IDENTITY CHECKER

RGPD, traitement des données personnelles.
15 février 2023 (remis en forme de 26 février 2023)

CADRE

Identity checker est une application Discord permettant la vérification des membres pour accéder à la communauté non officielle de l'Hénallux.
Ce renforcement de sécurité est dû à des évènements rencontrés qui ont nui à la sécurité des utilisateurs sur cette communauté en ligne.

Les données traitées par l'application ne sont utilisées qu'à but de vérification et ne sont pas communiquées à des tiers.

Identity Checker n'est en aucun cas lié à la Haute École que ce soit par ses membres du personnel ou par ses représentants.

HÉBERGEMENT DE L'APPLICATION ET DES DONNÉES

Les serveurs hébergeant les données du serveur de base de données ainsi que l'application sont situés à Paris chez la société Oracle Corporation (oracle.com).

L'application est conteneurisée grâce à Docker sur un réseau isolé. Le serveur de base de données est isolé de toute connexion externe. L'application ne communique qu'à travers les serveurs de la société Discord Inc (discord.com).

Le serveur de base de données est un serveur MariaDB mis à jour constamment dans les plus brefs délais suivant la sortie d'une mise à jour.

DONNÉES STOCKÉES PAR L'APPLICATION

Afin de garantir son bon fonctionnement, il est indispensable pour l'application de stocker des données. Notamment afin de prévenir l'utilisation des emails plusieurs fois.

Identity Checker garde dans une base de données les informations suivantes :

- Identifiant utilisateur Discord
- Email de l'utilisateur haché
- Code reçu par email
- Timestamp du moment où la vérification a été demandée.

L'application a été réfléchie pour n'utiliser que les permissions nécessaires à son bon fonctionnement.

SÉCURITÉ DES INFORMATIONS PERSONNELLES

Afin de garantir l'anonymisation des données, l'email de chaque utilisateur est haché. L'application utilise la fonction de hachage SHA3-256 considéré comme fiable au moment de l'écriture de ce document.

Les infrastructures utilisent des clés RSA 4096. Les disques durs des machines ainsi que les communications sur ceux-ci sont chiffrés par Oracle.

DEMANDES D'ACCÈS AUX DONNÉES PERSONNELLES

Chaque utilisateur peut demander de lui-même ses données et recevoir une réponse immédiate (indisponible en cas de maintenance ou de panne).

La demande se fait par le biais une requête sur l'application avec « /info ».
L'utilisateur recevra alors un message avec l'entièreté des informations stockées sur lui. Cependant, il n'aura pas le code de vérification envoyé par mail pour des raisons de sécurité.

DEMANDES DE SUPPRESSION DE DONNÉES PERSONNELLES

Les demandes de suppression de données sont faites automatiquement par l'application par le biais d'une simple requête d'un utilisateur (indisponible en cas de maintenance ou de panne).

Le serveur communautaire n'étant pas reconnu par la Haute École et n'étant pas soumis à une demande de sauvegarde des données par une autorité compétente, la demande est exécutée dès la demande de l'utilisateur.

Cependant, il est important de noter qu'un utilisateur demandant la suppression de ses données accepte de perdre ses accès au serveur communautaire. Dès la suppression des données, nous ne pouvons pas vérifier si une adresse email est déjà utilisée. Dès lors, nous retirons les accès pour ne valider l'email que pour un seul membre.

Les demandes de suppression des données sont impactées par la rétention des données de 72 heures expliquée au point suivant.

RÉTENTION DES DONNÉES

Afin d'assurer une tolérance aux pannes et assurer un service accessible, un système de sauvegardes est mis en place. Ce service sauvegarde toutes les heures le système de base de données ainsi que celui de l'application.

La sauvegarde des données est faite toutes les heures. Les fichiers de sauvegardes sont conservés 72 heures après leur création. Ensuite, ils sont supprimés automatiquement.

Les sauvegardes sont chiffrées à l'aide du cipher AES256.
Les données sont conservées pour une durée maximale de 7 ans. Au-delà de ce délai, les données sont supprimées. L'utilisateur devra repasser la vérification pour relancer un cycle de 7 ans de conservation et d'accès.