

Le duopole qui contrôle les données des communes françaises

JVS Group & Berger-Levrault

Deux groupes équipent 85 à 95% des communes françaises en logiciels de gestion (estimation basée sur ~15 000 + ~12 000 communes équipées sur 34 875). État civil, listes électorales, cadastres, services sociaux — 51 sites audités entre les deux, aucun pleinement conforme au RGPD. Trackers publicitaires américains sans consentement. Fausses déclarations d'hébergement. Zéro certification de sécurité. L'Autorité de la Concurrence n'a jamais enquêté.

Destinataires : CNIL • ANSSI • DGCCRF • Autorité de la Concurrence — Avril 2026

Le problème en bref

JVS Group (Citopia, PanneauPocket, Mairistem, Mémento, Familea) équipe ~15 000 communes. **Berger-Levrault** (Magnus, WeMagnus, CARL, Ciril) en équipe ~12 000. Ensemble, ils gèrent les données les plus sensibles des citoyens français.

Constats : PanneauPocket embarque 9 domaines publicitaires US (Google Ads, Facebook, DoubleClick) tout en affirmant « 0% Publicité ». Les sites de communes déclarent un faux hébergeur dans leurs mentions légales. Aucun des 51 sites audités n'est conforme RGPD. Le même cabinet M&A (Oaklins) conseille les deux groupes. Le même indice de prix (Syntec) sert les deux.

1. Preuves techniques — Vérifiées le 8 avril 2026

Toutes les preuves ci-dessous ont été obtenues par des commandes `curl` exécutées sur le code source public des sites. Elles sont **reproductibles par n'importe qui** en 30 secondes.

1.1 — Google Ads sur PanneauPocket (« 0% Publicité »)

Commande :

```
curl -sL https://www.panneaupocket.com/ | grep -oE "AW-[0-9]+"
```

Résultat :

AW-17989696875

Le code source contient littéralement :

```
<script defer src="https://www.googletagmanager.com/gtag/js?id=AW-17989696875">
</script>
```

AW-17989696875 est un identifiant **Google Ads** — de la publicité ciblée. PanneauPocket se présente comme « 100% Anonyme, 0% Publicité ». **C'EST FAUX.**

Deuxième tracker :

```
<iframe src="https://www.googletagmanager.com/ns.html?id=GTM-MVM6W7GS">
```

1.1b — 9 domaines publicitaires américains dans le container GTM

L'analyse du container Google Tag Manager GTM-MVM6W7GS révèle les connexions suivantes :

```
curl -sL "https://www.googletagmanager.com/gtm.js?id=GTM-MVM6W7GS" | grep -oE
"https?://[a-zA-Z0-9._-]+\.[a-z]{2,}" | sort -u
```

DOMAINE	SERVICE	TRANSFERT USA
ad.doubleclick.net	Google Ads / DoubleClick	OUI
ade.google syndication.com	Google AdSense	OUI
adservice.google.com	Google Ads	OUI
googleads.g.doubleclick.net	Google Ads	OUI
pagead2.google syndication.com	Google AdSense	OUI
www.googleadservices.com	Google Ads	OUI
www.facebook.com	Facebook Pixel	OUI
www.youtube.com	YouTube tracking	OUI
m.youtube.com	YouTube mobile	OUI

1.2 — Matomo sans consentement sur les sites de communes

Site de **Mondonville** (31700) — construit par Citopia/JVS :

```
curl -sL https://www.mondonville.fr/ | grep "analytics.tools.citopia"

var u="https://analytics.tools.citopia.fr/";
_paq.push(['trackPageView']);
```

Matomo s'exécute immédiatement, sans bannière de consentement, sans que le citoyen puisse refuser. Les habitudes de navigation de chaque administré sont enregistrées à son insu. **VIOLATION DIRECTIVE EPRIVACY + RGPD**

Même constat sur **Saint-Geniès-Bellevue** (31) : Tarteaucitron est présent mais Matomo charge **en dehors** du gestionnaire de consentement (lignes 28–37 du code source, avant l'initialisation de Tarteaucitron). Le tracking est effectif sans consentement.

Même constat sur **Récy** (51, siège de JVS) : Matomo via `analytics.tools.citopia.fr` .

1.3 — App Mémento des Élus — Facebook SDK non déclaré

L'analyse du binaire (v4.5.5) révèle :

SDK	TRANSFERT USA	DÉCLARÉ DANS LES CGU ?
Facebook SDK (fb886826858755594)	OUI	NON — CGU disent « aucun outil de traçage »
Google Sign-In	OUI	NON
Firebase	OUI	NON
Sentry	OUI	NON

Les CGU déclarent : « *L'Application ne comporte aucun outil de suivi publicitaire ni technologie de traçage à des fins marketing.* » C'est une **fausse déclaration** (art. 226–18 Code pénal + art. L121–2 Code de la consommation).

2. Pourquoi c'est grave pour les citoyens

Le « Cheval de Troie » des données citoyennes

Chaque fois qu'un habitant ouvre PanneauPocket pour lire une alerte météo ou une info de la mairie, le tracker **Google Ads AW-17989696875** envoie aux serveurs de Google :

- **Adresse IP** (localisation approximative du citoyen)
- **Modèle du téléphone**
- **Heure de consultation**
- **Page consultée** (quelle commune, quelle alerte)

Même si le citoyen n'a pas de compte Google, ces données permettent de créer un **profil publicitaire**. Google sait qu'un appareil à telle adresse s'intéresse aux activités de telle commune.

Avec **14 000 collectivités** et des millions d'utilisateurs, c'est une **fuite massive de données citoyennes vers une plateforme publicitaire américaine**, sans consentement.

Le maire est personnellement responsable

En proposant PanneauPocket à ses administrés, le maire devient **responsable de traitement** au sens du RGPD (art. 4.7). Si l'application envoie des données aux USA via Google Ads sans consentement explicite, **le maire est en infraction**.

Le problème : **le maire ne sait pas**. PanneauPocket lui a dit « 0% Publicité ». Le tracker est invisible. Seule une analyse technique du code source le révèle.

Transferts hors UE illégaux (Schrems II)

La CJUE a invalidé le Privacy Shield (arrêt Schrems II, C-311/18, 16 juillet 2020). Les transferts de données vers les USA via Google et Facebook sont problématiques en raison des lois de surveillance américaines (**FISA 702, Cloud Act**).

PanneauPocket envoie des données vers Google (USA) sans base juridique adéquate, sans information des personnes concernées, et en contradiction avec ses propres déclarations.

3. Sites de communes auditées — 0 conforme

CRITÈRE	RÉSULTAT	DANGER CITOYEN
DPO mentionné	0 / 26	Les citoyens ne savent pas à qui s'adresser pour leurs données
RGPD référencé	0 / 26	Template de 1978, jamais mis à jour en 8 ans

HSTS	600 SEC (10 MIN)	Connexion interceptable sur WiFi public (ANSSI exige 31 536 000)
CSP	ABSENTE SUR 26/26	Injection de scripts malveillants possible (XSS)
Matomo sans consentement	MONDONVILLE (31), RÉCY (51)	Citoyens tracés à leur insu — vérifié le 8 avril 2026
Matomo hors gestionnaire consentement	SAINT-GENIÈS-BELLEVUE (31)	Tarteaucitron présent mais Matomo charge avant — vérifié le 8 avril 2026
Hébergeur déclaré faux	MONDONVILLE + RÉCY : OVH DÉCLARÉ, IONOS RÉEL	Fausse information dans un document juridique obligatoire — vérifié par WHOIS le 8 avril 2026
Certificat SSL invalide	CROIX-MARE (76)	Certificat pour *.medialibs.com, pas pour croix-mare.fr — vérifié le 8 avril 2026

Négligence industrielle : le site de **Saint-Geniès-Bellevue** (31) contient en production **4 liens vers un serveur de test interne JVS** (`jvs51.atester.fr`), exposant l'infrastructure interne du prestataire aux visiteurs du site. Vérifiable le 8 avril 2026 : `curl -sL https://www.saint-genies-bellevue.fr/ | grep jvs51` .

4. Hébergement — « Cloud Souverain » sans certification

SITE	IP	HÉBERGEUR RÉEL	PAYS	DÉCLARÉ
panneaupocket.com	83.166.138.238	Infomaniak	Suisse	—
groupe-jvs.fr	83.166.138.238	Infomaniak	Suisse	—
Sites communes WeeCity	5.250.182.150	IONOS SE	Allemagne/France	OVH (FAUX)

JVS utilise le terme « Cloud Souverain » sans aucune certification :

CERTIFICATION	STATUT
SecNumCloud (ANSSI)	ABSENTE
ISO 27001	ABSENTE
HDS	ABSENTE

5. Ce que nous demandons

À la CNIL

- **Contrôler PanneauPocket** (14 000 collectivités) : Google Ads AW-17989696875 dans le code source, « 0% Publicité » = pratique commerciale trompeuse + violation RGPD
- **Contrôler l'app Mémento des Élus** : Facebook SDK non déclaré, CGU mensongères
- **Contrôler les ~200 sites WeeCity** : 0 DPO sur 26 audités, Matomo sans consentement, template 1978
- **Informers les maires** qu'ils sont responsables de traitement et que leur prestataire les met en infraction sans leur dire

À l'ANSSI

- **Exiger le retrait du terme « Cloud Souverain »** en l'absence de SecNumCloud
- **Alerter les collectivités** sur les défauts de sécurité (HSTS 600s, 0 CSP, 0 Referrer-Policy)
- **Vérifier la sécurité** d'un groupe qui gère les données d'état civil et les listes électorales sans aucune certification

À la DGCCRF

- **Enquêter sur « 100% Anonyme, 0% Publicité »** : Google Ads (AW-17989696875) + 9 domaines publicitaires US dans le container GTM (Facebook, DoubleClick, Google AdSense, YouTube) = ni anonyme ni sans publicité. Vérifiable en 30 secondes.
- **Vérifier « Cloud Souverain »** : allégation commerciale trompeuse au sens de l'art. L121-2 du Code de la consommation

Ce signalement est un acte de protection citoyenne

Les données d'état civil, les listes électorales, les cadastres et les services sociaux de **plus de 14 000 collectivités françaises** sont gérés par un groupe qui envoie les données de ses utilisateurs à Google et Facebook sans leur dire, qui n'a aucune certification de sécurité, et

qui déclare un faux hébergeur dans les mentions légales de ses clients. Les maires ne le savent pas. Les citoyens ne le savent pas. **Maintenant, vous le savez.**

Pièces justificatives détaillées

Chaque dossier ci-dessous détaille les constats, la méthodologie, les sources et les preuves complètes.

1 Dossier JVS Group / Citopia / PanneauPocket

17 sections • 26 sites audités • Organigrammes • BASTRA FI 19,2 M€ • DRACKARYS 16 M€ • Vatry 422 M€ • BNP Paribas Panama Papers • 1 141 lignes

2 Dossier Duopole JVS + Berger-Levrault

17 sections • 25 sites BL audités • 5 couches de holdings • 7 liens croisés • CRC Vosges • Oaklins • Numeum • 1 106 lignes

3 Dossier Berger-Levrault

Structure capitalistique • 25 sites audités • Vendor lock-in • Conformité RGPD • Tarification • Lobbying

4 Organigramme complet JVS Group

Chaîne de propriété • 4 LBO • Patrimoine • SCI • Diagrammes interactifs

5 Audit JVS — version originale

Première version du dossier technique JVS

M. V. — Lanceur d'alerte (loi n°2022-401 du 21 mars 2022)

Pièces justificatives disponibles : code source HTML, headers HTTP, WHOIS, binaire app Mémento.

Toute divulgation de l'identité du lanceur d'alerte est passible de 2 ans d'emprisonnement et 30 000 € d'amende (art. 9 loi 2022-401).

Dernière vérification technique : 8 avril 2026