

## Politique de sécurité des données personnelles — Flyerspots (MàJ)

**Version : 1.1 — Date :** le 24 septembre 2025

**Périmètre :** Plateforme Flyerspots (Web/App), réseau social « Le Village », systèmes et prestataires associés (Webflow, Bubble, Brevo).

### 1. Gouvernance & rôles

- **Responsable de traitement :** ANGIEL MEDIA.
- **Référent RGPD / DPO :** Monsieur Guillaume COURSIN (hello@angiel-media.com).
- **RSSI (référent sécurité) :** Monsieur Guillaume COURSIN.
- **Sous-traitants clés :**
  - **Webflow** (front/hébergement du site) — DPA & politique de confidentialité publiés ; transferts encadrés (SCC). [Webflow+2Webflow+2](#)
  - **Bubble** (back-office/base de données) — DPA, page sécurité & conformité (SOC 2 Type II mentionné) ; guide RGPD (SCC). [Bubble+3Bubble+3Bubble+3](#)
  - **Brevo / Sendinblue** (emailing & SMS) — conformité RGPD, DPA accessible via les CGU/aide. [Brevo Help+2Brevo+2](#)

Nous conservons les DPA signés et la **liste des sous-traitants** à jour dans notre Registre RGPD.

### 2. Principes directeurs

- **Privacy & Security by design/by default, minimisation, besoin d'en connaître.**
- **Encadrement des transferts :** SCC + mesures complémentaires si nécessaire (chiffrement, évaluation de transfert). [Webflow+1](#)

### 3. Contrôles d'accès & identité

- **RBAC** (rôles minimaux) sur Webflow, Bubble, Brevo ; **MFA obligatoire** pour comptes d'admin.
- **Revue trimestrielle** des droits ; retrait immédiat à la sortie d'un intervenant.

### 4. Chiffrement & protection

- **En transit :** TLS 1.2+ (prestataires).
- **Au repos :** chiffrement géré par les prestataires ; secrets en coffre-fort.
- **Sauvegardes :** chiffrées, tests de restauration planifiés.

### 5. Développement & qualité (Bubble)

- Intégration des exigences sécurité dans le cycle de dev ; revues de modifications ; environnements **dev/test/prod** strictement séparés.
- **Données de test** pseudonymisées ; jamais de données prod brutes en test.

- Référence aux pratiques et garanties de Bubble (sécurité/ conformité) au niveau plateforme. [Bubble](#)

## 6. Journalisation & supervision

- **Logs d'accès/événements** sur Webflow/Bubble/Brevo ; conservation des logs sécurité jusqu'à 12 mois (principe).
- Alertes en cas d'activités anormales (authentifications échouées, pics d'erreurs).

## 7. Gestion des vulnérabilités

- Veille (éditeurs/CERT), inventaire des dépendances.
- **Correctifs critiques ≤ 7 jours** (ou mesures compensatoires) ; élevés ≤ 30 jours.
- Scans périodiques ; pentest selon criticité.

## 8. Prestataires & transferts

- **DPA** signés avec Webflow, Bubble, Brevo ; **SCC** pour transferts hors UE/EEE quand applicables ; **TIA** documentée. [Webflow+2Bubble+2](#)
- Revue annuelle des politiques/certifications des prestataires ; sous-sous-traitance encadrée.

## 9. Marketing — Email/SMS (Brevo)

- **Opt-in distinct** par thématique ; **double opt-in** recommandé.
- **STOP** obligatoire pour SMS ; **désinscription 1 clic** pour emails ; **preuve des consentements** (horodatage) conservée. [Brevo Help](#)

## 10. Cookies & traceurs

- **CMP** avec **Accepter / Refuser / Personnaliser** au même niveau ; pas de traceurs non essentiels avant consentement.
- Preuve de consentement et lien **“Gérer mes cookies”** accessible à tout moment.

## 11. Cycle de vie & minimisation

- Collecte limitée au nécessaire ; cloisonnement CAPA/Coach/Invités.
- **Conservation** (référentiel) : comptes inactifs ≤ 3 ans ; logs sécurité ≤ 12 mois ; marketing = jusqu'au retrait du consentement.
- Suppression/anonymisation à échéance, y compris dans les sauvegardes quand faisable.

## 12. Continuité d'activité

- **RPO cible ≤ 24 h ; RTO cible 24–48 h** (à confirmer selon services).
- PCA/PRA testés annuellement.

## 13. Travail à distance & postes

- Postes durcis (chiffrement disque, anti-malware, pare-feu).

- Accès consoles via VPN/TLS + **MFA** ; interdiction d'exports nominatifs sur appareils non gérés.

#### 14. Sensibilisation & formation

- Parcours **onboarding sécurité/RGPD** ; refresh annuel (phishing, mots de passe, data minimization).

#### 15. Réponse aux incidents (72 h)

- **Triage** (gravité/périmètre/données/volume), **confinement**, rotation des secrets, journal d'incident.
- **Notification CNIL ≤ 72 h** si risque ; **information des personnes** sans délai injustifié si risque élevé (message clair + conseils).
- Bilan post-incident (actions correctives).

#### 16. Exercice des droits & demandes légales

- **Canal unique** : hello@angiel-media.com — réponse ≤ 1 mois (prorogeable si complexe).
- Vérification d'identité proportionnée ; traçabilité (ticketing).

#### 17. IA & contenus générés

- Pas de décision automatisée à effets juridiques sans base légale et garanties.
- **Filtrage** des prompts/datasets pour éviter l'ingestion de données perso non nécessaires.

#### 18. Audit & amélioration continue

- Audits internes/externes (sécurité/RGPD) planifiés ; **KPIs** (taux MFA, délais de patch, incidents, restauration).
- Revue de direction semestrielle.

#### 19. Entrée en vigueur & mises à jour

- Cette politique remplace la version 1.0.
- Révision au moins annuelle et à chaque évolution majeure (traitements, risques, prestataires).
- Historique des versions conservé.