

Politique de confidentialité et de protection des données personnelles

Version 1.0 — Cotonou, le 5 août 2026

Sommaire

1. Préambule
2. Identité et coordonnées du responsable de traitement
3. Définitions
4. Personnes concernées par la présente Politique
5. Données à caractère personnel traitées
6. Finalités, bases juridiques et caractère obligatoire ou facultatif
7. Durées de conservation
8. Destinataires et sous-traitants
9. Transferts internationaux de données
10. Sécurité des données
11. Cookies et autres traceurs
12. Mineurs
13. Communications commerciales
14. Droits des personnes concernées
15. Violation de données à caractère personnel
16. Réclamation auprès de l'Autorité de Protection des Données Personnelles
17. Modification de la présente Politique
18. Contact

Préambule

La présente Politique de confidentialité et de protection des données personnelles (ci-après la « Politique ») décrit la manière dont EB GROUP ENTERPRISE traite les données à caractère personnel des personnes qui utilisent ou entrent en contact avec la plateforme numérique de cagnottes en ligne dénommée « Ayélé » (ci-après la « Plateforme »).

La présente Politique complète les Conditions générales d'utilisation et de vente d'Ayélé, ci-après les « CGU/CGV », auxquelles il est renvoyé pour la définition des termes propres au fonctionnement du service, notamment Organisateur, Contributeur, Bénéficiaire, Cagnotte, Contribution, Reversement et Restitution.

Les CGU/CGV encadrent la relation contractuelle entre EB GROUP ENTERPRISE et les Utilisateurs. La présente Politique a pour objet spécifique d'informer les personnes concernées sur la manière dont leurs données à caractère personnel sont collectées, utilisées, conservées, partagées et protégées.

En cas de contradiction concernant exclusivement le traitement des données à caractère personnel, la présente Politique s'applique, sous réserve des dispositions légales et réglementaires impératives.

L'acceptation des CGU/CGV ne vaut pas consentement général au traitement des données personnelles. Lorsqu'un traitement requiert le consentement de la personne concernée, celui-ci est recueilli séparément, au moyen d'une action libre, spécifique, éclairée et non activée par défaut.

Ce traitement est effectué conformément à la loi n° 2017-20 du 20 avril 2018 portant Code du numérique en République du Bénin, modifiée par la loi n° 2020-35 du 6 janvier 2021, et sous le contrôle de l'Autorité de Protection des Données Personnelles du Bénin (APDP).

Identité et coordonnées du responsable de traitement

Le responsable des traitements de données à caractère personnel décrits dans la présente Politique est :

EB GROUP ENTERPRISE, société à responsabilité limitée au capital social de 1 000 000 FCFA, immatriculée au Registre du commerce et du crédit mobilier de Cotonou sous le numéro RB/COT/26 B 43099, identifiée sous le numéro IFU 3202686270991, dont le siège social est situé Îlot 1123, quartier Houéyiho, 11^e arrondissement, Cotonou, département du Littoral, République du Bénin, exploitant la plateforme Ayélé.

- **Téléphone** : +229 01 94 40 75 60
- **Courriel dédié aux données personnelles** : XXXprivacy@beaye.com, ou à défaut ayele.africa@outlook.com avec la mention « Protection des données personnelles »
- **Représentant légal** : Monsieur HOUINSA Louis Axel Audrey Koffi, Gérant

Certains prestataires intervenant dans l'exécution des paiements ou des vérifications réglementaires traitent une partie des données sous leur propre responsabilité, dans les conditions décrites à l'article 8 de la présente Politique.

Définitions

Les termes définis dans les CGU/CGV d'Ayélé (Plateforme, Société, Utilisateur, Organisateur, Contributeur, Bénéficiaire, Cagnotte, Contribution, Reversement, Restitution, Prestataire de services de paiement, Établissement de monnaie électronique) conservent la même signification dans la présente Politique.

Pour les besoins spécifiques de la présente Politique, les expressions suivantes ont la signification ci-après :

« **Donnée à caractère personnel** » : toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement.

« **Traitement** » : toute opération portant sur des données à caractère personnel, notamment leur collecte, leur enregistrement, leur conservation, leur utilisation, leur communication ou leur suppression.

« **Responsable de traitement** » : la personne qui détermine les finalités et les moyens d'un traitement.

« **Sous-traitant** » : la personne qui traite des données à caractère personnel pour le compte du responsable de traitement, sur instruction de celui-ci.

« **Destinataire** » : toute personne habilitée à recevoir communication de données à caractère personnel, qu'elle agisse en qualité de sous-traitant ou de responsable de traitement indépendant pour la part des traitements qui lui incombe.

Personnes concernées par la présente Politique

La présente Politique s'applique aux données à caractère personnel des personnes suivantes :

- les visiteurs de la Plateforme, y compris avant toute création de compte ;
- les Organismes, y compris les représentants d'une personne morale organisatrice ;
- les Contributeurs ;
- les Bénéficiaires, y compris lorsqu'ils ne créent pas eux-mêmes de compte ;
- les personnes physiques représentées dans les Contenus utilisateurs publiés sur une Cagnotte ;
- les représentants légaux ou mandataires d'une association, d'une entreprise ou d'une administration organisatrice ;
- les personnes contactant le service client ou le support d'Ayélé ;
- les auteurs d'un signalement ou d'une réclamation ;
- les personnes impliquées dans une vérification, une contestation ou une suspicion de fraude, y compris lorsqu'elles n'utilisent pas directement la Plateforme.

Lorsque la collecte concerne une personne qui n'utilise pas directement Ayélé, notamment un Bénéficiaire distinct de l'Organisme ou une personne représentée dans un Contenu, elle est limitée à ce qui est nécessaire à la gestion de la Cagnotte, à la vérification de son accord, à la sécurité de la Plateforme ou au respect d'une obligation légale.

Information des personnes dont les données sont fournies par un tiers

Lorsqu'un Organisme transmet à Ayélé des données concernant un Bénéficiaire, un représentant légal, un membre d'une association ou toute autre personne ne disposant pas directement d'un compte Ayélé, il doit :

- être autorisé à communiquer ces informations ;
- limiter les données transmises à ce qui est nécessaire à la création, à la vérification et à la gestion de la Cagnotte ;
- informer la personne concernée de la création de la Cagnotte et du traitement de ses données ;
- lui communiquer un lien permettant de consulter la présente Politique ;
- l'informer des informations susceptibles d'être rendues publiques ;
- lui permettre de contacter Ayélé afin d'exercer ses droits.

Lorsque les coordonnées de la personne concernée sont disponibles et que cette démarche est nécessaire, Ayélé peut lui adresser directement une notice d'information précisant notamment :

- l'identité d'EB GROUP ENTERPRISE ;
- la nature des données reçues ;
- l'identité de l'Organisateur ayant transmis les données ;
- l'objet de la Cagnotte ;
- les finalités du traitement ;
- les informations susceptibles d'être publiées ;
- les destinataires des données ;
- les modalités d'exercice de ses droits.

Cette information intervient dans un délai raisonnable après la réception des données et, au plus tard, lors du premier contact direct entre Ayélé et la personne concernée, sauf lorsque :

- la personne dispose déjà de ces informations ;
- cette information est juridiquement impossible ou exigerait des efforts manifestement disproportionnés ;
- sa communication compromettrait une vérification de sécurité, une enquête ou une obligation légale ;
- une disposition légale autorise ou impose expressément un traitement différent.

Le Bénéficiaire ou la personne concernée peut demander :

- la rectification d'une information inexacte ;
- le retrait d'une donnée manifestement excessive ;
- la limitation de l'affichage public ;
- la suppression d'un Contenu publié sans autorisation, lorsque les conditions légales sont remplies ;
- la suspension de la Cagnotte pendant l'examen de sa demande.

La transmission de données à Ayélé par l'Organisateur ne prive pas la personne concernée de ses droits et ne vaut pas autorisation automatique de publier ces données sur la page publique de la Cagnotte.

Données à caractère personnel traitées

Selon les fonctionnalités utilisées, Ayélé peut traiter les catégories de données suivantes :

- identité : nom, prénoms, date de naissance lorsque cette information est nécessaire, nationalité lorsqu'elle est requise ;
- coordonnées : numéro de téléphone, adresse électronique, adresse postale ou de résidence ;
- identifiants et données d'authentification : identifiant de compte, XXXmot de passe sous forme chiffrée, mot de passe conservé sous la forme d'une empreinte cryptographique sécurisée ne permettant pas sa restitution en clair, code de vérification à usage unique ;
- données relatives à une personne morale : dénomination sociale, numéro RCCM, numéro IFU, adresse du siège, identité des représentants et, lorsque cette information est requise, des bénéficiaires effectifs ;
- données de la Cagnotte : titre, description, objectif de collecte, images, messages et autres Contenus utilisateurs, informations relatives au Bénéficiaire et, lorsque cela est strictement nécessaire, données sensibles faisant l'objet des garanties spécifiques prévues par la présente Politique;
- données de Contribution : montant, date, statut de la transaction, référence de transaction transmise par le Prestataire de services de paiement, moyen de paiement utilisé, message éventuellement laissé par le Contributeur, choix d'affichage public ou anonyme ;
- numéro Mobile Money ou coordonnées du compte destiné à recevoir un Reversement ou une Restitution, le cas échéant sous une forme partiellement masquée à l'affichage ;
- justificatifs d'identité et documents transmis dans le cadre d'une vérification, notamment pièce d'identité, justificatif de domicile, document attestant du caractère collectif ou associatif d'une collecte ;
- historique des Reversements, Restitutions, contestations et Rétrofacturations ;
- communications échangées avec le service client, signalements et réclamations ;
- données techniques : adresse IP, identifiants d'appareil et de navigateur, journaux de connexion, de sécurité et d'activité ;
- choix relatifs à la confidentialité, aux cookies et aux communications facultatives.

Données sensibles et données relatives à la santé

Certaines Cagnottes peuvent révéler ou nécessiter le traitement de données présentant un caractère particulièrement sensible, notamment :

- des informations relatives à la santé physique ou mentale ;
- un handicap ou une situation de dépendance ;
- un diagnostic, un traitement ou une intervention médicale ;
- des informations sociales, familiales ou financières sensibles ;
- des informations relatives à un mineur ou à une personne vulnérable ;
- des données figurant dans un certificat, une ordonnance, un devis médical ou un document de prise en charge.

Ces données ne sont traitées que lorsqu'elles sont strictement nécessaires :

- à la présentation légitime de la Cagnotte ;
- à la vérification de son authenticité ;
- à la protection du Bénéficiaire et des Contributeurs ;
- au traitement d'une réclamation ou d'un signalement ;

- au respect d'une obligation légale ou d'une instruction émanant d'une autorité compétente.

Lorsque le traitement ou la publication repose sur le consentement de la personne concernée, Ayélé recueille ou demande à l'Organisateur de justifier un consentement explicite, spécifique et éclairé du Bénéficiaire ou, lorsque cela est nécessaire, de son représentant légal.

Le consentement à la création d'une Cagnotte ne vaut pas automatiquement consentement à la publication de l'intégralité des justificatifs transmis.

Ayélé distingue :

1. **les informations destinées à la page publique**, limitées à ce qui est nécessaire pour expliquer l'objet de la collecte ;
2. **les justificatifs privés de vérification**, accessibles uniquement aux personnes habilitées et aux prestataires compétents ;
3. **les données communiquées aux autorités ou Prestataires de paiement**, lorsque cette transmission est légalement requise ou nécessaire au traitement d'un incident.

Il est interdit de publier directement sur une page publique :

- un certificat médical complet ;
- une ordonnance médicale complète ;
- un dossier médical ;
- une pièce d'identité ;
- un numéro de sécurité sociale ou identifiant similaire ;
- des coordonnées bancaires ;
- une adresse personnelle précise ;
- une signature manuscrite ;
- toute information dont la publication exposerait la personne concernée à un risque disproportionné.

Lorsque la transmission d'un document complet est nécessaire à la vérification, celui-ci doit être déposé uniquement dans l'espace privé et sécurisé prévu par Ayélé.

Ayélé peut :

- masquer certaines informations ;
- demander une version expurgée du document ;
- refuser la publication d'un Contenu excessivement intrusif ;
- suspendre la Cagnotte jusqu'à l'obtention de l'accord de la personne concernée ;
- supprimer un justificatif devenu inutile.

Les traitements de données sensibles sont soumis aux formalités, autorisations et mesures de sécurité applicables avant leur mise en œuvre.

Ayélé ne collecte ni ne conserve directement les données complètes d'une carte bancaire. Ces données sont saisies et traitées exclusivement dans l'environnement sécurisé du Prestataire de services de paiement.

Une Contribution présentée comme anonyme sur la page publique d'une Cagnotte peut néanmoins rester identifiable par Ayélé, par le Prestataire de services de paiement, par l'établissement de monnaie électronique concerné ou par une autorité compétente, lorsque cette identification est nécessaire à l'exécution du paiement, à la sécurité ou au respect de la loi. L'anonymat choisi par le Contributeur ne concerne que l'affichage

public de son identité, non le traitement interne des données nécessaires au bon déroulement de l'opération.

Finalités, bases juridiques et caractère obligatoire ou facultatif

Le tableau ci-dessous présente, pour chaque finalité principale, les catégories de données concernées, la base juridique du traitement, son caractère obligatoire ou facultatif et les conséquences d'un refus.

Finalité	Catégories de données	Base juridique	Contrainte et Conséquence d'un refus
Création et du compte	Identité, coordonnées, identifiants	Exécution des CGU/CGV	Obligatoire ; Impossibilité de créer un compte
Authentification et sécurité du compte	Identifiants, codes de vérification, journaux de connexion	Exécution des CGU/CGV ; intérêt légitime à la sécurité	Obligatoire ; Impossibilité d'accéder au compte
Création et publication d'une Cagnotte	Données de la Cagnotte, informations sur le Bénéficiaire	Exécution des CGU/CGV	Obligatoire pour les champs requis ; Impossibilité de créer la Cagnotte
Vérification de l'Organisateur, du Bénéficiaire et sécurisation de la Cagnotte	Identité, coordonnées, pièce d'identité, justificatifs, numéro ou compte de Reversement, informations sur le Bénéficiaire	Exécution des CGU/CGV ; intérêt légitime d'EB GROUP ENTERPRISE à prévenir la fraude, l'usurpation d'identité et les détournements ; respect des obligations légales directement applicables ; coopération avec les Prestataires de paiement et autorités légalement habilités	Obligatoire ; Blocage de la Cagnotte ou du Reversement
Traitement et des Contributions	Données de Contribution, référence de transaction	Exécution des CGU/CGV	Obligatoire ; Impossibilité d'enregistrer la Contribution
Calcul et du Reversement	Données de Contribution, coordonnées de Reversement	Exécution des CGU/CGV	Obligatoire ; Impossibilité de recevoir le Reversement
Traitement d'une Restitution	Données de Contribution,	Exécution des CGU/CGV	Obligatoire pour traiter la demande ;

Finalité	Catégories de données	Base juridique	Contrainte et Conséquence d'un refus
	coordonnées du Contribuable		Impossibilité d'examiner la demande
Service client et assistance	Identité, coordonnées, contenu de la demande	Exécution des CGU/CGV ; intérêt légitime	Obligatoire pour traiter la demande ; Impossibilité de répondre à la demande
Sécurité de la Plateforme et prévention de la fraude	Données techniques, journaux, historique des opérations	Intérêt légitime ; obligation légale	Obligatoire ; Restriction ou refus d'accès au service
Respect des obligations légales, comptables et fiscales	Identité, données de transaction, factures	Obligation légale	Obligatoire ; Impossibilité de fournir le service concerné
Gestion des litiges, contestations et Rétrofacturations	Données de transaction, justificatifs, échanges	Exécution des CGU/CGV ; intérêt légitime ; obligation légale	Obligatoire pour le traitement du dossier ; Impossibilité de traiter la contestation
Statistiques internes et amélioration du service	Données d'usage agrégées ou pseudonymisées	Intérêt légitime	Facultatif lorsque la donnée est identifiante ; Aucune conséquence sur l'accès au service
Communications commerciales	Coordonnées, préférences	Consentement	Facultatif ; Aucune conséquence sur l'accès au service
Cookies facultatifs	Identifiants techniques, données de navigation	Consentement	Facultatif ; Aucune conséquence sur l'accès aux fonctionnalités principales

Lorsque la vérification implique des données sensibles, notamment des données relatives à la santé, celles-ci sont traitées sur le fondement juridique spécifiquement applicable à cette catégorie de données, notamment le consentement explicite de la personne concernée lorsqu'il est requis, sans préjudice des autres fondements expressément autorisés par la réglementation.

L'acceptation des CGU/CGV ne vaut pas consentement général à l'ensemble des traitements. Lorsque le consentement constitue le fondement requis pour un traitement

déterminé, il est recueilli par une action distincte, libre, spécifique, éclairée et non activée par défaut, et peut être retiré à tout moment sans remettre en cause la licéité des traitements déjà effectués.

Durées de conservation

Les données sont conservées pendant une durée proportionnée à la finalité poursuivie, conformément au tableau ci-dessous. À l'expiration de ces durées, les données sont supprimées, anonymisées, ou archivées avec un accès restreint lorsqu'une conservation résiduelle est légalement nécessaire.

Catégorie de données	Durée de conservation	Justification
Données de compte actif	Durée d'utilisation du compte	Nécessaire à l'exécution du service
Données de compte après clôture	5 ans à compter de la clôture, sauf procédure en cours	Prescription civile de droit commun et gestion des réclamations tardives
Données comptables et de transaction	10 ans à compter de l'opération	Obligations comptables (Acte uniforme OHADA relatif au droit comptable, article 24)
Copie de la pièce d'identité d'un Organisateur ou Bénéficiaire dont la vérification a été acceptée	Pendant la durée de la relation active, puis 12 mois après la clôture de la dernière Cagnotte ou opération, sauf litige, fraude, instruction d'une autorité ou obligation légale imposant une durée différente	Vérification de l'identité, prévention de la fraude et traitement des contestations rapprochées
Preuve de la vérification d'identité	5 ans après la clôture du compte ou de la dernière opération, sous une forme minimisée ne contenant pas nécessairement la copie complète de la pièce	Preuve de la réalisation du contrôle et défense des droits d'EB GROUP ENTERPRISE
Pièce d'identité ou justificatif transmis dans le cadre d'une demande refusée ou abandonnée	6 mois après la décision définitive ou le dernier échange, sauf suspicion de fraude ou litige	Prévention des demandes répétées, gestion des contestations et limitation de la conservation
Pièce associée à une fraude, une Rétrofacturation, une enquête ou un litige	Jusqu'à la clôture définitive du dossier et l'expiration des délais de recours applicables	Constataction, exercice et défense des droits
Données conservées directement par un Prestataire de services de paiement	Selon les durées et obligations propres à ce Prestataire, agissant sous sa responsabilité	Respect des obligations réglementaires du Prestataire

Catégorie de données	Durée de conservation	Justification
À l'expiration de la durée de conservation de la copie complète d'une pièce d'identité, Ayélé peut conserver une preuve minimisée de la vérification, comprenant notamment la date du contrôle, son résultat, le type de document présenté, son pays d'émission et une référence partiellement masquée. La durée de conservation peut être prolongée lorsqu'une obligation légale directement applicable, une autorisation de l'APDP, une demande d'une autorité compétente ou un litige en cours l'exige.		
Journaux de sécurité et de connexion	12 mois, sauf enquête de sécurité ou obligation légale prolongeant ce délai	Détection des incidents et preuve en cas de contestation
Code de vérification à usage unique	Jusqu'à son utilisation ou à l'expiration de sa durée de validité ; le code lui-même n'est ensuite plus conservé sous une forme permettant son utilisation	Authentification du compte
Journaux d'émission, d'envoi et de validation des codes	12 mois, sauf incident de sécurité nécessitant une conservation plus longue	Sécurité, détection des abus et preuve des opérations d'authentification
Tentatives de connexion et événements de sécurité	12 mois, sauf enquête ou incident en cours	Prévention des accès non autorisés et traitement des incidents
Historique des Reversements et Restitutions	10 ans à compter de l'opération	Obligations comptables et fiscales
Contestations, signalements et Rétrofacturations	5 ans à compter de la clôture du dossier	Gestion des litiges et prescription applicable
Communications avec le support	3 ans à compter du dernier échange	Gestion de la relation utilisateur et preuve en cas de litige
Cookies et preuve du consentement	13 mois à compter du dépôt ou du recueil du choix	Durée de validité usuelle d'un consentement aux cookies, renouvelable
Données relatives à une Cagnotte supprimée ou clôturée	Conservées selon les durées ci-dessus applicables à chaque catégorie de données concernée, à l'exclusion de l'affichage public	Le retrait de l'affichage public n'entraîne pas la suppression immédiate des données sous-jacentes
Données relatives à une Cagnotte expirée ou abandonnée	Retrait de l'affichage public à la clôture ; conservation des seules données nécessaires selon les durées applicables aux	Traitement des fonds, Restitutions, traçabilité et respect des obligations légales

Catégorie de données	Durée de conservation	Justification
	transactions, justificatifs, litiges et obligations comptables	
Le classement d'une Cagnotte comme expirée, inactive ou abandonnée n'entraîne pas la conservation indéfinie de tous ses Contenus. Les photographies, récits personnels et autres données non nécessaires sont supprimés ou anonymisés après la clôture, selon les délais définis dans la présente Politique.		
Certificats médicaux et autres justificatifs sensibles utilisés pour vérifier une Cagnotte	Pendant la durée strictement nécessaire à la vérification, puis suppression au plus tard 90 jours après le Reversement, l'annulation ou la clôture de la Cagnotte, sauf litige, fraude, obligation légale ou demande d'une autorité compétente	Vérification de la Cagnotte et minimisation des données sensibles
La suppression du justificatif complet n'empêche pas Ayélé de conserver une mention indiquant que la vérification a été réalisée, sa date, son résultat et la catégorie générale du document examiné.		

Destinataires et prestataires intervenant dans les traitements

Destinataires internes

Les données à caractère personnel sont accessibles uniquement aux personnes habilitées au sein d'EB GROUP ENTERPRISE, dans la limite :

- de leurs fonctions ;
- des opérations qu'elles sont autorisées à réaliser ;
- du besoin strict d'accéder aux informations concernées.

Selon l'organisation mise en place, peuvent notamment être concernés :

- la direction d'EB GROUP ENTERPRISE ;
- les personnes chargées du support utilisateur ;
- les personnes chargées des vérifications et de la prévention de la fraude ;
- les personnes chargées du suivi financier et du rapprochement des opérations ;
- les administrateurs techniques expressément habilités.

Les habilitations sont attribuées individuellement, réexaminées périodiquement et supprimées lorsqu'elles ne sont plus nécessaires.

Prestataires et partenaires externes

Ayélé fait intervenir des prestataires techniques et financiers pour fournir certaines fonctionnalités de la Plateforme.

Le rôle juridique d'un prestataire dépend des traitements qu'il réalise effectivement :

- un **sous-traitant** traite les données pour le compte et sur les instructions d'EB GROUP ENTERPRISE ;
- un **responsable de traitement indépendant** détermine lui-même certaines finalités et certains moyens du traitement, notamment lorsqu'il respecte ses propres obligations réglementaires ;
- un même prestataire peut relever de qualifications différentes selon l'opération concernée.

Les principaux prestataires ou catégories de prestataires utilisés par Ayélé sont les suivants :

Prestataire ou service	Fonction pour Ayélé	Principales données concernées	Qualification principale
OPEN SI, exploitant la solution Kkiapay	Traitement, confirmation et suivi des Contributions et des opérations de paiement activées pour Ayélé	Référence de transaction, montant, statut, moyen de paiement, identité et coordonnées nécessaires à l'opération	Responsable de traitement indépendant pour les traitements qu'il détermine dans le cadre des services de paiement et de ses obligations réglementaires ; toute autre qualification dépend du contrat applicable
MTN Mobile Money Benin	Exécution des opérations Mobile Money et gestion du compte professionnel utilisé dans le circuit financier d'Ayélé	Numéro Mobile Money, identité du titulaire lorsque requise, montant, référence et statut de l'opération	Responsable de traitement indépendant pour ses propres services et obligations réglementaires
Moov Money Benin	Exécution des opérations Mobile Money concernées	Numéro Mobile Money, identité du titulaire lorsque requise, montant, référence et statut de l'opération	Responsable de traitement indépendant pour ses propres services et obligations réglementaires
Celtiis Cash, Orange Money, Mixx, Airtel, Wave, Verve	Exécution des opérations Mobile Money concernées	Numéro Mobile Money, identité du titulaire lorsque requise, montant, référence et statut de l'opération	Responsable de traitement indépendant pour ses propres services et obligations réglementaires
Cloudflare	XXX	XXX	XXX

Twilio	Envoi et vérification de certains codes ou messages par SMS	Numéro de téléphone, contenu technique du message, statut d'envoi et données techniques associées	Sous-traitant pour les opérations réalisées pour le compte d'EB GROUP ENTERPRISE, sous réserve de ses propres traitements légalement autonomes
Mailjet	Envoi de courriels transactionnels et de notifications	Adresse électronique, identité ou nom d'affichage, contenu du message, statut d'envoi	Sous-traitant pour les opérations réalisées pour le compte d'EB GROUP ENTERPRISE
Vercel	Hébergement ou diffusion de certaines composantes de l'interface de la Plateforme	Données techniques de navigation, adresse IP, journaux nécessaires à la sécurité et au fonctionnement	Sous-traitant, selon la configuration et le contrat applicables
Render	Hébergement de certaines composantes applicatives de la Plateforme	Données traitées par les services applicatifs hébergés, selon la configuration technique	Sous-traitant
MongoDB Atlas	Hébergement et gestion de la base de données de la Plateforme	Données de compte, de Cagnotte, de transaction, de suivi et autres données enregistrées dans la base	Sous-traitant
Cloudinary	Stockage, optimisation et diffusion des images destinées à être affichées sur les Cagnottes	Images, photographies et métadonnées techniques associées	Sous-traitant
WhatsApp Business	Assistance générale, échange avec le support, suivi de certaines demandes et transmission de notifications lorsque ce canal est utilisé	Numéro de téléphone, nom ou nom d'affichage, contenu des messages, date et heure, statut des messages, métadonnées techniques et éventuelles pièces volontairement transmises	EB GROUP ENTERPRISE est responsable du traitement relatif à la gestion de la relation avec l'Utilisateur. WhatsApp traite également certaines données sous sa propre responsabilité pour fournir, sécuriser et administrer son service

Utilisation de WhatsApp

Ayéle peut proposer WhatsApp comme canal d'assistance et de communication.

Ce canal peut être utilisé notamment pour :

- demander une information générale ;
- suivre le statut d'une demande ;
- obtenir une orientation vers le parcours approprié ;
- recevoir une notification relative à une Cagnotte ou à une opération ;
- échanger avec le support.

WhatsApp ne constitue pas le canal sécurisé destiné à la transmission de documents sensibles.

L'Utilisateur ne doit pas transmettre par WhatsApp :

- une pièce d'identité ;
- un certificat ou dossier médical ;
- des coordonnées bancaires complètes ;
- les données complètes d'une carte ;
- un mot de passe ;
- un code à usage unique ;
- un code secret Mobile Money ;
- un justificatif financier confidentiel ;
- tout document comportant des données excessivement sensibles.

Lorsque la résolution d'une demande nécessite un document sensible, Ayéle dirige l'Utilisateur vers l'espace sécurisé ou le canal approprié.

Les échanges WhatsApp sont conservés uniquement pendant la durée nécessaire au traitement de la demande et selon les durées prévues pour les communications avec le support.

L'utilisation de WhatsApp peut entraîner un traitement de données à l'étranger. Les informations relatives aux transferts et au rôle du prestataire figurent dans la section consacrée aux transferts internationaux.

La qualification indiquée dans le présent tableau est fondée sur le rôle principal du prestataire. Elle est précisée ou adaptée lorsque les contrats conclus et la réalité des traitements imposent une qualification différente.

Séparation des contenus publics et des justificatifs sensibles

Cloudinary ou tout autre espace destiné à la diffusion publique d'images ne doit pas être utilisé pour stocker :

- les pièces d'identité complètes ;
- les certificats médicaux ;
- les justificatifs financiers ;
- les actes d'état civil ;
- les documents comportant des signatures ;
- les documents confidentiels utilisés pour les vérifications.

Ces documents sont conservés, lorsqu'ils sont nécessaires, dans un espace privé bénéficiant de mesures d'accès et de sécurité renforcées.

Une version expurgée ou une image spécifiquement autorisée peut être publiée sur la page de la Cagnotte lorsqu'elle ne révèle pas de données excessives.

Conseils et autorités compétentes

Les données peuvent également être communiquées, dans la limite strictement nécessaire :

- aux conseils juridiques, fiscaux, comptables ou techniques d'EB GROUP ENTERPRISE, soumis à une obligation de confidentialité ;
- aux auditeurs intervenant dans le cadre d'une mission autorisée ;
- aux autorités administratives, judiciaires, fiscales ou réglementaires légalement habilitées ;
- à l'Autorité de Protection des Données Personnelles ;
- aux autorités compétentes en matière de lutte contre la fraude et les infractions financières ;
- aux forces de police ou de justice sur demande légalement fondée.

EB GROUP ENTERPRISE vérifie la régularité apparente de toute demande de communication et limite les informations transmises à ce qui est nécessaire.

Absence de vente des données

EB GROUP ENTERPRISE ne vend, ne loue et ne commercialise pas les données à caractère personnel des Utilisateurs.

L'intervention d'un prestataire ou la transmission nécessaire à l'exécution du service ne constitue pas une vente de données.

Mise à jour de la liste

La présente liste correspond aux prestataires effectivement utilisés à la date d'entrée en vigueur de la Politique.

Lorsqu'un nouveau prestataire accède à des données personnelles, EB GROUP ENTERPRISE vérifie préalablement :

- son identité juridique ;
- son rôle ;
- les catégories de données auxquelles il accède ;
- les finalités concernées ;
- les pays ou régions de traitement ;
- ses mesures de sécurité ;
- les conditions de suppression ou de restitution des données ;
- les sous-traitants auxquels il peut lui-même recourir ;
- les garanties contractuelles applicables.

Une modification substantielle de la liste ou du circuit des données est portée à la connaissance des personnes concernées dans les conditions prévues par la présente Politique.

Transferts internationaux de données

Principe

Certains prestataires techniques utilisés par Ayélé peuvent traiter, héberger, sauvegarder ou rendre accessibles des données à caractère personnel depuis un pays situé en dehors de la République du Bénin.

Constitue notamment un transfert international :

- l'hébergement d'une base de données à l'étranger ;
- la sauvegarde de données dans une infrastructure étrangère ;
- l'accès à distance aux données depuis un autre pays ;
- la transmission de données à un prestataire étranger ;
- le recours par un prestataire à un sous-traitant établi dans un autre pays.

La simple utilisation d'un service ayant une société mère étrangère ne permet pas, à elle seule, d'identifier le pays réel de traitement. La localisation est déterminée en fonction de l'entité contractante, de la configuration technique, des régions d'hébergement et des sous-traitants effectivement utilisés.

Conditions préalables au transfert

EB GROUP ENTERPRISE ne met en œuvre un transfert international qu'après avoir :

- identifié le destinataire et son rôle ;
- identifié les pays ou régions de traitement concernés ;
- déterminé les catégories de données transférées ;

- défini la finalité et la durée du transfert ;
- vérifié la nécessité et la proportionnalité du transfert ;
- examiné les mesures de sécurité du destinataire ;
- conclu les engagements contractuels nécessaires ;
- vérifié les conditions de recours à des sous-traitants ultérieurs ;
- accompli les formalités requises auprès de l'Autorité de Protection des Données Personnelles.

Lorsqu'une autorisation, une déclaration, un avis ou une autre formalité préalable est requis, le transfert concerné n'est activé qu'après l'accomplissement de cette formalité.

Garanties mises en œuvre

Selon la nature du transfert et les exigences applicables, les garanties peuvent notamment comprendre :

- un contrat de traitement des données ;
- des clauses de confidentialité ;
- des obligations relatives à la sécurité ;
- une limitation documentée des finalités ;
- des restrictions d'accès ;
- le chiffrement des communications ;
- le chiffrement ou la protection renforcée des données stockées ;
- une obligation de notification des incidents ;
- une procédure de retour, de suppression ou de destruction des données ;
- un droit d'obtenir des informations sur les sous-traitants ultérieurs ;
- des mécanismes permettant l'exercice des droits des personnes concernées.

Le consentement de la personne concernée n'est pas utilisé comme fondement général et systématique de tous les transferts.

Lorsqu'un consentement est juridiquement requis pour un transfert déterminé, il est recueilli séparément après que la personne a été informée :

- du pays ou des pays concernés ;
- du destinataire ;
- de la finalité ;
- des données transférées ;
- des garanties existantes ;

- des risques éventuels ;
- de la possibilité de retirer son consentement pour l'avenir.

Prestataires et localisations

Les pays et régions de traitement effectivement utilisés sont indiqués dans le tableau ou l'annexe consacrée aux prestataires.

Cette information est établie à partir :

- du contrat applicable ;
- du document de traitement des données du prestataire ;
- de la région sélectionnée dans le service ;
- de la liste des sous-traitants ultérieurs ;
- des informations techniques disponibles.

Lorsque plusieurs pays peuvent être concernés, la Politique indique les principaux pays ou catégories de pays et explique la raison de cette pluralité.

Droits des personnes

Toute personne concernée peut demander à EB GROUP ENTERPRISE :

- si ses données font l'objet d'un transfert international ;
- l'identité ou la catégorie des destinataires ;
- les pays concernés ;
- les principales garanties appliquées ;
- les modalités d'exercice de ses droits à l'égard des données transférées.

La demande est adressée à privacy@beayele.com.

Évolution des transferts

Lorsqu'un changement de prestataire ou de configuration entraîne un nouveau pays de traitement ou une modification substantielle des garanties, EB GROUP ENTERPRISE :

- met à jour la présente Politique ;
- actualise son registre des traitements ;
- accomplit les formalités complémentaires requises ;
- informe les personnes concernées lorsque cette information est nécessaire ;
- recueille un nouveau consentement uniquement lorsqu'il constitue le fondement juridiquement requis.

Application éventuelle d'une réglementation étrangère

EB GROUP ENTERPRISE est établie en République du Bénin et applique en priorité la réglementation béninoise relative à la protection des données à caractère personnel.

La présence d'un Utilisateur dans un autre pays ne rend pas automatiquement applicable l'intégralité de la réglementation de ce pays.

Une réglementation étrangère peut toutefois s'appliquer à certains traitements lorsqu'un critère d'application territoriale prévu par cette réglementation est effectivement rempli.

Lorsque les conditions d'application territoriale du Règlement général sur la protection des données de l'Union européenne sont réunies, notamment lorsque les services d'Ayélé sont spécifiquement proposés à des personnes se trouvant dans l'Union européenne ou lorsque leur comportement y fait l'objet d'un suivi, EB GROUP ENTERPRISE applique aux traitements concernés les obligations complémentaires requises.

L'applicabilité d'une réglementation étrangère est appréciée en fonction notamment :

- des pays expressément ciblés par les offres et communications d'Ayélé ;
- des devises et moyens de paiement proposés ;
- des campagnes commerciales réalisées ;
- de la possibilité de livrer ou fournir le service à des personnes établies dans le territoire concerné ;
- des activités de suivi ou de profilage éventuellement mises en œuvre ;
- des critères territoriaux prévus par la réglementation concernée.

L'application d'une réglementation étrangère à certains traitements ne modifie pas automatiquement le régime applicable aux autres Utilisateurs.

Sécurité et confidentialité des données

EB GROUP ENTERPRISE met en œuvre des mesures techniques et organisationnelles proportionnées :

- à la nature des données ;
- aux fonctionnalités utilisées ;
- au volume des traitements ;
- aux risques de perte, d'altération, de divulgation ou d'accès non autorisé ;
- aux conséquences possibles pour les personnes concernées.

Selon la nature du traitement, ces mesures comprennent notamment :

- la protection des communications entre le terminal de l'Utilisateur et la Plateforme au moyen de protocoles sécurisés ;
- la conservation des mots de passe sous forme d'empreintes cryptographiques sécurisées ne permettant pas leur restitution en clair ;

- l'attribution d'accès individuels aux outils d'administration ;
- l'authentification renforcée des comptes administrateurs et des accès sensibles ;
- la limitation des habilitations au besoin d'en connaître ;
- la journalisation des opérations administratives et financières sensibles ;
- la séparation entre les images destinées à être publiées et les justificatifs privés ;
- la protection renforcée des pièces d'identité, justificatifs médicaux et autres documents sensibles ;
- la sauvegarde des données nécessaires à la continuité du service ;
- la mise à jour régulière des composantes techniques ;
- la surveillance des incidents et activités anormales ;
- une procédure de traitement et de notification des violations de données ;
- l'encadrement contractuel des prestataires ayant accès aux données ;
- le réexamen périodique des accès et des mesures de sécurité.

Les documents sensibles ne sont accessibles qu'aux personnes spécifiquement habilitées et pendant la durée nécessaire à la finalité concernée.

EB GROUP ENTERPRISE veille à ce que les environnements de développement et de test n'utilisent pas de copies complètes de données réelles, sauf nécessité dûment encadrée. Lorsque des données réelles sont indispensables, leur utilisation est limitée, protégée et documentée.

Les clés d'API, mots de passe techniques, secrets d'authentification et identifiants administratifs ne sont pas intégrés dans les parties publiques du code informatique.

EB GROUP ENTERPRISE met en place une procédure permettant notamment :

- d'identifier un incident ;
- d'en limiter l'extension ;
- de préserver les éléments nécessaires à l'analyse ;
- de rétablir le service ;
- d'évaluer les risques pour les personnes ;
- d'effectuer les notifications requises ;
- de mettre en œuvre les mesures correctives nécessaires.

Aucun système informatique ne pouvant garantir une sécurité absolue, l'Utilisateur doit notamment :

- choisir un mot de passe robuste et unique ;

- protéger son téléphone et son adresse électronique ;
- ne jamais communiquer ses codes à usage unique ;
- vérifier l'adresse du site avant de saisir une information ;
- informer immédiatement Ayélé lorsqu'il soupçonne une compromission.

EB GROUP ENTERPRISE ne demande jamais par téléphone, courriel ou messagerie :

- le mot de passe complet d'un Utilisateur ;
- son code secret Mobile Money ;
- le code confidentiel de sa carte ;
- un code à usage unique destiné à valider une opération.

Cookies et autres traceurs

Principe

La Plateforme peut utiliser des cookies et technologies similaires afin :

- de permettre son fonctionnement ;
- de sécuriser les comptes et les opérations ;
- de mémoriser certains choix ;
- de mesurer l'utilisation de la Plateforme ;
- d'améliorer ses performances ;
- de proposer, lorsque cette fonctionnalité est activée, des contenus ou communications personnalisés.

Les détails relatifs aux cookies effectivement utilisés sont présentés dans la Politique relative aux cookies accessible séparément sur la Plateforme.

Cookies strictement nécessaires

Les cookies strictement nécessaires peuvent être utilisés sans consentement facultatif lorsqu'ils sont indispensables notamment :

- à l'authentification ;
- à la sécurité ;
- au maintien d'une session ;
- à la prévention de la fraude ;
- à l'enregistrement des choix de confidentialité ;
- au fonctionnement d'un formulaire ;

- au traitement technique d'une opération demandée par l'Utilisateur.

Le blocage de ces cookies dans le navigateur peut empêcher certaines fonctionnalités de fonctionner correctement.

Cookies facultatifs

Les cookies facultatifs ne sont déposés ou lus qu'après le recueil du choix de l'Utilisateur lorsque la réglementation exige son consentement.

Ils peuvent notamment concerner :

- la mesure d'audience non strictement nécessaire ;
- l'analyse détaillée du parcours utilisateur ;
- la personnalisation ;
- la publicité ;
- le suivi entre plusieurs services ou sites ;
- les contenus provenant de plateformes tierces.

Une catégorie de cookies n'est affichée dans le gestionnaire que si elle est réellement utilisée ou susceptible d'être activée dans la configuration en cours.

Bandeau de choix

Lors de sa première visite, l'Utilisateur peut notamment :

- accepter les cookies facultatifs ;
- refuser les cookies facultatifs ;
- personnaliser son choix par catégorie.

Les boutons permettant d'accepter et de refuser sont présentés avec une visibilité et une accessibilité comparables.

Aucune case relative aux cookies facultatifs n'est cochée par défaut.

La poursuite de la navigation, l'utilisation du défilement de la page ou la fermeture du bandeau ne valent pas automatiquement consentement lorsque celui-ci est requis.

Gestion et retrait du choix

L'Utilisateur peut modifier ou retirer son choix à tout moment au moyen :

- du lien « Gérer mes cookies » disponible sur la Plateforme ;
- du gestionnaire de confidentialité ;
- des paramètres de son navigateur.

Le retrait du consentement empêche les nouvelles utilisations facultatives concernées, sans remettre en cause les traitements réalisés avant ce retrait.

Preuve du choix

Ayélé conserve les informations nécessaires pour démontrer le choix exprimé, notamment :

- la date et l'heure ;
- les catégories acceptées ou refusées ;
- la version du bandeau ;
- un identifiant technique de consentement ;
- la date d'une modification ou d'un retrait.

La preuve du choix ne doit pas être utilisée à d'autres fins incompatibles.

Durée

La durée de vie de chaque cookie et la durée de validité du choix sont indiquées dans la Politique relative aux cookies.

Ayélé renouvelle la demande de choix lorsque :

- la durée de validité du consentement a expiré ;
- les finalités évoluent substantiellement ;
- de nouvelles catégories de cookies sont ajoutées ;
- un changement réglementaire l'exige.

Services de tiers

Lorsqu'une fonctionnalité tierce dépose ou lit des cookies, la Politique relative aux cookies identifie, dans la mesure du possible :

- le fournisseur ;
- la finalité ;
- les catégories de données ;
- la durée ;
- les modalités permettant de modifier le choix.

Aucun outil publicitaire ou de suivi tiers ne doit être activé avant que sa présence soit documentée et que le mécanisme de consentement approprié soit opérationnel.

Mineurs

Capacité à utiliser le service Ayélé

La création d'un compte Organisateur, la création d'une Cagnotte et la conclusion du contrat de service Ayélé sont réservées aux personnes physiques âgées d'au moins dix-huit ans et disposant de la capacité juridique nécessaire.

Le seuil applicable au consentement d'un mineur en matière de données personnelles ne lui confère pas la capacité de conclure seul les CGU/CGV ni de créer une Cagnotte en qualité d'Organisateur.

Mineur désigné comme Bénéficiaire

Une personne mineure peut être désignée comme Bénéficiaire d'une Cagnotte sous réserve :

- de l'intervention de son représentant légal ;
- de la vérification de l'autorisation nécessaire ;
- de la protection de son intérêt supérieur ;
- de la limitation des données publiées ;
- de l'absence d'exposition disproportionnée de sa vie privée, de sa santé ou de sa situation familiale.

L'Organisateur doit pouvoir justifier de sa qualité ou de l'autorisation du représentant légal.

Ayéle peut contacter directement le représentant légal et suspendre la Cagnotte tant que les vérifications ne sont pas achevées.

Consentement du mineur au traitement de ses données

Lorsqu'un traitement repose sur le consentement dans le cadre d'une offre directe de services de la société de l'information à un mineur :

- le mineur âgé d'au moins seize ans peut donner son consentement dans les conditions prévues par la réglementation ;
- lorsque le mineur est âgé de moins de seize ans, le consentement doit être donné ou autorisé par le titulaire de la responsabilité parentale ;
- EB GROUP ENTERPRISE met en œuvre des moyens raisonnables pour vérifier cette autorisation compte tenu des technologies disponibles.

Cette règle ne s'applique qu'aux traitements dont la base juridique est le consentement. Elle ne dispense pas Ayélé de respecter les autres conditions de licéité, de minimisation, de sécurité et de protection du mineur.

Publication des données d'un mineur

La page publique d'une Cagnotte concernant un mineur ne doit pas comporter, sauf nécessité particulière dûment justifiée :

- son adresse précise ;
- le nom de son établissement scolaire ;

- ses horaires ou lieux habituels ;
- son numéro de téléphone ;
- une pièce d'identité ;
- un acte d'état civil complet ;
- un dossier médical ;
- toute information facilitant sa localisation ou l'exposition de sa vulnérabilité.

Les photographies et informations relatives à la santé du mineur sont limitées à ce qui est nécessaire à la compréhension de la Cagnotte et doivent faire l'objet des autorisations requises.

Ayélé peut masquer ou supprimer tout contenu portant atteinte à la dignité, à la sécurité ou à la vie privée du mineur.

Communications commerciales et profilage

Ayélé n'utilise pas les données d'un mineur à des fins de prospection commerciale ou de profilage publicitaire sans avoir vérifié que les conditions légales spécifiques sont remplies.

Aucune Cagnotte impliquant un mineur ne doit être utilisée dans une communication promotionnelle extérieure sans autorisation distincte du représentant légal et vérification de l'intérêt du mineur.

Exercice des droits

Les droits relatifs aux données d'un mineur peuvent être exercés :

- par le mineur lorsque la réglementation et son niveau de capacité le permettent ;
- par le titulaire de la responsabilité parentale ;
- par un représentant légalement habilité.

Ayélé associe le mineur à l'exercice de ses droits autant que possible, en tenant compte de son âge, de sa capacité de compréhension et de son intérêt.

Communications nécessaires et communications commerciales

Communications nécessaires au service

Ayélé peut adresser sans consentement commercial distinct les communications nécessaires :

- à la création et à la sécurité du compte ;
- à l'authentification de l'Utilisateur ;
- à la création, à l'activation ou à la suspension d'une Cagnotte ;
- à la vérification de l'Organisateur ou du Bénéficiaire ;

- à la confirmation ou au suivi d'une Contribution ;
- à une Demande de Reversement ;
- à une Restitution ;
- à une Contestation de paiement ou une Rétrofacturation ;
- à l'expiration, l'inactivité ou l'abandon d'une Cagnotte ;
- à une modification importante des documents contractuels ;
- à un incident de sécurité ;
- au respect d'une obligation légale.

Ces communications font partie du fonctionnement du service concerné.

L'Utilisateur ne peut pas s'y opposer tant qu'elles sont nécessaires à l'exécution de son compte, de sa Cagnotte ou d'une opération en cours.

Communications commerciales d'Ayélé

Ayélé peut adresser des communications relatives notamment :

- à de nouvelles fonctionnalités ;
- à des conseils pour organiser une Cagnotte ;
- à des offres promotionnelles ;
- à des actualités d'Ayélé ;
- à des partenariats ou campagnes commerciales.

Lorsque le consentement est requis, ces communications ne sont adressées qu'après une acceptation distincte de l'Utilisateur.

Le choix est recueilli au moyen d'une case ou d'un mécanisme :

- clairement identifiable ;
- distinct de l'acceptation des CGU/CGV ;
- non activé par défaut ;
- formulé de manière compréhensible ;
- précisant les canaux concernés, notamment courriel ou SMS.

Le refus de recevoir des communications commerciales :

- n'empêche pas de créer un compte ;
- n'empêche pas de créer une Cagnotte ;
- n'affecte pas le traitement des Contributions ;

- ne modifie pas les tarifs applicables ;
- n'entraîne aucun désavantage sur les fonctionnalités principales.

Retrait du consentement et opposition

L'Utilisateur peut retirer son consentement ou s'opposer à la prospection commerciale à tout moment :

- au moyen du lien de désabonnement figurant dans les courriels concernés ;
- depuis les paramètres de son compte, lorsque cette fonctionnalité est disponible ;
- en adressant une demande à privacy@beayele.com ;
- au moyen de toute autre procédure simple indiquée dans le message reçu.

Le retrait est pris en compte pour les communications futures.

Un délai technique raisonnable peut être nécessaire pour mettre à jour l'ensemble des outils d'envoi. Pendant ce délai, Ayélé évite tout nouvel envoi non indispensable dans la mesure techniquement possible.

Preuve du choix

Ayélé conserve les informations nécessaires pour démontrer le choix de l'Utilisateur, notamment :

- l'identité ou l'identifiant de la personne ;
- le canal accepté ;
- la formulation présentée ;
- la date et l'heure ;
- la version du formulaire ;
- la source du consentement ;
- la date du retrait ou de l'opposition.

Cette preuve est conservée pendant la durée nécessaire pour démontrer le respect du choix de l'Utilisateur et gérer les réclamations.

Communication des données à des partenaires

Ayélé ne transmet pas les coordonnées d'un Utilisateur à un partenaire afin que celui-ci effectue sa propre prospection commerciale sans :

- informer préalablement l'Utilisateur de l'identité ou de la catégorie du partenaire ;
- préciser la finalité de la transmission ;
- recueillir un consentement distinct lorsque celui-ci est requis ;

- permettre le retrait ou l'opposition.

L'autorisation de recevoir les communications commerciales d'Ayélé ne vaut pas autorisation de recevoir les communications commerciales d'autres entreprises.

Mineurs

Ayélé n'utilise pas les données d'un mineur à des fins de prospection commerciale ou de profilage publicitaire sans vérification préalable des conditions légales et des autorisations nécessaires.

Situation au lancement

Lorsque les communications commerciales ne sont pas encore activées, la Plateforme n'affiche pas de case de consentement inutile.

La présente section s'applique dès l'activation effective de ces communications.

Droits des personnes concernées

Dans les conditions prévues par la réglementation applicable, toute personne concernée peut demander à EB GROUP ENTERPRISE :

Droits pouvant être exercés

Dans les conditions prévues par la réglementation applicable, toute personne concernée peut demander à EB GROUP ENTERPRISE :

- la confirmation que des données la concernant sont ou ne sont pas traitées ;
- l'accès aux données traitées et aux informations relatives à leur utilisation ;
- la rectification ou l'actualisation des données inexactes, incomplètes ou obsolètes ;
- l'effacement de données lorsque les conditions légales sont réunies ;
- la limitation ou le verrouillage temporaire d'un traitement ;
- l'opposition à un traitement fondé sur un intérêt légitime, pour des motifs tenant à sa situation particulière ;
- l'opposition, sans justification et sans frais, à l'utilisation de ses données à des fins de prospection commerciale ;
- le retrait, pour l'avenir, d'un consentement précédemment donné ;
- la portabilité de ses données lorsque ce droit est applicable ;
- des informations sur l'origine de ses données lorsqu'elles n'ont pas été recueillies directement auprès d'elle ;
- des informations sur les destinataires et les transferts internationaux de ses données ;

- le réexamen d'une décision exclusivement automatisée produisant un effet juridique ou un effet significatif comparable, lorsqu'une telle décision est mise en œuvre.

Le retrait d'un consentement ne remet pas en cause la licéité des traitements réalisés avant son retrait.

Limites à certains droits

L'exercice d'un droit ne permet pas d'obtenir :

- l'effacement de données qu'EB GROUP ENTERPRISE doit conserver en vertu d'une obligation légale ;
- la suppression de données nécessaires à l'exécution d'une opération encore en cours ;
- l'effacement d'éléments nécessaires à la constatation, à l'exercice ou à la défense d'un droit ;
- la modification rétroactive des données financières ou transactionnelles dont l'intégrité doit être préservée ;
- la suppression immédiate de données contenues dans des sauvegardes techniques, lorsque celles-ci sont isolées, protégées et supprimées selon leur cycle normal ;
- la communication de données portant atteinte aux droits et libertés d'un tiers.

Lorsqu'une demande ne peut être satisfaite intégralement, Ayélé explique au demandeur les raisons de cette limitation, sous réserve des informations dont la divulgation est légalement interdite.

Suppression du compte et effacement des données

La suppression du compte Ayélé n'entraîne pas automatiquement l'effacement immédiat de toutes les données.

Avant de clôturer le compte, Ayélé vérifie notamment :

- qu'aucune Cagnotte active ne subsiste ;
- qu'aucun Reversement ou aucune Restitution n'est en cours ;
- qu'aucune contestation ou Rétrofacturation n'est pendante ;
- qu'aucune somme ne reste due ;
- qu'aucune obligation légale ne s'oppose à la clôture.

Après la clôture, les données qui ne sont plus nécessaires sont supprimées ou anonymisées. Les données comptables, transactionnelles, de sécurité ou de preuve restent conservées pendant les durées prévues dans la présente Politique.

Décisions automatisées et contrôles de sécurité

À la date d'entrée en vigueur de la présente Politique, Ayélé ne prend pas de décision produisant un effet juridique ou un effet significatif comparable à l'égard d'un Utilisateur sur la seule base d'un traitement entièrement automatisé, sans possibilité d'intervention humaine.

La Plateforme peut utiliser des règles ou signaux automatisés afin notamment :

- d'identifier une activité inhabituelle ;
- de limiter une tentative de connexion ;
- de signaler une incohérence ;
- de classer temporairement une opération comme nécessitant une vérification ;
- d'empêcher provisoirement une opération présentant un risque immédiat.

Lorsqu'une mesure automatisée entraîne la suspension prolongée d'une Cagnotte, le refus d'un Reversement ou une autre conséquence significative, l'Utilisateur peut demander :

- l'examen de sa situation par une personne habilitée ;
- la communication des raisons générales de la décision, sous réserve de ne pas révéler les méthodes de détection de la fraude ;
- la possibilité de présenter ses observations et justificatifs ;
- la révision de la mesure.

Modalités d'exercice

Les demandes doivent être adressées :

- par courrier électronique à privacy@beayele.com ;
- ou par courrier postal à l'adresse d'EB GROUP ENTERPRISE indiquée dans la section « Contact ».

La demande doit préciser, dans la mesure du possible :

- les nom et prénoms du demandeur ;
- l'adresse électronique ou le numéro de téléphone associé au compte ;
- le droit exercé ;
- les données, la Cagnotte ou l'opération concernées ;
- toute information permettant de retrouver les données ;
- les motifs de la demande lorsque la réglementation les exige, notamment pour certaines demandes d'opposition.

Aucun mot de passe, code Mobile Money, code à usage unique ou numéro complet de carte bancaire ne doit être transmis dans une demande.

Vérification de l'identité du demandeur

Ayélé peut demander des informations complémentaires lorsqu'elle dispose d'un doute raisonnable sur l'identité du demandeur ou sur son pouvoir d'agir pour le compte d'un tiers.

Le justificatif demandé doit être proportionné au risque et aux données concernées.

Ayélé ne demande pas systématiquement une copie de pièce d'identité lorsqu'une vérification moins intrusive permet d'authentifier la personne, notamment :

- une confirmation depuis l'adresse électronique liée au compte ;
- une authentification dans l'espace utilisateur ;
- une vérification du numéro de téléphone ;
- la fourniture d'informations déjà connues de l'Utilisateur.

Lorsqu'une pièce d'identité est nécessaire, elle est utilisée uniquement pour traiter la demande et supprimée après la vérification, sauf obligation légale ou litige justifiant une conservation différente.

Traitement de la demande

Ayélé accuse réception de la demande dans un délai indicatif de cinq jours ouvrés.

Elle peut :

- demander des précisions ;
- vérifier l'identité ou le pouvoir de représentation du demandeur ;
- rechercher les données concernées ;
- consulter un Prestataire lorsque la demande porte sur un traitement relevant également de sa responsabilité ;
- informer le demandeur que tout ou partie de sa demande doit être adressé directement au Prestataire compétent.

Ayélé apporte une réponse dans les meilleurs délais et au plus tard dans le délai légal applicable au droit exercé.

Lorsque la réglementation permet une prolongation en raison de la complexité ou du nombre de demandes, Ayélé informe le demandeur :

- de la prolongation ;
- de ses motifs ;
- du nouveau délai estimé.

En cas de refus total ou partiel, Ayélé communique :

- les motifs généraux du refus ;
- les voies de recours disponibles ;
- la possibilité d'introduire une réclamation auprès de l'Autorité de Protection des Données Personnelles.

Représentation d'un tiers

Une demande peut être présentée par :

- le représentant légal d'un mineur ;
- le représentant d'une personne juridiquement protégée ;
- un mandataire disposant d'une autorisation valable ;
- un représentant légalement habilité d'une personne morale.

Ayélé peut demander tout document raisonnablement nécessaire pour vérifier la qualité du représentant ou l'étendue de son mandat.

Réclamation et recours

La personne concernée peut saisir l'Autorité de Protection des Données Personnelles lorsqu'elle estime que le traitement de sa demande ou de ses données n'est pas conforme à la réglementation.

L'exercice de ce recours ne l'empêche pas de rechercher une solution amiable avec Ayélé ni d'exercer les autres voies de recours prévues par la loi.

Violation de données à caractère personnel

Définition

Une violation de données à caractère personnel est un incident de sécurité entraînant, de manière accidentelle ou illicite :

- la destruction de données ;
- la perte de données ;
- l'altération de données ;
- leur divulgation à une personne non autorisée ;
- un accès non autorisé ;
- une perte temporaire ou définitive de disponibilité ;
- ou toute autre atteinte à leur confidentialité, leur intégrité, leur disponibilité ou leur traçabilité.

Peuvent notamment constituer une violation :

- l'accès frauduleux à un compte administrateur ;

- l'exposition publique accidentelle d'un justificatif privé ;
- l'envoi d'un document au mauvais destinataire ;
- la perte ou le vol d'un appareil contenant des données ;
- la compromission d'un prestataire ;
- la suppression accidentelle de données sans sauvegarde utilisable ;
- l'altération non autorisée des montants ou informations d'une Cagnotte ;
- la divulgation d'une pièce d'identité, d'un certificat médical ou d'un numéro Mobile Money.

Signalement d'un incident

Toute personne qui constate ou soupçonne une violation de données concernant Ayélé est invitée à la signaler sans délai à : privacy@beayele.com

Le signalement doit, dans la mesure du possible, indiquer :

- la date et l'heure de la découverte ;
- la nature de l'incident ;
- les données susceptibles d'être concernées ;
- les personnes potentiellement affectées ;
- les circonstances de l'incident ;
- les premières mesures éventuellement prises.

La personne ne doit pas transmettre publiquement les données compromises ni les joindre à un message lorsque cela n'est pas nécessaire.

Évaluation et confinement

Lorsqu'EB GROUP ENTERPRISE prend connaissance d'un incident réel ou suspecté, elle met en œuvre les mesures nécessaires pour :

- vérifier si une violation s'est effectivement produite ;
- identifier son origine et son périmètre ;
- empêcher la poursuite de l'accès ou de la divulgation ;
- sécuriser les comptes, clés et systèmes concernés ;
- préserver les éléments utiles à l'analyse ;
- restaurer les données ou services lorsque cela est nécessaire ;
- évaluer les conséquences possibles pour les personnes ;
- solliciter les Prestataires techniques ou financiers concernés ;

- déterminer les notifications et informations requises.

L'évaluation tient notamment compte :

- de la nature et de la sensibilité des données ;
- du nombre de personnes concernées ;
- de la possibilité d'identifier directement les personnes ;
- de l'existence de mesures de chiffrement ou de protection ;
- du risque de fraude, d'usurpation, de discrimination, de perte financière ou d'atteinte à la réputation ;
- de la situation particulière des mineurs et personnes vulnérables ;
- de la durée et de l'étendue de l'exposition.

Notification à l'APDP

Lorsqu'une notification à l'Autorité de Protection des Données Personnelles est requise, EB GROUP ENTERPRISE l'effectue dans les meilleurs délais après avoir acquis un degré raisonnable de certitude qu'une violation a eu lieu.

La notification contient, dans la mesure où ces informations sont disponibles :

- la nature de la violation ;
- les catégories de personnes concernées ;
- les catégories de données concernées ;
- le nombre approximatif de personnes ou d'enregistrements affectés ;
- les conséquences probables ;
- les mesures prises ou envisagées ;
- les coordonnées du point de contact d'EB GROUP ENTERPRISE.

Lorsque toutes les informations ne sont pas immédiatement disponibles, elles peuvent être communiquées progressivement dans les conditions prévues par la réglementation.

Information des personnes concernées

Lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, EB GROUP ENTERPRISE les informe dans les meilleurs délais, sauf lorsque la réglementation prévoit qu'une communication individuelle n'est pas nécessaire.

L'information est rédigée de manière claire et précise et indique notamment :

- la nature générale de l'incident ;
- les principales catégories de données concernées ;

- les conséquences possibles ;
- les mesures prises par Ayélé ;
- les précautions que la personne peut prendre ;
- les coordonnées du point de contact.

Selon l'incident, les précautions peuvent notamment comprendre :

- modifier son mot de passe ;
- sécuriser son adresse électronique ;
- contacter son opérateur Mobile Money ou sa banque ;
- surveiller les opérations inhabituelles ;
- se méfier des messages frauduleux ;
- ne communiquer aucun code à usage unique.

Ayélé ne minimise pas volontairement la portée d'une violation et ne demande aucun paiement pour assister une personne concernée par l'incident.

Incidents impliquant un Prestataire

Tout Prestataire agissant pour le compte d'EB GROUP ENTERPRISE doit informer celle-ci dans les meilleurs délais après avoir pris connaissance d'un incident affectant les données traitées pour Ayélé.

EB GROUP ENTERPRISE coopère avec le Prestataire afin de :

- identifier les données concernées ;
- contenir l'incident ;
- déterminer les responsabilités respectives ;
- effectuer les notifications requises ;
- informer les personnes concernées ;
- mettre en œuvre les mesures correctives.

Lorsqu'un Prestataire agit comme responsable de traitement indépendant, il demeure responsable de ses propres obligations de notification. Ayélé coopère néanmoins dans la limite des informations et moyens dont elle dispose.

Registre des violations et incidents

EB GROUP ENTERPRISE tient un registre interne centralisé des incidents et violations de données.

Ce registre peut notamment contenir :

- la date de découverte ;

- la nature de l'incident ;
- les systèmes et données concernés ;
- les personnes potentiellement affectées ;
- l'évaluation du niveau de risque ;
- les décisions prises ;
- les notifications réalisées ;
- les mesures de confinement ;
- les actions correctives ;
- la date de clôture de l'incident.

Les incidents sont documentés même lorsqu'ils ne donnent pas lieu à une notification à l'APDP ou aux personnes concernées.

Amélioration continue

Après un incident, EB GROUP ENTERPRISE examine notamment :

- son origine ;
- l'efficacité des mesures appliquées ;
- les défauts techniques ou organisationnels identifiés ;
- les besoins de mise à jour des procédures ;
- les actions nécessaires pour prévenir un incident similaire.

La présente Politique et les mesures de sécurité peuvent être actualisées à la suite de cet examen.

Réclamation auprès de l'Autorité de Protection des Données Personnelles

Toute personne qui estime que ses droits n'ont pas été respectés peut introduire une réclamation auprès de l'Autorité de Protection des Données Personnelles du Bénin (APDP), dont les coordonnées actualisées sont disponibles sur son site officiel. L'introduction d'une réclamation auprès de l'APDP ne prive pas la personne concernée des autres recours dont elle dispose.

Modification de la Politique

EB GROUP ENTERPRISE peut modifier la présente Politique afin notamment de tenir compte :

- d'une évolution de la Plateforme ;
- d'un changement dans les traitements ;

- de l'intégration ou du remplacement d'un Prestataire ;
- d'une nouvelle catégorie de données ;
- d'une modification des durées de conservation ;
- d'une évolution des transferts internationaux ;
- d'un changement législatif ou réglementaire ;
- d'une recommandation de l'Autorité de Protection des Données Personnelles ;
- d'une amélioration de la sécurité ou de la transparence.

Chaque version indique :

- son numéro ;
- sa date de publication ;
- sa date d'entrée en vigueur ;
- lorsque cela est utile, un résumé des principales modifications.

Une modification purement rédactionnelle ou destinée à améliorer la compréhension peut être publiée sans notification individuelle lorsqu'elle ne modifie pas substantiellement les traitements ou les droits des personnes.

Une modification substantielle est portée à la connaissance des personnes concernées par un moyen approprié, notamment :

- une notification dans le compte ;
- un courrier électronique ;
- un message visible sur la Plateforme.

Lorsque la modification introduit un traitement nécessitant un consentement, celui-ci est recueilli séparément avant l'activation du traitement concerné.

Une modification de la Politique ne peut pas :

- rendre rétroactivement licite un traitement qui ne l'était pas ;
- remplacer un consentement qui devait être recueilli séparément ;
- réduire rétroactivement les droits d'une personne ;
- étendre à une nouvelle finalité des données déjà collectées lorsque cette utilisation est incompatible avec l'information initialement fournie.

EB GROUP ENTERPRISE conserve un historique des versions et permet à l'Utilisateur d'identifier la version applicable au moment de la collecte de ses données ou de l'expression de son choix.

Contact

Pour toute question relative à la présente Politique, au traitement des données ou à l'exercice d'un droit, vous pouvez contacter EB GROUP ENTERPRISE :

- **Courriel dédié aux données personnelles :** XXXprivacy@beaye.com, ou à défaut ayele.africa@outlook.com avec la mention « Protection des données personnelles »
- **Téléphone :** +229 01 94 40 75 60
- **Adresse postale :** Îlot 1123, quartier Houéyiho, 11^e arrondissement, Cotonou, département du Littoral, République du Bénin

Entrée en vigueur

La présente Politique entre en vigueur à la date indiquée en première page et remplace toute version antérieure.