



N° _____/N/MINEPAT/SG/DI/SMI/eojis

Yaoundé le,

NOTE

A

**la haute attention de Monsieur le Ministre de l'Economie,
de la Planification et de l'Aménagement du Territoire
-Yaoundé-**

Objet : Signalement de la plateforme <https://minepat-cm.org/> non conforme à la circulaire N°007/CAB/PM du 23 août 2000 et aux directives internes du MINEPAT

Monsieur le Ministre,

J'ai l'honneur de vous alerter sur une situation critique relative à la plateforme <https://minepat-cm.org/>, dont la configuration actuelle contrevient à la circulaire N°007/CAB/PM du 23 août 2000 et aux directives internes du MINEPAT, notamment en matière de souveraineté numérique et de sécurité des données.

Contexte réglementaire

La circulaire du Premier Ministre impose :

1. L'hébergement des sites gouvernementaux sous le domaine « **.gov.cm** » et sur des infrastructures nationales supervisées par les services compétents.
2. Le respect du bilinguisme institutionnel (français/anglais).
3. La validation préalable par la Division Informatique de tout projet numérique ministériel.

Irrégularités identifiées

La plateforme incriminée présente les manquements suivants :

1. Non-conformité procédurale

La création de cette plateforme a contourné la Division Informatique, pourtant mandatée pour piloter les projets numériques. Cette exclusion compromet l'harmonisation des outils technologiques du ministère et viole l'article 4 de la circulaire.

2. Risques liés à la non-souveraineté des données

L'hébergement de la plateforme en dehors des serveurs gouvernementaux camerounais soulève des enjeux majeurs :

- **Exposition juridique** : Les données sensibles (informations administratives, projets stratégiques) sont soumises aux législations étrangères (ex : *Cloud Act* américain ou *RGPD européen*), permettant à des entités externes d'y accéder légalement.
- **Perte de contrôle** : L'absence de maîtrise des infrastructures d'hébergement limite la capacité du MINEPAT à auditer, sécuriser ou récupérer les données en cas de crise.
- **Vulnérabilité géopolitique** : Une dépendance à des hébergeurs étrangers expose le ministère à des risques de blocage technique ou de censure en cas de tensions diplomatiques.

3. Sécurité déficiente

L'externalisation de l'hébergement accroît les risques de :

- **Cyberattaques ciblées** (ransomware, phishing) en raison de protocoles de sécurité non conformes aux normes gouvernementales.
- **Falsification de contenu**, nuisant à l'intégrité des informations publiées.
- **Fuites de données** sensibles, avec des conséquences potentielles sur la confidentialité des projets d'État.

4. Atteinte à la crédibilité institutionnelle

- **Domaine non officiel** (.org au lieu de .gov.cm) : crée la confusion entre une plateforme gouvernementale et une initiative privée ou associative, érodant la confiance des citoyens et partenaires.
- **Non-respect du bilinguisme** : Certaines sections de la plateforme ne sont pas disponibles en anglais, en contradiction avec l'article 3 de la circulaire.

5. Fragmentation de la stratégie numérique nationale

Cette initiative parallèle sape les efforts de modernisation de l'administration publique, en créant un précédent dangereux pour l'harmonisation des systèmes d'information étatiques.

Recommandations urgentes

1. **Audit technique et juridique** de la plateforme pour évaluer sa conformité et identifier les données exposées.
2. **Migration immédiate** vers un domaine **.gov.cm** hébergé sur des serveurs nationaux sécurisés (ex : infrastructure certifiée par l'ANTIC).
3. **Implication obligatoire de la Division Informatique** pour :
 - Garantir le respect des normes techniques et linguistiques.
 - Mettre en place des protocoles de sécurité conformes aux standards nationaux (ex : chiffrement AES-256, sauvegardes locales).
4. **Sensibilisation interne** sur les enjeux de souveraineté numérique et les procédures à suivre pour tout projet informatique.

Je vous prie de croire, Monsieur le Ministre, en l'assurance de ma haute considération.

Ing. ESSONGO OHANDJA Joël Stéphane
Cadre, SMI/DI