

Politique de confidentialité

Zamana · ZAMANA BUDDIES · Version révisée du 1er octobre 2026

VERSION À VALIDER AVANT PUBLICATION. Les mentions [À CONFIRMER] concernent les modalités encore non vérifiées, notamment le consentement biométrique et les paramètres Didit. Ce texte décrit les règles à appliquer et ne certifie pas leur mise en œuvre technique.

1. Qui est responsable de vos données ?

L'application Zamana est éditée par ZAMANA BUDDIES, société par actions simplifiée, dont le siège social est situé 17 allée des Sucriers, lotissement La Carib, 97229 Les Trois-Îlets, Martinique, France.

SIREN : 944 975 259. SIRET du siège : 944 975 259 00010. Numéro de TVA intracommunautaire : FR06944975259.

ZAMANA BUDDIES est responsable des traitements réalisés pour le fonctionnement de Zamana. Pour toute question ou demande concernant vos données, contactez contact@axelv.tech, adresse du référent données personnelles mandaté par ZAMANA BUDDIES, ou écrivez au siège social en précisant « Données personnelles - Zamana ».

Ce contact est un référent ; il n'est pas présenté comme un délégué à la protection des données officiellement désigné.

2. À qui s'adresse cette politique ?

Cette politique concerne les utilisateurs de Zamana sur iOS, Android et, lorsqu'elle est proposée, sa version web, ainsi que les organisateurs et partenaires utilisant les fonctionnalités correspondantes. Elle explique les données utilisées pour les comptes, la communauté, les événements, les offres, les paiements et les services techniques associés.

Zamana est réservée aux personnes âgées de 18 ans et plus. La date de naissance permet de vérifier cette condition. Si vous pensez qu'un mineur utilise le service, vous pouvez nous le signaler à l'adresse ci-dessus.

Les organisateurs ou partenaires peuvent traiter des données pour leurs propres activités. Lorsqu'ils agissent comme responsables indépendants, ils doivent vous fournir leurs propres informations de confidentialité.

L'essentiel

- Vos données servent à fournir les fonctionnalités que vous utilisez et à assurer leur sécurité.
- Certaines informations de profil et de participation peuvent être visibles par d'autres utilisateurs, selon les fonctionnalités et vos réglages.
- La localisation, la caméra, les images et les notifications disposent de contrôles spécifiques.
- Vous pouvez exercer vos droits en écrivant à contact@axelv.tech.
- Vous pouvez demander la suppression du compte et l'effacement ou l'anonymisation irréversible des données associées, sous réserve des exceptions légales expliquées dans cette politique.

3. Quelles données utilisons-nous et pourquoi ?

Compte et accès au service. Nous utilisons votre nom, prénom, e-mail, mot de passe enregistré sous forme de condensat, identifiant de compte, rôle, téléphone, ville, date de naissance et préférences. Ces données permettent de créer et gérer le compte, vous authentifier, réinitialiser l'accès, vérifier la majorité et vous contacter au sujet du service. Base légale : exécution du contrat, pour les seules données nécessaires au service ; intérêt légitime de protéger les utilisateurs pour la prévention des inscriptions de mineurs, après mise en balance de leurs droits.

Profil et communauté. Photo de profil, centres d'intérêt, favoris, relations et demandes d'amitié, réglages de visibilité, messages, images partagées et dates d'échange permettent les interactions demandées. Base légale : exécution du contrat. Les éventuels traitements de modération et de prévention des abus reposent sur notre intérêt légitime à protéger la communauté, avec des accès limités et proportionnés.

Événements et offres. Inscriptions, réservations, billets et codes QR, contrôle d'entrée, événements créés, offres réclamées ou utilisées, favoris et points de fidélité servent à organiser vos activités et à appliquer les avantages prévus. Base légale : exécution du contrat. Les coordonnées d'un lieu d'événement sont distinctes de votre position personnelle.

Paiements et abonnements. Nous utilisons les références de transaction, montants, statuts, factures, références d'abonnement et échéances pour traiter les achats, remboursements et abonnements. Base légale : exécution du contrat ; obligation légale pour les pièces comptables et fiscales. Les informations de carte sont traitées dans le parcours du prestataire de paiement Stripe. Zamana utilise les références et résultats de paiement pour gérer vos achats. Les informations de carte sont saisies auprès de Stripe, dans le parcours de paiement.

Notifications. Identifiant technique de notification de l'appareil, compte destinataire, préférences et contenu de notification permettent les alertes relatives aux messages, demandes d'amitié et activités. Base légale : exécution du contrat pour les alertes de service demandées. Les communications promotionnelles facultatives doivent faire l'objet d'un choix distinct ; leur activation ne conditionne pas l'accès au service.

Fonctions facultatives. La localisation sert à afficher votre position et les activités à proximité ; la caméra et les images servent aux photos, images de discussion et scans proposés. Le traitement nécessaire à une fonction expressément demandée repose sur le contrat. Si un usage excède cette nécessité, nous demandons un consentement préalable adapté. Les permissions techniques du téléphone et les consentements éventuels sont distincts.

Diagnostic et sécurité. Informations techniques sur l'appareil et le système, erreurs, traces de performance, dates et métadonnées réseau peuvent servir à corriger les incidents et sécuriser le service. Base légale : intérêt légitime pour les opérations strictement nécessaires et proportionnées ; consentement préalable pour les traceurs ou mesures facultatives qui le nécessitent.

4. D'où viennent vos données ?

Vous fournissez les informations de compte, le profil, les photos, messages, intérêts et contenus que vous publiez. L'utilisation de l'application génère des réservations, favoris, relations, points, transactions et informations techniques.

Un organisateur ou partenaire peut enregistrer une inscription ou l'utilisation d'une offre. Stripe transmet les statuts et références de paiement ; Didit transmet les résultats du parcours de vérification d'identité. Lorsque nous recevons des données indirectement, nous vous informons selon les conditions et délais prévus par le RGPD.

Les formulaires doivent distinguer les champs obligatoires et facultatifs. Le refus de fournir une donnée nécessaire peut empêcher la fonction concernée, par exemple la création du compte, une réservation ou un achat. Les données facultatives ne doivent pas être exigées pour accéder à une fonctionnalité qui n'en dépend pas.

5. Qui peut voir votre profil et vos contenus ?

Les informations de profil peuvent être consultées par les autres utilisateurs autorisés à accéder à cette fonction. Les réglages de masquage sont désactivés par défaut : la photo, le nom et les centres d'intérêt peuvent donc être visibles. Votre ville et vos contributions peuvent également apparaître dans les espaces concernés.

Vous pouvez modifier les options depuis Profil > Paramètres > Vie privée et notifications. L'option « Cacher mon nom complet » conserve actuellement le prénom et l'initiale du nom ; elle ne rend pas votre profil anonyme. L'option de masquage des événements doit s'appliquer aux affichages de participation concernés ; elle n'efface pas les informations nécessaires à l'organisateur pour gérer votre inscription.

Vos messages privés et images sont destinés aux interlocuteurs de la discussion. Les contenus d'une discussion d'événement sont accessibles aux participants habilités dans cet espace. Les organisateurs et partenaires reçoivent les informations nécessaires aux inscriptions, accès, réservations ou offres dont ils ont la charge.

Les échanges sont stockés sur les systèmes du service. Aucune garantie de chiffrement de bout en bout n'est fournie par cette politique. Les personnes habilitées peuvent accéder aux données lorsque cela est nécessaire au support, à la sécurité, à la modération ou au respect d'une obligation légale, dans les limites applicables.

Les e-mails, téléphones et dates de naissance ne doivent pas être exposés dans le profil communautaire. Vous êtes invité à ne pas publier de documents d'identité ou de données sensibles dans les discussions.

Si vous partagez un contenu avec une application externe, les informations que vous choisissez de transmettre relèvent également des règles de cette application. Les copies réalisées par un autre utilisateur peuvent subsister hors des systèmes de Zamana ; cela ne réduit pas nos obligations d'effacement sur nos propres systèmes.

6. Vos permissions et préférences

Localisation : vous pouvez refuser ou retirer l'autorisation dans les réglages du téléphone. La fonction de proximité utilise une position ponctuelle ; elle n'a pas pour finalité de constituer un historique de déplacements. La carte reste consultable sans afficher votre position, selon les fonctions disponibles. [À CONFIRMER : absence de conservation serveur et flux exacts du SDK cartographique.]

Caméra et images : l'accès est limité à la fonction que vous déclenchez. Privilégiez le sélecteur système pour choisir une image sans ouvrir l'ensemble de votre bibliothèque.

Notifications : modifiez vos préférences dans Zamana ou désactivez les notifications dans les réglages du téléphone. Leur contenu peut inclure le nom de l'expéditeur et un extrait de message, également visibles sur l'écran verrouillé selon vos réglages système.

7. Prestataires, hébergement et destinataires

Les données sont accessibles aux personnes habilitées de ZAMANA BUDDIES et aux intervenants techniques mandatés, uniquement dans le cadre de leurs missions. Les prestataires traitant des données sur nos instructions doivent être encadrés par des engagements de confidentialité, de sécurité et de protection des données adaptés, notamment un contrat conforme à l'article 28 du RGPD lorsqu'ils sont sous-traitants.

OVH / OVHcloud - hébergement. Les données hébergées chez OVHcloud sont situées en France, à Gravelines, selon la localisation confirmée par l'éditeur. Cela concerne l'hébergement OVH des systèmes du service et ne préjuge pas de la localisation des traitements propres aux autres prestataires.

Stripe - paiement. Reçoit les informations nécessaires au règlement et transmet les statuts, références de transactions et d'abonnements. Stripe peut exercer des responsabilités propres pour la sécurité des paiements et ses obligations réglementaires. Voir sa [politique de confidentialité](#).

Google Firebase Cloud Messaging et, sur iOS, le service de notifications Apple - acheminement des notifications. Traitent des identifiants d'appareil, données techniques et contenus nécessaires à l'envoi. Certains messages peuvent contenir des extraits de conversation. Voir les [informations Firebase](#) et la [politique Apple](#).

Google Maps - cartographie. Le chargement de la carte implique des communications avec les services Google et peut transmettre des métadonnées techniques et des informations relatives à la zone affichée. Les flux exacts dépendent du SDK et de sa configuration. Voir les [informations Google](#).

Didit - vérification d'identité. Reçoit les informations du parcours demandé et nous communique ses résultats. Les précisions et limites figurent à la section suivante et dans sa [notice de vérification](#).

GlitchTip - diagnostic technique. Logiciel open source utilisé pour suivre les erreurs et les performances de l'application. Toutes les données de cette instance sont hébergées chez OVHcloud, à Gravelines, en France, selon les informations confirmées par l'éditeur. Les informations techniques ne sont utilisées que pour les finalités de diagnostic et de sécurité décrites dans cette politique.

Google - messagerie transactionnelle. Le service d'envoi configuré pour les e-mails de compte traite votre adresse et les informations nécessaires au message, notamment pour la réinitialisation de l'accès. Voir les [informations Google](#).

Des autorités, conseils ou organismes habilités peuvent recevoir des données lorsqu'une obligation légale ou la défense de droits l'exige. Les organisateurs et partenaires accèdent uniquement aux données utiles à leurs missions ; leurs usages propres doivent être expliqués séparément.

8. Localisation des traitements et transferts

OVHcloud et GlitchTip : France, Gravelines. La localisation française concerne les données hébergées par Zamana chez OVHcloud et les données de son instance GlitchTip. Les services externes ont leurs propres infrastructures.

Didit : Union européenne par défaut. Sa documentation indique un traitement et un stockage par défaut sur AWS en Irlande, y compris pour les opérations biométriques. Son accord de traitement prévoit des garanties pour les éventuels transferts hors EEE. Cette localisation provient de la [documentation Didit](#), et ne signifie pas que les pièces sont hébergées sur les serveurs OVH de Zamana.

Stripe : traitements internationaux, notamment aux États-Unis. Sa notice et son [accord sur les transferts](#) prévoient le cadre de protection des données UE-États-Unis pour les entités et transferts couverts, ainsi que les clauses contractuelles types européennes selon les conditions applicables.

Google Firebase : infrastructure mondiale, dont des pays hors EEE. Les données de notifications peuvent être traitées dans les pays où Google ou ses sous-traitants disposent d'infrastructures, notamment aux États-Unis. Les [conditions Firebase](#), section 10, prévoient les mécanismes de transfert applicables, dont le cadre UE-États-Unis pour les entités certifiées et les clauses contractuelles types selon les cas. Les [sous-traitants et leurs lieux d'activité](#) sont publiés par Google.

Google Maps et messagerie Google : traitements internationaux possibles. Google décrit ses garanties dans ses [cadres de transfert](#). Google Maps documente également les [clauses contractuelles types applicables](#). Les responsabilités propres de Google et celles de Zamana dépendent du service concerné.

Apple : acheminement des notifications iOS. Les données nécessaires à cet acheminement relèvent aussi des infrastructures et garanties décrites dans sa [politique de confidentialité](#), qui prévoit des traitements internationaux.

Ces informations reprennent les documents officiels consultés le 1er octobre 2026. Les mécanismes de protection s'appliquent selon le fournisseur, l'entité destinataire, le contrat et le transfert concernés ; aucune garantie de stockage exclusivement français n'est donnée pour l'ensemble des services tiers. Vous pouvez demander les précisions et une copie des garanties pertinentes à contact@axelv.tech, avec les occultations nécessaires à la confidentialité de tiers.

9. Vérification des participants avec Dikit

La vérification est nécessaire pour confirmer l'identité des participants, renforcer la sécurité de chacun et vérifier les conditions d'accès au public prévu pour un événement, notamment la majorité. Elle ne sert pas à déduire des caractéristiques sensibles ou à sélectionner des personnes selon des critères discriminatoires.

Lorsque vous lancez le parcours, Zamana transmet à Dikit l'identifiant de votre compte, vos nom et prénom et votre date de naissance lorsqu'elle est renseignée. Vous fournissez à Dikit une pièce d'identité et un selfie ou une vidéo. Le dispositif contrôle le document, la présence réelle de la personne et compare son visage avec celui du document.

Dikit traite les images du document et du visage, les données extraites utiles au contrôle, les caractéristiques biométriques nécessaires à la comparaison, les informations techniques de session et le résultat. Zamana reçoit les références et le statut de vérification et les informations nécessaires au contrôle de votre profil. [À CONFIRMER : accès éventuel de Zamana aux pièces, captures, scores et gabarits dans la console ou via API.]

Base légale et protection des données biométriques

Pour le contrôle non biométrique, la finalité de sécurité et de prévention des usurpations correspond à l'intérêt légitime de ZAMANA BUDDIES, sous réserve d'une évaluation documentée de la nécessité et de la proportionnalité du dispositif.

La comparaison faciale destinée à vérifier une identité relève également des protections de l'article 9 du RGPD. L'intérêt légitime seul ne suffit pas à l'autoriser. En l'absence d'une autre exception légale applicable, ce parcours nécessite votre consentement explicite au traitement biométrique, en complément de la base légale de l'article 6.

Le consentement doit être recueilli avant la capture, après information sur les opérations, destinataires, conservation, retrait et conséquences du refus. La nécessité de vérifier une identité n'implique pas automatiquement celle d'imposer une comparaison biométrique.

[À CONFIRMER avant publication : dispositif de consentement explicite réellement actif ; alternative non biométrique et modalités d'accès aux événements en cas de refus ou retrait. Aucune alternative déjà déployée n'est affirmée dans ce projet.]

Pour contester un résultat ou demander un examen humain, contactez contact@axelv.tech. [À CONFIRMER : rôle des scores et existence éventuelle d'une décision entièrement automatisée ayant un effet significatif, ainsi que les informations et garanties de l'article 22 le cas échéant.]

Conservation et éventuelles réutilisations chez Didit

La durée utile du contrôle, les pièces et captures conservées ainsi que les éventuels gabarits sont distincts du simple statut « vérifié » enregistré dans Zamana. La finalisation du contrôle ne justifie pas, à elle seule, une conservation illimitée des pièces ou des données biométriques.

La [notice Didit](#) décrit des usages propres de sécurité et d'amélioration des modèles, dépendant notamment des paramètres de compte. [À CONFIRMER : durée finie configurée pour Zamana, conservation des gabarits et option de réutilisation réellement appliquée.] Vous pouvez adresser votre demande à Zamana ou, pour les usages dont Didit est responsable, à privacy@didit.me. Cette politique n'accorde aucun consentement global à ces usages secondaires.

10. Durées et critères de conservation

Nous limitons la conservation à ce qui est nécessaire à chaque finalité et appliquons les délais légaux français lorsqu'un texte en impose un. Il n'existe pas de délai légal unique pour toutes les données de l'application. Lorsqu'aucune durée n'est fixée par la loi, les critères suivants déterminent la durée utile en base active :

- Compte, profil, photo, intérêts et relations : maintien de la relation de service et utilisation du compte ; cessation de cette relation ou demande d'effacement lorsque aucune exception ne justifie de conserver les données. Le caractère inactif du compte doit faire l'objet d'un examen régulier et ne justifie pas une conservation sans limite.
- Événements, réservations, offres et points : exécution de la réservation ou de l'avantage, contrôle d'accès et traitement des remboursements ou réclamations associés. À la fin de ces besoins, les informations inutiles sont supprimées ou anonymisées irréversiblement.
- Messages et images : fonctionnement de la discussion et disponibilité du contenu pour ses participants ; suppression recevable du compte ou des contenus et fin de l'utilité de la discussion, en tenant compte des droits des autres personnes. Les copies internes de notifications sont soumises au même principe de nécessité.
- Localisation : traitement temporaire pour la fonction de proximité demandée, sans finalité d'historique des déplacements. Les éventuelles données techniques du fournisseur cartographique relèvent également de ses conditions.
- Jetons de notification : validité du jeton et utilisation de la fonction ; remplacement, invalidation, retrait de la fonction ou effacement du compte entraînent leur retrait lorsqu'ils ne sont plus nécessaires.
- Diagnostic GlitchTip : identification, analyse et résolution des incidents ou problèmes de sécurité concernés ; seules les informations justifiées par une investigation encore ouverte peuvent être conservées au-delà de sa résolution.
- Pièces, captures et biométrie Didit : réalisation du contrôle et résolution d'une éventuelle contestation justifiée ; conservation séparée du statut minimal utile. La durée finie du parcours doit être configurée et cohérente avec ces besoins, comme précisé à la section 9.
- Sauvegardes : durée nécessaire à leur rotation et à la reprise du service ; accès restreint et réapplication des effacements lors d'une restauration. Une sauvegarde ne doit pas remettre durablement en circulation des données effacées.

Obligations légales et archivage distinct de l'usage courant

Les pièces comptables et justificatifs, dont les factures, sont conservés 10 ans à partir de la clôture de l'exercice concerné. Certains contrats électroniques conclus avec un consommateur, notamment à partir de 120 euros, sont soumis à une conservation de 10 ans selon les règles applicables. Les preuves nécessaires à un litige sont limitées aux éléments utiles et à la prescription pertinente, généralement 5 ans en matière civile, sous réserve des points de départ, interruptions et exceptions propres au cas.

Les informations ainsi conservées sont distinguées des données utilisées au quotidien et leur accès est restreint. Aucun archivage permanent du profil complet n'est prévu au seul motif de satisfaire une obligation comptable.

11. Suppression du compte et anonymisation

Vous pouvez lancer la suppression depuis Profil > Paramètres > Supprimer mon profil. Vous pouvez également envoyer une demande à contact@axelv.tech, y compris après avoir désinstallé l'application.

La suppression peut être réalisée par effacement ou anonymisation irréversible, sous réserve des données dont une obligation légale ou un litige justifie la conservation. Des lignes techniques peuvent être maintenues pour préserver la cohérence de la base uniquement si elles ne permettent plus raisonnablement de vous identifier, directement ou par rapprochement avec d'autres données.

Une simple substitution du nom ou de l'e-mail ne constitue pas une anonymisation si des photos, dates, messages, identifiants ou autres informations permettent encore de retrouver la personne. Les données pseudonymisées restent soumises aux règles de protection des données et aux demandes de droits.

Les demandes doivent couvrir les données associées devenues inutiles et les instructions nécessaires aux prestataires. Les seules exceptions concernent des obligations ou besoins précisément justifiés ; elles sont limitées dans leur objet, leurs accès et leur durée. Les conséquences sur vos réservations et votre abonnement doivent être indiquées lors de la demande.

L'URL du PDF de confidentialité n'est pas un formulaire de suppression. [À CONFIRMER pour Google Play : URL publique de la ressource externe permettant la demande de suppression du compte.]

12. Vos droits

Dans les conditions prévues par le RGPD, vous pouvez :

- demander l'accès à vos données et une copie compréhensible ;
- faire rectifier des informations inexactes ou incomplètes ;
- demander l'effacement ou la limitation d'un traitement ;
- recevoir les données que vous avez fournies dans un format structuré, couramment utilisé et lisible par machine lorsque la portabilité s'applique ;
- vous opposer, pour des raisons tenant à votre situation, à un traitement fondé sur l'intérêt légitime ;
- vous opposer à tout moment à la prospection commerciale ;
- retirer un consentement à tout moment, sans remettre en cause la licéité du traitement effectué avant le retrait ;
- bénéficier des garanties applicables en matière de décision entièrement automatisée ;
- définir des directives sur le sort de vos données après votre décès, dans les conditions de la loi française.

Écrivez à contact@axelv.tech, en indiquant le compte concerné et votre demande, ou adressez votre courrier au siège de ZAMANA BUDDIES. Une vérification d'identité proportionnée peut être demandée en cas de doute raisonnable ; une copie de pièce d'identité ne doit pas être exigée systématiquement.

Nous répondons en principe dans un délai d'un mois à compter de la réception. Une prolongation de deux mois est possible lorsque la complexité ou le nombre de demandes le justifie ; vous en êtes informé dans le premier mois avec les motifs. Les demandes sont en principe gratuites, sous réserve des exceptions prévues par le RGPD pour les demandes manifestement infondées ou excessives.

Vous pouvez déposer une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL) : cnil.fr/fr/plaintes, ou par courrier à la CNIL, 3 place de Fontenoy, TSA 80715, 75334 Paris Cedex 07. Vous pouvez également saisir l'autorité compétente de votre résidence habituelle, lieu de travail ou lieu de la violation alléguée dans les conditions prévues par le RGPD.

13. Maîtrise de vos données et sécurité

Vous gardez la maîtrise de vos données grâce aux réglages de votre profil, aux permissions du téléphone et aux droits décrits ci-dessus. Vous pouvez demander l'accès, la rectification, l'effacement, la limitation, la portabilité lorsqu'elle s'applique, et retirer un consentement.

Ces droits s'exercent dans les conditions légales : certaines données ne peuvent pas être effacées immédiatement lorsqu'une obligation impose leur conservation, et le retrait d'une permission peut rendre indisponible la fonction qui en dépend. Cela n'autorise pas à réutiliser les données pour une autre finalité sans base légale.

ZAMANA BUDDIES est tenue de protéger les données par des mesures techniques et organisationnelles adaptées, notamment des accès limités aux personnes habilitées et des communications protégées. La gestion des droits et préférences ne supprime pas les obligations de sécurité de l'éditeur.

Des jetons et préférences sont stockés sur votre appareil pour maintenir la connexion et le service demandé. Les opérations strictement nécessaires peuvent être exemptées de consentement au titre de l'article 82 de la loi Informatique et Libertés. Les traceurs ou mesures facultatives qui nécessitent un consentement doivent rester bloqués avant votre choix, avec un refus et un retrait simples.

[À CONFIRMER : qualification des traces de performance et inventaire des traceurs des versions mobile et web, ainsi que le dispositif de choix lorsqu'il est requis.] GlitchTip est utilisé pour le diagnostic technique ; cette finalité ne dispense pas d'évaluer les opérations effectivement réalisées sur le terminal.

14. Évolution de la politique

Nous mettons à jour cette politique lorsque les traitements ou le cadre applicable changent. La version et la date sont indiquées au début du document. Toute modification importante est portée à votre connaissance par un moyen adapté avant son application lorsque cela est nécessaire. Un nouvel usage nécessitant un consentement ne peut pas être autorisé par la seule mise à jour du texte.

Version révisée le 1er octobre 2026. Cette version s'appliquera après sa validation et sa publication effective.

Adresse prévue du PDF : www.zamanabuddies.com/confidentialite.pdf. La présente génération de fichier ne constitue pas sa mise en ligne.