Procédure d'exercice des droits des personnes concernées

Articles 21 à 25 — Loi N° 2013-450

Honoré DEMBÉLÉ · Ingénieur d'État · Expert Industriel Assermenté Mali · DPO
Cocody Riviera M'BADON-M'POUTO, Lot 117 et 119, Abidjan · dpo@pixelakwaba.com · +225 05 00 21 67 67

Document opérationnel, tenu par le DPO, applicable à tout utilisateur souhaitant exercer ses droits sur ses données personnelles. **Base légale** : articles 21 à 25 de la Loi N° 2013-450 du 19 juin 2013.

---

1. Objet de la procédure

Décrire le processus complet par lequel un utilisateur d'Akwaba AI peut exercer l'un des droits suivants :

Droit	Article Loi 2013-450
Information préalable	Article 21
Accès aux données	Article 22
Rectification	Article 23
Opposition	Article 24
Effacement	Article 25
Portabilité	Bonne pratique (RGPD-équivalent)
Limitation	Bonne pratique (RGPD-équivalent)

---

2. Canal unique de réception

Toute demande d'exercice de droits doit être adressée à :

dpo@pixelakwaba.com

Subsidiairement, des canaux secondaires sont acceptés : - Email à `support@pixelakwaba.com` (sera redirigé au DPO) - Bouton "Exporter mes données" dans l'application mobile (droit d'accès) - Bouton "Supprimer mon compte" dans les réglages (droit d'effacement) - Courrier postal recommandé à : **DPO Akwaba AI, Cocody Riviera M'BADON-M'POUTO, Lot 117 et 119, Abidjan**

---

3. Vérification d'identité

Avant toute action, le DPO vérifie l'identité du demandeur pour éviter qu'une personne malveillante puisse exfiltrer ou supprimer les données d'un tiers.

3.1 Pour les demandes depuis l'application

L'utilisateur étant déjà authentifié (JWT actif), aucune vérification supplémentaire n'est requise.

3.2 Pour les demandes par email externe

Le DPO demande au requérant : 1. Une **copie de sa pièce d'identité** (CNI, passeport, permis) 2. Une **confirmation du numéro de téléphone associé au compte** (via réception d'un OTP envoyé par le DPO sur ce numéro)

Cette double vérification est **obligatoire** pour les demandes d'accès, de rectification d'éléments sensibles et d'effacement.

3.3 Cas particulier – Demande au nom d'un tiers

Sont acceptés : - **Représentant légal** (parent pour un mineur, tuteur, curateur) : copie de l'acte de représentation + pièce d'identité du représentant - **Avocat** : pouvoir signé par le requérant + carte professionnelle d'avocat - **Héritier** (en cas de décès) : copie de l'acte de décès + acte de notoriété successorale

---

4. Traitement des demandes par type

4.1 Demande d'accès (art. 22)

Délai de réponse : 30 jours maximum à compter de la réception de la demande validée.

Processus : 1. DPO vérifie l'identité (cf. §3) 2. DPO génère un export JSON via le script `/opt/akwaba/api/scripts/export_user_data.py` (à créer) 3. L'export contient TOUTES les données associées au compte : - Profil (nom, téléphone, code09, pseudo, etc.) - Historique des courses - Historique des paiements - Notations émises et reçues - Signalements émis - Messages échangés - Logs d'audit le concernant 4. Envoi de l'export par email chiffré à l'adresse du requérant (avec mot de passe transmis par autre canal – SMS) 5. Conservation d'une copie du fichier exporté pendant 12 mois pour preuve de la communication

Format de l'export : JSON + PDF lisible (généré automatiquement).

4.2 Demande de rectification (art. 23)

Délai de réponse : 7 jours maximum.

Processus : 1. DPO vérifie l'identité 2. DPO vérifie la véracité de la rectification demandée (justificatif requis pour changements sensibles : nouvelle CNI, justificatif de domicile, etc.) 3. DPO modifie la donnée en base via requête SQL ciblée, tracée dans `audit_log` 4. Confirmation par email au requérant 5. Notification aux destinataires de la donnée erronée si pertinent

4.3 Demande d'opposition (art. 24)

Délai de réponse : 7 jours maximum.

Cas typiques : - Désinscription des newsletters → désactivation immédiate du flag `marketing_consent` - Désactivation des notifications push promotionnelles → flag `push_promotional` à FALSE - Refus du profilage statistique → flag `analytics_optout` à TRUE

Processus : 1. DPO vérifie l'identité (ou autorisation directe via l'app) 2. DPO modifie les préférences en base 3. Confirmation par email

4.4 Demande d'effacement (art. 25)

Délai de réponse : 30 jours maximum.

Processus : 1. DPO vérifie l'identité (double vérification CNI + OTP téléphone) 2. DPO vérifie qu'il n'y a **aucune obligation légale** s'opposant à la suppression : - Transactions financières en cours (< 10 ans) → conservation des données comptables uniquement, anonymisation du reste - Litige en cours → conservation sous séquestre pendant la procédure - Documents KYC chauffeur < 2 ans après dernière activité → conservation obligation transport 3. Suppression des données via script `/opt/akwaba/api/scripts/delete_user_data.py` : - Suppression hard des données non soumises à obligation - Anonymisation (remplacement par UUID) des données soumises à obligation 4. Anonymisation des entrées de l'utilisateur dans les logs (remplacement du téléphone par hash) 5. Suppression du compte dans le Pixel AI Hub (cross-app) 6. Notification au requérant par email 7. Conservation d'une **preuve d'effacement** dans `audit_log` pendant 10 ans

4.5 Demande de portabilité

Délai de réponse : 30 jours maximum.

Identique à la demande d'accès (§4.1) mais avec format machine-lisible standardisé (JSON Schema documenté).

4.6 Demande de limitation

Délai de réponse : 7 jours maximum.

Cas typique : utilisateur contestant l'exactitude de ses données, demandant le gel du traitement le temps de la vérification.

Processus : 1. Marquage du compte avec flag `processing_restricted` = TRUE 2. Le compte reste accessible en lecture par l'utilisateur mais n'est plus utilisé pour les finalités contestées 3. Levée du gel après résolution de la contestation

---

5. Refus motivé

Une demande peut être refusée par le DPO uniquement si :

- L'identité du requérant **n'est pas vérifiée** après deux relances
- La demande est **manifestement infondée ou excessive** (art. 25-3) — par exemple, multiples demandes répétitives en moins de 12 mois
- L'exécution porterait atteinte aux **droits d'un tiers** (par exemple, une demande d'effacement de l'historique des courses effacerait aussi les notations laissées au chauffeur, ce qui nécessite anonymisation et non suppression)
- Une **obligation légale** s'y oppose (conservation comptable, KYC transport)

Tout refus est : - **Motivé par écrit** au requérant - **Notifié** dans le délai de réponse standard - **Accompagné de la mention** du droit d'introduire une réclamation auprès de l'Autorité de Protection des Données (ARTCI)

---

6. Documentation et traçabilité

Toutes les demandes d'exercice de droits sont consignées dans un registre interne :

Champ	Détail
Date de réception	Date et heure
Identité du requérant	Nom, téléphone, code09
Type de droit invoqué	Accès / Rectification / Opposition / Effacement / Portabilité / Limitation
Canal d'arrivée	Email / App / Postal / Téléphone
Date de réponse	Date d'envoi de la réponse
Issue	Acceptée / Refusée (motif) / En cours
Actions effectuées	Description
Document de preuve	Lien vers export, capture de la modification, etc.

Ce registre est tenu dans la table SQL `dpo_requests_log` (à créer) et conservé pendant **10 ans**.

---

7. Notification de violation de données (art. 38)

En cas de **violation de données** (accès non autorisé, fuite, destruction accidentelle) :

1. **Détection** : analyse continue des logs + alertes fail2ban + audit des accès admin
2. **Évaluation** : le DPO évalue dans les **24 heures** la gravité (volume de données concernées, sensibilité, risque pour les personnes)

3. **Notification à l'autorité** : si risque élevé, notification écrite à l'Autorité de Protection sous **72 heures** maximum à compter de la prise de connaissance
4. **Notification aux personnes concernées** : si risque élevé pour leurs droits, notification individuelle par email + SMS + push notification
5. **Mesures correctives** : isolation du système compromis, rotation des secrets, déploiement de correctifs, communication publique si pertinent
6. **Documentation** : tenue d'un registre des violations dans `dpo_breach_register` (table à créer), conservé 10 ans

Modèle de notification à l'autorité :

```
Objet : Notification de violation de données - Akwaba AI - <<<DATE>>>
À : <<<adresse email autorité>>>

Madame, Monsieur,

Conformément à l'article 38 de la Loi N° 2013-450, je vous informe par la
présente d'une violation de données à caractère personnel survenue le
<<<DATE>>> à <<<HEURE>>> et détectée le <<<DATE DÉTECTION>>>.

1. Nature de la violation : <<<accès non autorisé / fuite / destruction>>>
2. Catégories de personnes concernées : <<<précisément>>>
3. Nombre approximatif : <<<X>>>
4. Catégories de données : <<<précisément>>>
5. Conséquences probables : <<<analyse>>>
6. Mesures prises : <<<actions correctives>>>
7. Mesures préventives futures : <<<roadmap>>>

Le DPO se tient à votre disposition pour tout complément d'information.

Honoré DEMBÉLÉ
DPO Akwaba AI
dpo@pixelakwaba.com
+225 05 00 21 67 67
```

---

8. Auto-évaluation annuelle

Le DPO procède chaque année (1er février) à une auto-évaluation de la mise en œuvre de la présente procédure :

- Nombre de demandes traitées par type
- Délai moyen de réponse
- Taux de refus motivé
- Nombre de violations notifiées
- Améliorations apportées

Un rapport synthétique est conservé en interne et présenté à l'Autorité de Protection sur demande.

---

9. Mise à jour de la présente procédure

Toute modification substantielle de la présente procédure est : - Approuvée par le responsable de traitement (Honoré DEMBÉLÉ) - Notifiée à l'Autorité de Protection (déclaration modificative) - Publiée sur https://pixelakwaba.com/privacy.html - Notifiée aux utilisateurs si elle restreint leurs droits

---

Procédure rédigée le 30 mai 2026, v1.0. Prochaine révision : 30 mai 2027.