

Aperçu de l'analyse

INFORMATIONS GÉNÉRALES



éditer

100%

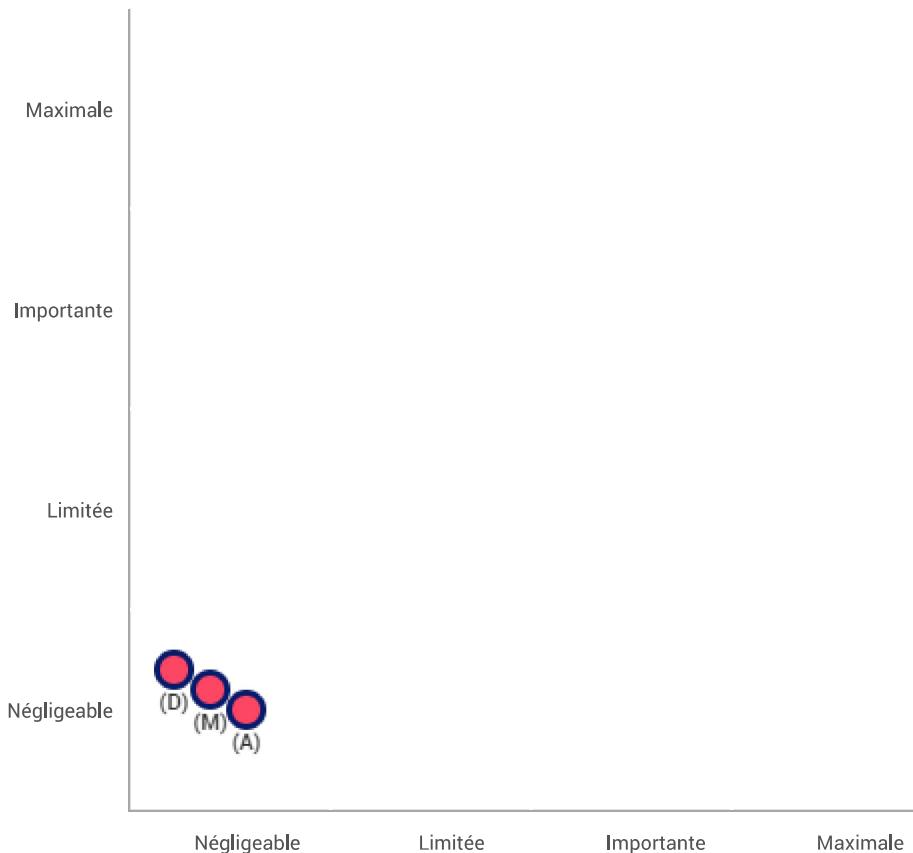
Aperçu

Saisie : Déborah GENETET Statut : Validation simple
Évaluation : Junior SEDOGBO
Validation : Ali ESSASSI

Validation

Cartographie des risques

Gravité du risque



- Mesures prévues ou existantes
- Avec les mesures correctives mises en oeuvre
- (A)ccès illégitime à des données
- (M)odification non désirée de données
- (D)isparition de données

Vraisemblance du risque

06/12/2024

Validation

Plan d'action

Vue d'ensemble

Principes fondamentaux	Mesures existantes ou prévues
Finalités	Chiffrement
Fondement	Clé d'accès.
Données adéquates	
Données exactes	
Durée de conservation	
Information des personnes	
Recueil du consentement	
Droit d'accès et à la portabilité	
Droit de rectification et d'effacement	Accès illégitime à des données
Droit de limitation et d'opposition	Modification non désirée de données
Sous-traitance	Disparition de données
Transferts	

Mesures Améliorables

Mesures Acceptables

Principes fondamentaux

Aucun plan d'action enregistré.

Mesures existantes ou prévues

Aucun plan d'action enregistré.

Risques

Aucun plan d'action enregistré.

Validation

Avis du DPD et des personnes concernées

Nom du DPD

Sansané Hugo, Waxin Alban, Krill Maxence, Schell Jules, Guyot Joshua, Essassi Ali, Sedogbo Sosthene, Genetet Déborah

Opinion du DPD

Pas besoin de traiter les données, pas de raisons.

Recherche de l'avis des personnes concernées

L'avis des personnes concernées n'a pas été demandé.

Raison pour laquelle l'avis des personnes concernées n'a pas été demandé

L'avis des personnes n'a pas été demandé car leurs données personnelles ne sont pas collectées.

Contexte

Vue d'ensemble

Quel est le traitement qui fait l'objet de l'étude ?

Le traitement étudié dans ce PIA concerne une application web éducative et interactive qui explore les parallèles entre les systèmes humains et océaniques. L'objectif est de sensibiliser les utilisateurs, par une approche ludique et immersive, aux mécanismes biologiques et environnementaux, en illustrant les bénéfices d'un bon fonctionnement et les impacts des dysfonctionnements.

Cette application, accessible en HTTPS et ne collectant aucune donnée personnelle, vise un usage éducatif dans des contextes scolaires ou individuels. Elle permet d'approfondir les connaissances sur les liens entre la santé humaine et la préservation des écosystèmes, tout en garantissant un haut niveau de sécurité et de confidentialité.

Quelles sont les responsabilités liées au traitement ?

Les huit développeurs (Sansané Hugo, Waxin Alban, Krill Maxence, Schell Jules, Guyot Joshua, Essassi Ali, Sedogbo Sosthene, Genetet Déborah) sont coresponsables du traitement et partagent équitablement la responsabilité de la conception, du déploiement, et de la gestion de l'application. Ils garantissent collectivement la conformité au RGPD, notamment en matière de sécurité et de respect des droits des utilisateurs : l'application ne collecte aucune donnée personnelle.

Quels sont les référentiels applicables ?

Le principal référentiel applicable à ce traitement est le Règlement Général sur la Protection des Données (RGPD), qui impose des principes tels que la sécurité dès la conception (privacy by design) et par défaut (privacy by default). Même si aucune donnée personnelle n'est collectée, il est essentiel de démontrer que la plateforme garantit la confidentialité et la sécurité des interactions des utilisateurs.

Les normes de sécurité reconnues, comme l'ISO/IEC 27001 pour la gestion de la sécurité de l'information et l'ISO/IEC 27005 pour la gestion des risques, peuvent être utilisées pour structurer les mesures de sécurité et évaluer les risques techniques liés à la plateforme. Par ailleurs, le respect des recommandations de la CNIL, notamment en matière de développement sécurisé et de protection contre les vulnérabilités courantes, renforce la conformité du projet.

Enfin, il est possible de prendre en compte des référentiels complémentaires, comme le guide OWASP pour prévenir les vulnérabilités des applications web, et le Référentiel Général d'Amélioration de l'Accessibilité (RGAA) pour garantir une application accessible et inclusive. Ces éléments assurent que l'application respecte les meilleures pratiques techniques, juridiques et éthiques.

Évaluation : Acceptable

Contexte

Données, processus et supports

Quelles sont les données traitées ?

Dans le cadre de cEAUrps, **aucune donnée personnelle n'est collectée, stockée ou traitée**. Les interactions des utilisateurs avec la plateforme sont entièrement anonymes. Ainsi, aucun accès à des données utilisateur personnellement identifiable n'est requis ni possible pour l'équipe de développement ou tout autre tiers. Seuls des éléments techniques, tels que l'user-agent de l'utilisateur et le chemin de la ressource demandée, sont enregistrés par le serveur.

Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?

Il n'y a pas de cycle de vie des données personnelles. En effet, l'application fonctionne de manière purement interactive : les utilisateurs explorent le contenu éducatif directement via leur navigateur, ce qui ne nécessite ni enregistrement, ni suivi, ni traitement de données personnelles.

Ainsi, aucune donnée n'est collectée, traitée ou conservée à aucun moment. Cela reflète un choix délibéré de minimisation des risques liés à la vie privée et à la sécurité des données.

Les connexions sont sécurisées grâce au protocole HTTPS, garantissant la confidentialité et l'intégrité des échanges entre le navigateur et le serveur.

Quels sont les supports des données ?

L'application utilise les serveurs sécurisés de Versem pour son hébergement. Les systèmes informatiques des développeurs sont utilisés pour le développement, le déploiement et la maintenance de l'application, avec des logs techniques mais sans données personnelles. Aucun support papier n'est utilisé.

Les seules données pouvant être conservées localement sur les appareils des utilisateurs sont l'historique de navigation.

Évaluation : Acceptable

Principes fondamentaux

Proportionnalité et nécessité

Les finalités du traitement sont-elles déterminées, explicites et légitimes ?

Les finalités du traitement sont déterminées : aucun traitement. L'utilisateur n'est pas prévenu que ses données ne sont pas traités. Ce non traitement n'est donc pas explicite. Les finalités de traitement ne sont pas illégitimes.

Évaluation : Acceptable

Quel(s) est(sont) les fondement(s) qui rend(ent) votre traitement licite ?

Il n'y a pas de traitement donc le traitement ne peut pas être illicite.

Évaluation : Acceptable

Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?

Les données collectées sont entièrement minimisées.

Évaluation : Acceptable

Les données sont-elles exactes et tenues à jour ?

Aucune donnée personnelle n'est collectée, stockée ou traitée, donc la question de l'exactitude et de la mise à jour des données personnelles ne se pose pas. En revanche, les données techniques, comme l'user-agent et le chemin de la ressource demandée, sont générées automatiquement lors de l'interaction avec la plateforme. Ces données sont purement techniques et ne nécessitent pas de mise à jour ou de vérification d'exactitude, car elles n'ont pas vocation à identifier un utilisateur ou à être utilisées au-delà de l'amélioration du fonctionnement de l'application.

Évaluation : Acceptable

Quelle est la durée de conservation des données ?

Les seules informations techniques enregistrées par le serveur, telles que l'user-agent de l'utilisateur et le chemin de la ressource demandée, sont temporaires. Ces données sont conservées pendant 30 jours.

Évaluation : Acceptable

Principes fondamentaux

Mesures protectrices des droits

Comment les personnes concernées sont-elles informées à propos du traitement ?

Les personnes concernées ne sont pas explicitement informées du traitement des données, car aucune donnée personnelle n'est collectée, traitée ou conservée. L'application fonctionne de manière entièrement anonyme, et les interactions avec les utilisateurs ne génèrent aucune donnée identifiable.

Évaluation : Acceptable

Si applicable, comment le consentement des personnes concernées est-il obtenu ?

Non applicable.

Évaluation : Acceptable

Comment les personnes concernées peuvent-elles exercer leurs droit d'accès et droit à la portabilité ?

Non applicable.

Évaluation : Acceptable

Comment les personnes concernées peuvent-elles exercer leurs droit de rectification et droit à l'effacement (droit à l'oubli) ?

Non applicable.

Évaluation : Acceptable

Comment les personnes concernées peuvent-elles exercer leurs droit de limitation et droit d'opposition ?

Non applicable.

Évaluation : Acceptable

Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?

Non applicable.

Évaluation : Acceptable

En cas de transfert de données en dehors de l'Union européenne, les données sont-elles protégées de manière équivalente ?

Il est possible que les données techniques soient conservées en dehors de l'UE car Versem a des serveurs dans différentes régions du monde. Les données sont protégées de manière équivalente, elles restent anonymes.

Évaluation : Acceptable

Risques

Mesures existantes ou prévues

Chiffrement

Toutes les connexions, entre le serveur Versem et l'utilisateur se font en SSL/TLS via le protocole https.

Évaluation : Acceptable

Clé d'accès.

Pour se connecter au serveur et push, une clé est requise. A noter que cette clé est présente côté serveur, dans des variables d'environnement non publique.

Évaluation : Acceptable

Risques

Accès illégitime à des données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Etant donné qu'aucune donnée personnelle n'est collectée, un accès illégitime aux données techniques (comme l'user-agent ou le chemin de la ressource demandée) aurait un impact limité. Les principales causes pourraient être une faille de sécurité ou un piratage. Les conséquences seraient principalement techniques, comme la possibilité de cibler des vulnérabilités de l'application, mais

sans danger direct pour la vie privée des utilisateurs. La gravité du risque est faible, d'autant plus que les communications sont sécurisées en HTTPS.

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Les principales menaces qui pourraient permettre un accès illégitime aux données techniques incluent des vulnérabilités du serveur, comme une mauvaise configuration ou des failles de sécurité dans le logiciel utilisé. Des attaques par interception, notamment des attaques Man-in-the-Middle, pourraient aussi se produire si la connexion n'est pas sécurisée, bien que HTTPS atténue ce risque. De plus, une mauvaise gestion des accès internes ou externes ou l'exploitation de logs non sécurisés pourraient permettre à un attaquant d'obtenir des informations techniques non sensibles.

Quelles sources de risques pourraient-elles en être à l'origine ?

Les sources de risques pouvant être à l'origine d'un accès illégitime à des données peuvent être des attaquants externes, des personnes mal intentionnées qui haïssent les océans, ou nos concurrents, les autres participants à la nuit de l'info 2024.

Quelles sont les mesures initiales, parmi celles identifiées, qui contribuent à traiter le risque ?

Chiffrement, Clé d'accès.

Comment estimatez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Négligeable, Étant donné qu'aucune donnée personnelle identifiable (PII) n'est collectée, le potentiel d'impact sur la vie privée des utilisateurs est extrêmement faible.

Comment estimatez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Négligeable, Aucune donnée personnelle identifiable n'est collectée, ce qui diminue l'attractivité des données pour les attaquant.

Évaluation : Acceptable

Risques

Modification non désirée de données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Étant donné qu'aucune donnée collectée n'est traitée, l'impact est nul.

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Les principales menaces qui pourraient le permettre incluent des vulnérabilités du serveur, comme une mauvaise configuration ou des failles de sécurité dans le logiciel utilisé. Des attaques par interception, notamment des attaques Man-in-the-Middle, pourraient aussi se produire si la connexion n'est pas sécurisée, bien que HTTPS atténue ce risque. De plus, une mauvaise gestion des accès internes ou externes pourraient permettre à un attaquant de modifier des informations techniques non sensibles., Altération des données sur le serveur

Quelles sources de risques pourraient-elles en être à l'origine ?

Les sources de risques pouvant en être à l'origine peuvent être des attaquants externes, des personnes mal intentionnées qui haïssent les océans, ou nos concurrents, les autres participants à la nuit de l'info 2024.

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque :

Chiffrement, Clé d'accès.

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Négligeable, Étant donné qu'aucune donnée personnelle identifiable (PII) n'est collectée, le potentiel d'impact sur la vie privée des utilisateurs est extrêmement faible.

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Négligeable, Aucune donnée collectée n'est traitée, ce qui diminue l'intérêt d'une attaque.

Évaluation : Acceptable

Risques

Disparition de données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Étant donné qu'aucune donnée collectée n'est traitée, l'impact est nul.

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Les principales menaces qui pourraient le permettre incluent des vulnérabilités du serveur, comme une mauvaise configuration ou des failles de sécurité dans le logiciel utilisé. De plus, une mauvaise gestion des accès internes ou externes pourraient permettre à un attaquant de supprimer des informations techniques non sensibles.

Quelles sources de risques pourraient-elles en être à l'origine ?

Les sources de risques pouvant être à l'origine d'un accès illégitime à des données peuvent être des attaquants externes, des personnes mal intentionnées qui haïssent les océans, ou nos concurrents, les autres participants à la nuit de l'info 2024.

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Chiffrement, Clé d'accès.

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Négligeable, Étant donné qu'aucune donnée personnelle identifiable (PII) n'est collectée ou utilisée, le potentiel d'impact sur la vie privée des utilisateurs est extrêmement faible.

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Négligeable, Aucune donnée collectée n'est traitée, ce qui diminue l'intérêt d'une attaque.

Évaluation : Acceptable

Risques

Vue d'ensemble des risques

Impacts potentiels

