

POLITIQUE DE GOUVERNANCE

Gouvernance des données et confidentialité

Politique opérationnelle - consentement, accès, conservation, sécurité et droits

Statut	Édition consolidée - validation juridique et formalités locales requises avant production
Édition	Consolidée
Audience	Direction, responsable données, opérations, équipe terrain, partenaires et conseil juridique
Édition	12 juillet 2026

Confidentiel - diffusion contrôlée

Les objectifs et hypothèses ne doivent pas être présentés comme des résultats obtenus.

Gouvernance des données et confidentialité

Un cadre de contrôle destiné au pilote - à faire valider par un conseil qualifié et par les autorités compétentes lorsque requis.

100 % consentements traçables	Finalité définie avant collecte	Minimum de données nécessaires
Filtré partage partenaire	Révocable autorisation d'accès	72 h objectif interne de triage incident

	Statut du document Ce document organise les contrôles internes. Il ne constitue pas un avis juridique et ne remplace ni l'analyse de la loi sénégalaise applicable, ni les formalités auprès de la Commission de protection des données personnelles, ni les clauses contractuelles définitives.
--	--

Table des matières

Section	Page
1. Objet et principes directeurs	2
2. Cadre juridique et décisions préalables	2
3. Gouvernance et responsabilités	3
4. Registre des traitements	3
5. Catalogue et classification des données	4
6. Consentement et preuve du choix	4
7. Accès interne et partage partenaire	5
8. Conservation, archivage et suppression	5
9. Droits et demandes des personnes	5
10. Sécurité minimale du pilote	6
11. Gestion des incidents	6
12. Analyse d'impact et lancement	7
13. Indicateurs de conformité	7
14. Annexes à maintenir	7
15. Sources et limites	7

1. Objet et principes directeurs

Déggal traite des informations permettant de décrire et de vérifier une activité économique. Même lorsqu'une information semble banale, son association à une personne, un lieu, une photo, un numéro ou une transaction peut créer un risque. Le dispositif doit donc être conçu autour de la finalité, de la proportionnalité, du contrôle par la personne et de la traçabilité.

Principe	Règle Déggal	Preuve de contrôle
Finalité	Chaque champ, preuve et partage répond à un objectif documenté.	Catalogue des données et fiche de traitement.
Minimisation	Ne collecter que ce qui est nécessaire au cas d'usage approuvé.	Formulaire versionné et revue de champs.
Transparence	Expliquer simplement la collecte, l'usage, la durée et les destinataires.	Notice et script dans la langue comprise.
Choix	Séparer le consentement à la collecte du consentement à chaque partage.	Journal horodaté des choix.
Exactitude	Distinguer déclaration, observation, pièce et confirmation externe.	Niveau de preuve et date de vérification.
Sécurité	Limiter l'accès selon le rôle et protéger les supports.	Registre d'accès, authentification et revue périodique.
Durée limitée	Conserver selon une règle approuvée et supprimer ou anonymiser à échéance.	Calendrier de conservation et preuve de suppression.
Responsabilité	Attribuer un propriétaire à chaque traitement et incident.	Matrice RACI, registre des décisions et audits.

2. Cadre juridique et décisions préalables

Le Sénégal dispose d'un cadre relatif à la protection des données à caractère personnel, notamment la loi n° 2008-12 du 25 janvier 2008 et une autorité de contrôle dédiée. La version en vigueur des textes, la qualification exacte des rôles, les formalités applicables et les règles sectorielles doivent être confirmées avant toute collecte réelle.

Décision	Question à trancher	Responsable	Échéance
Porteur de traitement	Quelle personne morale détermine les finalités et moyens?	Direction + conseil juridique	Avant contrat et collecte.
Base de traitement	Le consentement est-il suffisant pour chaque finalité ou une autre base s'applique-t-elle?	Conseil juridique	Avant formulaire final.
Formalités CDP	Déclaration, autorisation, consultation ou autre démarche?	Responsable données + conseil	Avant mise en production.
Sous-traitants	Quels hébergeurs, outils, messageries et prestataires accèdent aux données?	Technologie + juridique	Avant activation.
Transferts	Des données sortent-elles du Sénégal ou de la zone autorisée?	Technologie + juridique	Avant choix d'hébergement.
Données sensibles	Certains champs ou preuves reçoivent-ils une protection renforcée?	Juridique + produit	Avant catalogue V1.
Conservation	Quelles durées sont nécessaires par finalité et obligation?	Juridique + opérations	Avant ouverture du pilote.

Sénégal - loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel - texte à vérifier dans sa version en vigueur. Commission de protection des données personnelles du Sénégal: <https://www.cdp.sn/>

3. Gouvernance et responsabilités

Rôle	Responsabilités minimales	Droit de décision
Direction	Approuve finalités, risques acceptés, budget, contrats et réponse aux incidents majeurs.	Suspendre un traitement ou un partenaire.
Responsable données	Tient les registres, contrôle accès et conservation, coordonne les droits et incidents.	Bloquer un partage non conforme.
Responsable opérations	S'assure que les scripts, formulaires et pratiques terrain suivent la politique.	Retirer un agent ou une zone du pilote.
Produit / technologie	Met en œuvre les contrôles, journaux, sauvegardes, tests et correctifs.	Désactiver une fonctionnalité risquée.
Back-office QA	Contrôle exactitude, complétude, niveau de preuve et consentement.	Refuser ou renvoyer un dossier.
Agent terrain	Informe, recueille les choix, minimise la collecte et signale les anomalies.	Arrêter une visite en cas de doute.
Partenariats	Documente la finalité, l'étendue et la durée de chaque accès.	Aucun accès direct sans validation données.
Conseil juridique	Valide les documents, contrats, formalités et réponses réglementaires.	Avis requis pour les cas à risque élevé.

Séparation obligatoire

La personne qui négocie un partenariat ne doit pas pouvoir ouvrir seule l'accès aux dossiers. La validation du responsable données et la présence d'un consentement correspondant sont exigées.

4. Registre des traitements

Chaque traitement reçoit un identifiant, un propriétaire, une finalité, une liste de données, une catégorie de personnes, une base à confirmer, des destinataires, une durée, des mesures de sécurité et une date de revue.

ID	Traitement	Finalité	Données principales	Destinataires	Statut
T-01	Préinscription marchand	Planifier et éviter les doublons.	Nom usuel, contact choisi, zone, activité.	Opérations.	À valider.
T-02	Création de passeport	Documenter l'activité avec preuves proportionnées.	Déclarations, observations, photo ou pièce choisie.	QA et marchand.	Pilote.
T-03	Partage partenaire	Répondre à une finalité et une demande précises.	Vue filtrée et métadonnées de preuve.	Partenaire autorisé.	Au cas par cas.
T-04	Mesure qualité	Améliorer le processus et détecter les erreurs.	Statuts, délais, motifs de reprise.	Direction et opérations.	Interne.
T-05	Gestion des droits	Répondre à une demande d'accès, correction ou retrait.	Identité de vérification, demande, décision.	Responsable données.	Obligatoire.
T-06	Gestion incident	Contenir, analyser et remédier.	Journal technique, personnes concernées, actions.	Cellule incident et conseil.	Obligatoire.

5. Catalogue et classification des données

Classe	Exemples	Règle d'accès	Partage
C0 - Public / institutionnel	Description générale du service, méthodologie publiée.	Large, après validation communication.	Autorisé.
C1 - Interne	Planning, KPI agrégés, procédures, zones.	Équipe selon besoin.	Seulement agrégé.
C2 - Personnel courant	Nom, téléphone choisi, activité, localisation approximative.	Rôle habilité et journalisé.	Filtré et finalisé.
C3 - Personnel à risque élevé	Photo identifiable, pièce, coordonnées précises, transaction ou référence.	Accès restreint, justification et protection renforcée.	Exceptionnel et explicite.
C4 - Interdit au pilote	PIN, mot de passe, code mobile money, solde, accès complet au téléphone.	Aucun.	Jamais.

Données interdites

L'équipe ne demande jamais un PIN, un mot de passe, un code à usage unique, un solde, une copie de carnet d'adresses ou un accès général au téléphone. Toute apparition accidentelle doit être masquée ou supprimée selon la procédure d'incident.

6. Consentement et preuve du choix

Le consentement doit être libre, spécifique, éclairé et traçable. Il n'est pas obtenu par défaut, ne doit pas être présenté comme une condition d'accès à un financement hypothétique et peut être retiré selon la procédure communiquée.

Moment	Information minimale	Trace attendue
Avant collecte	Identité de Déggal, but, caractère volontaire, données envisagées, risques et contact.	Version de notice, langue, date, agent et choix.
Avant photo / audio	Utilité précise, caractère facultatif et alternative.	Case distincte ou trace orale approuvée.
Avant partage	Partenaire, finalité, champs, durée et conséquence du refus.	Autorisation distincte avec expiration.
Après modification	Nouveau champ, nouveau destinataire ou nouvelle finalité.	Nouveau consentement, pas une extension tacite.
Retrait	Canal, délai et effets sur les partages futurs.	Ticket, décision, révocation et confirmation.

1. Expliquer en langage simple et dans la langue comprise.
2. Faire reformuler la personne pour vérifier la compréhension.
3. Présenter chaque catégorie de preuve comme un choix séparé.
4. Enregistrer la version du formulaire et l'identité de l'agent.
5. Remettre un identifiant ou un moyen de retrouver la demande.
6. Ne poursuivre que si le choix est clair; sinon arrêter.

7. Accès interne et partage partenaire

Contrôle	Exigence	Fréquence
Moindre privilège	Accès limité au rôle et au portefeuille assigné.	À la création et à chaque changement de poste.
Authentification	Compte individuel; aucune identité partagée.	Permanent.
Journalisation	Ouverture, téléchargement, modification, partage et retrait.	Automatique ou registre contrôlé.
Expiration	Accès partenaire avec date de fin et révocation.	Pour chaque autorisation.
Revue	Liste des utilisateurs, droits et accès dormants.	Mensuelle au pilote.
Export	Justification, format minimal, chiffrement et destinataire.	Avant chaque export.
Partage secondaire	Interdit sauf clause, finalité et nouveau consentement applicables.	Permanent.

Vue partenaire

Le partenaire reçoit une vue créée pour son cas d'usage - jamais le dossier brut par défaut. La vue affiche les faits, leur date, leur niveau de preuve et les limites d'interprétation.

8. Conservation, archivage et suppression

Les durées ci-dessous sont des propositions opérationnelles et non des conclusions juridiques. Elles doivent être validées avant usage.

Catégorie	Durée proposée	Déclencheur	Fin de cycle
Dossier incomplet sans consentement valide	7 jours maximum.	Création du brouillon.	Suppression sécurisée.
Dossier pilote actif	Durée du pilote + 90 jours.	Validation du dossier.	Revue, renouvellement ou suppression.
Autorisation de partage	Durée indiquée, maximum pilote proposé de 90 jours.	Activation de l'accès.	Révocation automatique.
Journal d'accès	12 mois proposés.	Événement journalisé.	Archivage ou suppression selon avis.
Incident	Selon obligations et besoins de preuve.	Ouverture de l'incident.	Décision juridique documentée.
KPI agrégés / anonymisés	Selon utilité démontrée.	Agrégation contrôlée.	Revue annuelle.

9. Droits et demandes des personnes

Demande	Étapes	Délai interne cible	Escalade
Accès	Authentifier proportionnellement, rechercher, relire les tiers, répondre.	15 jours.	Juridique si conflit.
Correction	Vérifier la preuve, modifier sans effacer l'historique, confirmer.	7 jours.	QA si preuve contestée.
Retrait du consentement	Enregistrer, bloquer futurs accès, révoquer, informer les destinataires.	48 heures.	Direction si impact contractuel.

Demande	Étapes	Délai interne cible	Escalade
Suppression	Qualifier obligations, suspendre partage, supprimer ou expliquer la limite.	15 jours.	Juridique.
Opposition / restriction	Geler le traitement concerné pendant analyse.	48 heures.	Responsable données.
Réclamation	Accuser réception, enquêter, remédier et informer des voies disponibles.	2 jours ouvrés.	Direction + conseil.

10. Sécurité minimale du pilote

Domaine	Mesure minimale	Preuve
Terminaux	Verrouillage, mise à jour, chiffrement lorsque disponible, inventaire.	Registre des appareils.
Comptes	Comptes nominatifs, mot de passe robuste, MFA si disponible.	Liste et revue d'accès.
Collecte hors ligne	Stockage temporaire limité et synchronisation contrôlée.	Journal de synchronisation.
Transfert	Canal approuvé; pas de messagerie personnelle ni clé non inventoriée.	Procédure et logs.
Stockage	Dossiers séparés, contrôle d'accès, sauvegarde testée.	Rapport de test.
Exports	Minimisés, nommés, expirables et supprimés après usage.	Registre d'export.
Supports papier	Numérotés, sous clé, remis et détruits de manière contrôlée.	Bordereau.
Prestataires	Évaluation, clause de sécurité, accès minimal et fin de contrat.	Fiche fournisseur.

11. Gestion des incidents

7. Détecter et protéger - arrêter le partage, isoler l'appareil ou le compte, ne pas effacer les traces.
8. Alerter - contacter immédiatement le responsable données et le responsable opérations.
9. Trier - évaluer nature, volume, sensibilité, personnes, exposition et continuité.
10. Contenir - révoquer les accès, changer les secrets, récupérer le support ou bloquer l'export.
11. Analyser - établir la chronologie, la cause, les obligations et les mesures correctives.
12. Notifier - suivre l'avis juridique et les exigences applicables envers personnes, partenaires ou autorité.
13. Clôturer - documenter les preuves, le retour d'expérience et l'efficacité des actions.

Sévérité	Exemple	Action immédiate
S1 - Faible	Erreur interne sans accès externe et donnée peu sensible.	Corriger, tracer et revoir.
S2 - Modérée	Dossier envoyé au mauvais collègue ou support temporairement perdu.	Confinement, responsable données, analyse sous 24 h.
S3 - Élevée	Accès partenaire non autorisé, photo ou transaction exposée.	Cellule incident, direction et conseil.
S4 - Critique	Exposition large, exploitation malveillante ou danger physique.	Suspension, réponse de crise et autorités selon avis.

12. Analyse d'impact et lancement

Avant le pilote, Dëggal doit mener une analyse structurée des risques sur les personnes. Une analyse d'impact approfondie doit être envisagée lorsque la nature, le volume, le suivi, les croisements, la vulnérabilité des personnes ou la sensibilité des preuves augmentent le risque.

Question de lancement	Critère de passage
La personne morale et les rôles sont-ils confirmés?	Oui, documents et responsables nommés.
Le registre des traitements est-il validé?	Finalité, champs, base, destinataires et durées approuvés.
Les formalités et avis juridiques sont-ils complétés?	Preuves archivées avant collecte.
Les formulaires sont-ils compréhensibles?	Test utilisateur et script validés.
Les accès et journaux fonctionnent-ils?	Test de bout en bout et révocation réussie.
Une demande de droit peut-elle être traitée?	Exercice simulé concluant.
Un incident peut-il être contenu?	Exercice de table et contacts actifs.
Les prestataires sont-ils contrôlés?	Inventaire et clauses approuvés.

13. Indicateurs de conformité

Indicateur	Calcul	Seuil pilote
Consentements traçables	Dossiers avec consentement valide / dossiers collectés.	100 %.
Partages conformes	Partages avec finalité, consentement et expiration / partages.	100 %.
Accès revus	Comptes revus / comptes actifs.	100 % mensuel.
Délai de retrait	Temps médian entre demande et blocage.	< 48 h cible.
Données interdites	Incidents impliquant une donnée interdite.	0.
Incidents ouverts	Nombre par sévérité et ancienneté.	Aucun S3/S4 non contenu.
Suppression à échéance	Objets supprimés ou anonymisés / objets arrivés à échéance.	100 %.

14. Annexes à maintenir

- Registre des traitements et catalogue de données.
- Matrice des accès et registre des utilisateurs.
- Journal des consentements et des partages.
- Calendrier de conservation et certificats de suppression.
- Registre des incidents, demandes et décisions.
- Inventaire des fournisseurs et transferts.
- Versions des notices, scripts et formulaires.
- Analyses de risques et comptes rendus de revue.

15. Sources et limites

Pack Dëggal reconstruit, version du 12 juillet 2026 - source interne. Sénégal - loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel - texte à vérifier dans sa version en vigueur. Commission de protection des données personnelles du Sénégal: <https://www.cdp.sn/> OHADA - actes uniformes applicables aux sociétés et aux contrats commerciaux: <https://www.ohada.org/> À valider juridiquement selon l'entité porteuse, les outils, les contrats et la version en vigueur des textes.