firing after refusal
- ❑ **Server-side tracking** — GTM-SS containers and CAPI relays
- ❑ **CNAME resolution** — third parties disguised as first-party
- ❑ **Consent Mode v2** — gcd and gcs parameters under the DMA
- ❑ **Storage tracking** — localStorage, sessionStorage, IndexedDB
- ❑ **Session replay** — recording tools capturing form input
- ❑ **Third-country transfers** — endpoints outside the EEA
- ❑ **Embedded content** — video, maps and social widgets
- ❑ **Banner design** — asymmetric buttons and dark patterns
- ❑ **Information notices** — presence, reachability, completeness
- ❑ **Security headers** — HSTS, CSP, X-Frame-Options, nosniff
- ❑ **Contact forms** — consent checkbox and purpose statement

PRICING

Billed annually. No per-seat pricing.

AGENCY PACK

€1,990 /year

50 audits per year, €39.80 each. Co-branded reports, dedicated partner portal. For teams of three to twenty.

AGENCY PRO PACK · MOST CHOSEN

€4,990 /year

150 audits per year, €33.27 each. Full white label with no ScanRGPD mention, Art. 28 timestamping. For agencies running at scale.

Scan one site you delivered. Then decide.

Pick a client site from last year. If the report does not give you a reason to call them, the tool is not for you.

Free · no account
scanrgpd.fr/en

EVERY FIGURE AND EVERY RULING IN THIS DOCUMENT

Where it comes from.

1. DLA Piper, *GDPR fines and data breach survey*, January 2026. Cumulative total across the EEA, 2025 volume, and share imposed since January 2023.
2. CMS, *GDPR Enforcement Tracker*, case count as of 1 March 2026. [enforcementtracker.com](https://www.enforcementtracker.com)
3. EDPB, *Coordinated Enforcement Action on the implementation of the right to erasure by controllers*, 2025. Report adopted 10 February 2026.
4. EDPB, *CEF 2026: coordinated enforcement action on transparency and information obligations under the GDPR*. edpb.europa.eu
5. Court of Justice of the European Union, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, Case C-40/17, judgment of 29 July 2019.
6. Regulation (EU) 2016/679, Articles 28 and 82. eur-lex.europa.eu

This document describes technical and contractual exposure. It is not legal advice, and the assessment of any individual case belongs to a qualified lawyer in the relevant jurisdiction.

Scan one site you built. That is the whole evaluation.

No SDRs, no ticket queue. ScanRGPD is built by one person, and that same person answers you, on GDPR strategy, on the Argus engine, on your specific case.

TRY IT

scanrgpd.fr/en

PARTNER PACKS

scanrgpd.fr/en/partenaires/agences

CONTACT

contact@scanrgpd.fr