



SOCIETE TOGOLAISE DES EAUX SA

Siège Social : 53, Avenue de la Libération

B.P. 1301 - Tél. (+228) 2221 3481 - (+228) 2221 59 63 - Fax : (+228) 22 21 46 13.- Lomé -TOGO

SOCIETE TOGOLAISE DES EAUX S.A

MISE EN ŒUVRE DE LA CONFORMITE RELATIVE A LA LOI SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL DU TOGO

Phase 2 : Politique de la Protection des Données à Caractère Personne

Code:	2-PPDCP
Version :	1.0.0
Date de la version:	29-08-2022
Créé par:	e Chef Projet Consultant GCENT
Approuvé par :	
Niveau de confidentialité:	Faible

Comptes Bancaires :

UTB: 310044541004000 - BTCl : 010305905000192-54 - BIA- TOGO : 00136010775-23 - CCP : 6310009625001000-34

ECOBANK : 70102314073357 01 - ORABANK: 402 100 09725-35 - ORABANK SPECIAL : 402 100 18723-07

NSIA BANQUE : 223005939012-33 - BSIC : 020270600112

NIF 1000166680

:

Table des matières

DEFINITION DE SIGLES ET D'ACRONYMES.....	3
1. OBJET, CHAMP D'APPLICATION ET UTILISATEUR.....	4
2. DOCUMENTS DE REFERENCE.....	4
3. DÉFINITION.....	4
4. PRINCIPES DE BASE CONCERNANT LE TRAITEMENT DES DONNÉES PERSONNELLES.....	6
4.1. CONSENTEMENT ET LEGITIMITE.....	6
4.2. LICEITE ET TRANSPARENCE.....	6
4.3. DELIMITATION DES FINALITE.....	6
4.4. MINIMISATION DES DONNEES.....	6
4.5. EXACTITUDE.....	6
4.6. LIMITATION DE LA DUREE DE CONSERVATI.....	7
4.7. INTEGRITE ET CONFIDENTIALITE.....	7
4.8. RESPONSABILISATION.....	7
5. RENFORCER LA PROTECTION DES DONNÉES DANS LES ACTIVITÉS COMMERCIALES.....	7
5.1. INFORMATION AUX PERSONNES CONCERNEES.....	7
5.2. CHOIX ET CONSENTEMENT DE LA PERSONNE CONCERNEE.....	7
5.3. 5.3. COLLECTE DES DONNEES.....	7
5.4. UTILISATION, CONSERVATION ET SUPPRESSION	8
5.5. DIVULGATION A DESTIERS.....	9
5.6. TRANSFERT TRANSFRONTALIER DE DONNEES PERSONNEL.....	9
5.7. DROITS D'ACCES DES PERSONNES CON.....	9
5.8. PORTABILITE DES DONNEES.....	9
5.9. DROIT A L'OUBLI.....	10
6. LIGNES DIRECTRICES SUR LE TRAITEMENT TRANSPAREN.....	10
6.1. AVIS AUX PERSONNES CONCERNEES.....	10
6.2. OBTENTION DES CONSENTEMENTS.....	11
7. ORGANISATION ET RESPONSABILITÉS.....	11
8. RÉPONSE AUX INCIDENTS DE VIOLATION DE DONNÉES PERSONNELLES.....	13
9. AUDIT ET RESPONSABILITE.....	13
10. GESTION DES DOCUMENTS ISSUS DE CE DOCUMENT DE POLITIQUE.....	13
11. VALIDITÉ ET GESTION DU DOCUMENT.....	14

Définition de sigles et acronymes

- IPDCP : Instance sur la Protection des Données à Caractère Personnel
LPDCPT : Loi sur la Protection sur les Données à Caractères Personnel du Togo
CPD : Correspondant à la Protection des Données
RGPD : Règlement Général pour la Protection des Données (UE)
- PSSI : Politique de Sécurité du Système d'Information
RSSI • Responsable de la Sécurité du Système d'Information

1. Obiet, champ d'application et utilisateurs

La Société Togolaise des Eaux, ci-après dénommée la « TdE », s'engage à respecter la loi N° 2019- 014- du 29 octobre 2019 (LPDCPT) relative à la protection des données à caractère personnel au Togo par la mise en place d'une politique de protection.

Cette politique énonce les principes de base et lignes directrices mis en œuvre par la Société en matière de traitement de données personnelles des abonnés, clients, fournisseurs, partenaires commerciaux, employés et autres personnes, et indique les responsabilités de ses structures et employés lors du traitement des données personnelles.

Cette politique s'applique à la TdE à travers toutes les directions et les agences sur l'ensemble du territoire national.

Les utilisateurs de ce document sont tous les employés permanents ou temporaires, et tous les sous-traitants travaillant pour le compte de la TdE.

2. Documents de référence

1. • Loi N° 2019- 014- du 29 octobre 2019 relative à la Protection des données à caractère personnel au Togo (LPDCPT)
2. • RGPD 2016/679 (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE)
3. • Politique de protection des données personnelles des employés
4. • Politique de conservation des données
5. • Description du poste de correspondant à la protection des données
6. • Procédure de demande d'accès à la personne concernée
7. • Procédure de transfert transfrontalier de données personnelles
8. • Politiques de Sécurité du Système d' Information (PSSI)
9. • Procédure de notification de violation

3. Définitions

Les définitions suivantes et les termes utilisés dans ce document sont tirés de l'article 4 de la LPDCPT et du RGPD... ;

Consentement de la personne concernée toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel, accepte que ses données à caractère personnel fassent l'objet d'un traitement manuel ou électronique.

Données Personnelles : Toute information relative à une personne physique identifiée ou identifiable qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique.

Données Personnelles Sensibles : Les données personnelles qui sont, par leur nature, particulièrement sensibles au regard des libertés et droits fondamentaux méritent une protection spécifique car le contexte de leur traitement pourrait engendrer des risques significatifs pour les droits et libertés fondamentaux. Ces données à caractère personnel comprennent les données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance à un syndicat, les données génétiques, les données biométriques aux fins d'identification unique d'une personne physique, les données concernant la santé ou les données concernant le sexe d'une personne physique la vie ou l'orientation sexuelle.

Responsable du traitement : La personne physique ou morale, l'autorité publique, l'agence ou tout autre organisme, qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données personnelles.

Sous-traitant : une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui traite des données à caractère personnel pour le compte d'un responsable du traitement.

Traitement : opération ou ensemble d'opérations effectuées sur des données à caractère personnel ou sur des ensembles de données à caractère personnel, par des moyens automatisés ou non, telles que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou autre mise à disposition, l'alignement ou la combinaison, la restriction, l'effacement ou la destruction des données.

Traitement transfrontalier de données à caractère personnel : traitement de données à caractère personnel qui a lieu dans le cadre des activités d'établissements dans d'autres États en dehors du Togo d'un responsable du traitement ou d'un soustraitant.

Anonymisation : désidentification irréversible des données personnelles de sorte que la personne ne puisse pas être identifiée en utilisant un délai, un coût et une

technologie raisonnables, soit par le responsable du traitement, soit par toute autre personne pour identifier cette personne. Les principes de traitement des données personnelles ne s'appliquent pas aux données anonymisées car il ne s'agit plus de données personnelles.

Pseudonymisation : le traitement de données à caractère personnel de manière à ce que les données à caractère personnel ne puissent plus être attribuées à une personne concernée spécifique sans l'utilisation d'informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles pour garantir que les données personnelles ne soient pas attribuées à une personne physique identifiée ou identifiable. La pseudonymisation réduit, mais n'élimine pas complètement, la possibilité de lier des données personnelles à une personne concernée. Étant donné que les données pseudonymisées sont toujours des données personnelles, le traitement des données pseudonymisées doit respecter les principes de traitement des données personnelles. 4. Principes de base concernant le traitement des données personnelles

Les principes de protection des données décrivent les responsabilités fondamentales des organisations qui traitent des données personnelles. Les sections 3 et 4 du chapitre 2 de LPDCPT définissent les principes de base régissant le traitement des données à caractère personnel et ceux des données sensibles.

.1.Consentement et légitimité

Le traitement des données à caractère personnel est considéré comme légitime si la personne concernée donne son consentement. En dehors des cas d'exception prévus par la loi, le principe de consentement préalable de la personne concernée demeure la règle.

4.2. Licéité et transparence

Les données personnelles doivent être traitées de manière licite, loyale et transparente vis-à-vis de la personne concernée.

4.3. Délimitation des finalités

Les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités.

4,4. Minimisation des données

Les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

La société doit appliquer si possible l'anonymisation ou la pseudonymisation des données personnelles afin de réduire les risques pour les personnes concernées.

4.5. Exactitude des données

Les données personnelles doivent être exactes et, le cas échéant, tenues à jour ; des mesures raisonnables doivent être prises pour que les données à caractère personnel inexactes, au regard des finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées en temps utile.

4.6. Limitation de la durée de conservation

Les données personnelles ne doivent pas être conservées plus longtemps que nécessaire aux fins pour lesquelles elles sont traitées.

4.7. Intégrité et confidentialité

Compte tenu de l'état de la technologie et des autres mesures de sécurité disponibles, du coût de mise en œuvre, de la probabilité et de la gravité des risques liés aux données personnelles,

la Société doit utiliser des mesures techniques ou organisationnelles appropriées pour traiter les données personnelles d'une manière qui assure une sécurité appropriée à ces données, y compris la protection contre la destruction accidentelle ou illégale, la perte, l'altération, l'accès non autorisé ou la divulgation.

4.8. Responsabilisation

Le responsable de traitement des données doit être en mesure de démontrer le respect des principes énoncés ci-dessus et doit s'assurer que les sous contractants les respectent.

5. Renforcer la protection des données dans les activités commerciales

Afin de démontrer la conformité aux principes de protection des données, une organisation doit intégrer la protection des données dans ses activités commerciales.

5.1. Information aux personnes concernées

L'article 35 de LPDCPT précise la façon dont les personnes concernées doivent être informées :

« Lorsque des données à caractère personnel sont collectées directement auprès de la personne concernée, le responsable du traitement doit communiquer à celle-ci, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, les informations suivantes :

- 1) l'identité du responsable du traitement et, le cas échéant, de son représentant ; 2) la ou les finalités déterminées du traitement auquel les données sont destinées ; 3) les catégories de données concernées ;
- 4) le ou les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;
- 5) le caractère obligatoire ou non de répondre aux questions et les conséquences éventuelles d'un défaut de réponse ;
- 6) la possibilité de demander à ne plus figurer sur le fichier ;
- 7) l'existence d'un droit d'accès aux données la concernant et de rectification de ces données ;
- 8) la durée de conservation des données ;
- 9) le cas échéant, des transferts de données à caractère personnel envisagés à destination de l'étranger. ».

5.2. Choix et consentement de la personne concernée

La nécessité d'avoir le consentement des abonnés, clients et employés de la TdE avant le traitement de leurs données personnelles par nos services est de rigueur.

Le principe de consentement n'est pas applicable si la société peut démontrer que les traitements interviennent dans l'un des cas suivants :

- le respect d'une obligation légale à laquelle la TdE est soumise ;
- l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investie la TdE ou le tiers auquel les données sont communiquées
- l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande ;
- la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée.

Les usagers des services de la TdE sont directement éclairés des divers choix dont ils disposent en s'engageant avec la société au regard des exigences de la loi sur la protection des données personnelles au Togo.

5.3. Collecte des données

La TdE doit s'efforcer de collecter le moins possible de données personnelles. Si des données personnelles sont collectées auprès d'un tiers, le Correspondant à la protection des données personnelles doit s'assurer que les données personnelles sont collectées légalement.

5.4. Utilisation, conservation et suppression

Les objectifs, les méthodes, la limitation de stockage et la durée de conservation des données personnelles doivent être cohérents avec les informations contenues dans l'avis de confidentialité. La société doit maintenir l'exactitude, l'intégrité, la

confidentialité et la pertinence des données personnelles en fonction de la finalité du traitement. Des mécanismes de sécurité adéquats conçus pour protéger les données personnelles doivent être utilisés pour empêcher qu'elles soient volées, mal utilisées ou abusées, et prévenir toute atteinte contre elles. Le Correspondant à la protection des données personnelles conjointement avec le DSI/RSSI sont responsables du respect des exigences énumérées dans cette section.

5.5. Divulgateion à des tiers

Chaque fois que la TdE fait appel à un sous-traitant, un fournisseur, ou à un partenaire commercial pour traiter des données personnelles en son nom,

Le Correspondant à la Protection des Données personnelles doit s'assurer que ce sous-traitant fournira des mesures de sécurité pour protéger les données personnelles adaptées aux risques associés. À cette fin, le questionnaire de conformité à LPDCPT du sous-traitant doit être utilisé.

La TdE doit exiger contractuellement du sous-traitant, du fournisseur ou du partenaire commercial qu'il fournisse le même niveau de protection des données.

Le sous-traitant, le fournisseur ou le partenaire commercial ne doit traiter les données personnelles que pour exécuter ses obligations contractuelles envers la TdE ou sur les instructions de la celle-ci et non à d'autres fins. Lorsque la TdE traite des données personnelles conjointement avec un tiers indépendant, elle doit explicitement spécifier ses responsabilités respectives vis-à-vis du tiers dans le contrat concerné ou tout autre document juridiquement contraignant, tel que l'Accord de traitement des données du fournisseur.

5.6. Transfert transfrontalier de données personnelles

Avant de transférer des données personnelles hors du Togo, des garanties adéquates doivent être utilisées, notamment l'accord de l'autorité de protection des données (Instance de Protection des Données à Caractère Personnel). L'entité recevant les données personnelles doit se conformer aux principes de traitement des données personnelles énoncés dans la procédure de transfert transfrontalier de données.

5.7. Droits d'accès des personnes concernées

Lorsqu'il agit en tant que responsable de traitement, le Correspondant à la protection des données personnelles ou son relais est responsable de fournir aux personnes concernées un mécanisme d'accès raisonnable pour leur permettre d'accéder à leurs données personnelles, et doit leur permettre de mettre à jour, rectifier, effacer ou transmettre leurs données personnelles, le cas échéant ou requis par la loi. Le mécanisme d'accès sera détaillé dans la procédure de demande d'accès de la personne concernée.

5.8. Portabilité des données

Les personnes concernées ont le droit de recevoir, sur demande, une copie des données qu'elles nous ont fournies dans un format structuré et de transmettre ces données à un autre responsable du traitement, gratuitement. Le Correspondant à la protection des données personnelles est responsable de s'assurer que ces demandes sont traitées dans un délai d'un (1) mois, ne sont pas excessives et n'affectent pas les droits aux données personnelles d'autres personnes.

5.9. Droit à l'oubli

Sur demande, les Personnes concernées ont le droit d'obtenir de la Société l'effacement de leurs données personnelles.

Lorsque la Société agit en tant que Responsable du traitement, le Délégué/Correspondant à la protection des données personnelles doit prendre les mesures nécessaires (y compris les mesures techniques) pour informer les tiers qui utilisent ou traitent ces données afin de se conformer à la demande.

6. Lignes directrices sur le traitement transparent

Les données personnelles ne doivent être traitées qu'avec l'autorisation explicite du Directeur Général ou du Correspondant à la protection des données personnelles.

La Société a décidé d'effectuer l'évaluation de l'impact sur la protection des données pour chaque activité de traitement de données conformément aux lignes directrices sur l'évaluation de l'impact sur la protection des données.

6.1. Avis aux personnes concernées

Au moment de la collecte ou avant de collecter des données personnelles pour tout type d'activités de traitement, y compris, mais sans s'y limiter, la vente de produits, de services ou d'activités de marketing, le Correspondant à la protection des données ou son relais (Directeur Commercial, chef d'Agence, Directrice des Ressources humaines etc..) est responsable d'informer correctement les personnes concernées de ce qui suit : les types de données personnelles collectées, les finalités du traitement, les méthodes de traitement, les droits des personnes concernées à l'égard de leurs données personnelles, la durée de conservation, les éventuels transferts internationaux de données, si les données seront partagées avec des tiers et les mesures de sécurité de la Société pour protéger les données personnelles. Ces informations sont fournies par le biais de l'Avis de confidentialité.

Lorsque des données personnelles sont partagées avec un tiers, le Correspondant à la protection des données doit s'assurer que les personnes concernées en ont été informées par le biais d'un avis de confidentialité.

Lorsque des données personnelles sont transférées vers un pays tiers conformément à la politique de transfert transfrontalier de données, l'avis de confidentialité doit le

refléter et indiquer clairement où et à quelle entité les données personnelles sont transférées.

Lorsque des données personnelles sensibles sont collectées, le Correspondant à la protection des données doit s'assurer que l'avis de confidentialité indique explicitement la finalité pour laquelle ces données personnelles sensibles sont collectées.

6.2. Obtention des consentements

Chaque fois que le traitement des données personnelles est basé sur le consentement de la personne concernée ou sur d'autres motifs légaux, le Correspondant à la protection des données personnelles ou son relais est responsable de la conservation de l'enregistrement de ce consentement.

Il est chargé de fournir aux personnes concernées des options pour donner leur consentement et doit informer et veiller à ce que leur consentement (chaque fois que le consentement est utilisé comme motif légal de traitement) puisse être retiré à tout moment.

Lors des demandes de correction, de modification ou de destruction d'enregistrements de données personnelles, le Correspondant à la protection des données personnelles doit s'assurer que ces demandes sont traitées dans un délai raisonnable. Il doit également enregistrer les demandes et en tenir un journal.

Les données personnelles ne doivent être traitées que dans le but pour lequel elles ont été initialement collectées. Dans le cas où la Société souhaite traiter les données personnelles collectées dans un autre but, la Société doit solliciter le consentement de ces personnes concernées par un écrit clair et concis. Toute demande de ce type doit inclure la finalité initiale pour laquelle les données ont été collectées, ainsi que la ou les finalités nouvelles ou supplémentaires. La demande doit également inclure la raison du changement de finalité(s). Le Correspondant à la protection des données est responsable du respect des règles énoncées dans ce paragraphe.

Aujourd'hui et à l'avenir, Le Directeur Général ou son représentant désigné doit s'assurer que les méthodes de collecte sont conformes à la législation, aux bonnes pratiques et aux normes de l'industrie en vigueur.

Le Correspondant à la protection des données personnelles est responsable de la création et de la maintenance d'un registre des avis de confidentialité.

7. Organisation et responsabilités

La responsabilité d'assurer un traitement approprié des données personnelles incombe à toute personne travaillant pour ou avec la TdE et ayant accès aux données personnelles traitées par la TdE.

Les principaux domaines de responsabilité pour le traitement des données personnelles relèvent des rôles organisationnels suivants :

Le conseil d'administration ou tout autre organe décisionnel compétent prend des décisions et approuve les stratégies générales de la Société en matière de protection des données personnelles.

Le Correspondant à la Protection des Données (CPD) ou tout autre employé concerné, est responsable de la gestion du programme de protection des données personnelles et est responsable du développement et de la promotion des politiques de protection des données personnelles de bout en bout, telles que définies dans la description de poste du Correspondant à la protection des données ;

La Direction Juridique/Conseils, en collaboration avec le Correspondant à la Protection des Données, surveille et analyse les lois sur les données personnelles et les évolutions réglementaires, élabore les exigences de conformité et assiste les directions métiers dans la réalisation de leurs objectifs en matière de Données Personnelles.

Le Directeur des Services Informatiques, est chargé de :

- S'assurer que tous les systèmes, services et équipements utilisés pour stocker les données répondent aux normes de sécurité acceptables.
- Effectuer des vérifications et des analyses régulières pour s'assurer que le matériel et les logiciels de sécurité fonctionnent correctement.

Le Directeur Commercial, est chargé de :

- Approuver toutes les déclarations de protection des données jointes aux communications telles que les e-mails et les lettres.
- Répondre à toute question relative à la protection des données émanant de journalistes ou de médias tels que les journaux.
- Si nécessaire, travailler avec le Correspondant à la protection des données pour s'assurer que les initiatives commerciales et marketing respectent les principes de protection des données.

Le Directeur des Ressources Humaines est chargé de :

- Sensibiliser l'ensemble des collaborateurs à la protection des données personnelles des utilisateurs.
- Organiser une expertise et une sensibilisation à la protection des données personnelles pour les collaborateurs travaillant avec des données personnelles.
- Protéger les données personnelles des employés de bout en bout. Elle doit veiller à ce que ces données soient traitées en fonction des objectifs commerciaux légitimes et de la nécessité de l'employeur.

Le responsable des achats est chargé de:

- e transmettre les responsabilités de protection des données personnelles aux fournisseurs ;
- d'améliorer les niveaux de sensibilisation des fournisseurs à la protection des données personnelles ;
- transmettre les exigences en matière de données personnelles à tout tiers un fournisseur qu'il utilise.

Le Directeur de l'Audit Interne et du Contrôle doit s'assurer que la TdE se réserve le droit d'auditer les fournisseurs et les sous-traitants.

8. Réponse aux incidents de violation de données personnelles

Lorsque l'entreprise prend connaissance d'une violation de données personnelles suspectée ou réelle, le Responsable de la Sécurité du Système d' Information (RSSI) doit mener une enquête interne et prendre les mesures correctives appropriées en temps opportun, conformément à la politique de violation de données.

En cas de risque pour les droits et libertés des personnes concernées, la Société doit en informer les autorités compétentes en matière de protection des données sans retard injustifié et, si possible, dans les 72 heures.

9. Audit et responsabilité

Le service d'audit ou tout autre service concerné est responsable de l'audit de la manière dont les services de la TdE mettent en œuvre cette politique.

Tout employé qui enfreint à cette politique fera l'objet de mesures disciplinaires et l'employé peut également être passible de poursuites civiles ou pénales si sa conduite enfreint aux lois ou aux règlements.

10. Gestion des documents issus de ce document de Politique

Nom de Venregistrement	Emplacement de stockage	Personne responsable du stockage	Contrôles pour la protection des enregistrements	Durée de conservation

Formulaire de consentement des personnes concernées	[Préciser le dossier sur l'intranet de l'entreprise ou la base de données de votre système d'information]	Correspondant à la protection des données personnelles	Seules les personnes autorisées peuvent accéder aux formulaires	10 ans
Formulaire de retrait du consentement de la personne concernée	[Préciser le dossier sur l'intranet de l'entreprise ou la base de données de votre système d'information]	Correspondant à la protection des données personnelles	Seules les personnes autorisées peuvent accéder aux formulaires	10 ans
Accords de traitement des données des fournisseurs	[Préciser le dossier sur l'intranet de l'entreprise ou la base de données de votre système d'information]	Correspondant à la protection des données personnelles	Seules les personnes autorisées peuvent accéder aux formulaires	5 ans après l'expiration du contrat
Registre des avis de confidentialité	[Préciser le dossier sur l'intranet de l'entreprise ou la base de données de votre système d'information]	Correspondant à la protection des données personnelles	Seules les personnes autorisées peuvent accéder aux formulaires	En permanence

11. Validité et gestion du document

Ce document est valable à compter du 05 octobre 2022, date de sa validation par le Comité de Pilotage.

Le propriétaire de ce document est la Direction Générale, qui doit vérifier et, si nécessaire, mettre à jour le document au moins une fois par an.

Le Directeur Général,



Gbati YAWANKE WAKE