Aperçu de l'analyse

INFORMATIONS GÉNÉRALES

éditer

100%

Aperçu

Saisie : FREMONT Vincent, **Statut :** Validation simple
Évaluation : DPO de PrivateRun
Validation : PDG de PrivateRun

Validation

Cartographie des risques

Gravité du risque

Vraisemblance 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

02/03/2024

Validation

Plan d'action

Vue d'ensemble

Principes fondamentaux | Mesures existantes ou prévues

Principes fondamentaux

Finalités
Fondement
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
Droit de limitation et d'opposition
Sous-traitance
Transferts

Mesures existantes ou prévues

Chiffrement

Risques

Accès illégitime à des données
Modification non désirée de données
Disparition de données

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

Fremont Vincent

Statut du DPD

Le traitement pourrait être mis en oeuvre.

Opinion du DPD

Oui, le traitement est justifié. Les objectifs sont clairs, les utilisateurs ont consenti et des mesures de sécurité sont en place.

Recherche de l'avis des personnes concernées

L'avis des personnes concernées a été demandé.

Noms des personnes concernées

Noms des personnes concernées

utilisateur de la montre

Statuts des personnes concernées

Le traitement pourrait être mis en oeuvre.

Opinions des personnes concernées

Les avis des personnes concernées ont été collectés via un formulaire de consentement. Si aucune recherche d'avis n'a été entreprise, cela peut être dû à plusieurs raisons, comme un consentement implicite, des bases légales alternatives ou l'absence de besoin jugé nécessaire.

Contexte

Vue d'ensemble

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

Le traitement qui fait l'objet de l'étude est le processus complet d'acquisition, de stockage et de traitement des données de course à pied issues des montres connectées des utilisateurs par la société PrivateRun.Le traitement des données implique l'ensemble des opérations réalisées sur les données de course à pied depuis leur acquisition jusqu'à leur présentation aux utilisateurs via PrivateRun.

Quelles sont les responsabilités liées au traitement ?

Les responsabilités liées au traitement des données dans ce contexte impliquent plusieurs parties prenantes, chacune ayant des rôles spécifiques :

1.Les utilisateurs: Les utilisateurs doivent consentir au traitement de leurs données et s'assurer de l'installation et de l'utilisation correcte du logiciel PrivateRun sur leur montre connectée, ainsi que de l'envoi sécurisé de leurs données vers les serveurs de PrivateRun.

2.PrivateRun: PrivateRun est chargé de développer, maintenir et sécuriser le logiciel pour l'acquisition, le stockage et le traitement des données des utilisateurs. Ils doivent garantir la transparence et la sécurité du processus de consentement des utilisateurs, ainsi que la protection des données stockées sur leurs serveurs.

3.SuperCloudProvider: SuperCloudProvider fournit une infrastructure cloud pour le stockage et le traitement des données à PrivateRun, garantissant la fiabilité, la disponibilité et la sécurité des serveurs cloud.

4.Webcourses: Webcourses surveille l'utilisation des données pour assurer la conformité aux politiques de confidentialité, de la protection des données
et contribuer à leur élaboration.

Quels sont les référentiels applicables ?

Utilisateurs :

Le consentement sur traitement des données
La sécurisation des informations sur l'identification.

PrivateRun :

Développement, maintenance la sécurité du logiciel.
Collecte transparente du consentement des utilisateurs.
La confidentialité et la sécurité des données stockées.
il y a aussi la disponibilité et la précision des informations dans le site web.

SuperCloudProvider :

SuperCloudProvider :

La fourniture de l'infrastructure cloud sécurisée et fiable.

Webcourses :

Surveillance de l'utilisation des données.
Contribution à l'élaboration des politiques de protection des données.

Évaluation : Acceptable

Contexte

Données, processus et supports

Quelles sont les données traitées ?

La liste des données traitées et leur durée de conservation sont les : Données de géolocalisation avec la positions géographiques et la durée de conservation n'est pas mentionné Les données d'identification avec le nom, prénom, date de naissance, identifiant de la montre connectée et la durée de conservation est seulement pendant l'utilisation du service, ou jusqu'à demande de supprimer le compte.

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

Acquisition des données :

Les données de course sont collectées par la montre connectée pendant l'activité physique de l'utilisateur.
Stockage et Transfert :

Les données sont stockées localement sur la montre.
Elles peuvent être transférées vers les serveurs de PrivateRun sur le cloud.
Traitement :

Les données sont traitées sur les serveurs de PrivateRun pour générer des statistiques et des cartes de chaleur.
Présentation :

Les résultats du traitement sont présentés sur le site web de PrivateRun, avec une partie privée pour les utilisateurs authentifiés et une partie publique.
Consentement des Utilisateurs :

Le consentement des utilisateurs est obtenu via un formulaire pour le stockage et le traitement de leurs données conformément aux finalités spécifiées.

Suppression :

À la fin de leur cycle d'utilisation ou sur demande de l'utilisateur, les données peuvent être supprimées de manière sécurisée des serveurs de PrivateRun et de la montre connectée, conformément aux politiques de conservation des données de l'entreprise et aux exigences réglementaires en matière de protection des données.

Quels sont les supports des données ?

Les supports des données sont:

- Dans la Montre en local grace au logiciel propriétaire

- Dans un serveur de PrivateRun loué à la société SuperCloudProvider sur un logiciel de PrivateRun

Évaluation : Acceptable
Commentaire d'évaluation :
Les mesures de protection des données de PrivateRun semblent solides, avec le consentement des utilisateurs par formulaire signé et la séparation des données sur le site web. L'utilisation de serveurs cloud sécurisés renforce la sécurité, mais il est crucial de gérer les accès et les mises à jour régulièrement.

Principes fondamentaux

Proportionnalité et nécessité

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

Oui, les finalités de traitement des données sont déterminées, explicites et légitimes. Elles sont spécifiées dans le formulaire de consentement signé par les utilisateurs et incluent l'affichage privé des traces des utilisateurs ainsi que la présentation anonyme des traces de tous les coureurs.

Évaluation : Acceptable
Commentaire d'évaluation :
Il serait judicieux d'envisager l'introduction d'une clause dans le formulaire de consentement permettant aux utilisateurs de révoquer leur consentement à tout moment. Cela renforcerait davantage la transparence et la protection des données, offrant aux utilisateurs un plus grand contrôle sur l'utilisation de leurs informations personnelles. Cette mesure serait conforme aux normes de confidentialité des données et améliorerait la conformité aux réglementations en matière de protection de la vie privée.

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

Le traitement des données par PrivateRun est rendu licite grâce au consentement explicite des utilisateurs, au respect de leur vie privée, à la légitimité des finalités du traitement et à la transparence dans la collecte et l'utilisation des données.

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) ?

Oui, les données collectées par PrivateRun sont adéquates, permanentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées, répondant ainsi au principe de minimisation des données.

Évaluation : Acceptable

Les données sont-elles exactes et tenues à jour ?

Les données collectées par PrivateRun à partir des montres connectées des utilisateurs sont généralement précises, étant donné qu'elles sont issues des capteurs de géolocalisation en temps réel. Cependant, leur exactitude dépend de la qualité des capteurs de la montre. En ce qui concerne leur mise à jour, elle dépend de la fréquence à laquelle les utilisateurs synchronisent leurs montres avec l'application. PrivateRun doit s'assurer que ces données sont correctes en mettant en place des

processus de vérification. En ce qui concerne le consentement, PrivateRun le recueille via un formulaire signé par les utilisateurs, incluant leur nom, prénom, date de naissance et géolocalisation, pour les deux finalités déclarées.

Évaluation : Acceptable

Quelle est la durée de conservation des données ?

Pour toutes les données stockées, la durée de conservation est de 1 an

Évaluation : Acceptable

Principes fondamentaux

Mesures protectrices des droits

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

Les utilisateurs sont informés du traitement de leurs données par PrivateRun via un formulaire de consentement explicite, des politiques de confidentialité et des notifications lors de la collecte de données.

Évaluation : Acceptable

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

Le consentement des utilisateurs est obtenu par PrivateRun via un formulaire signé où les utilisateurs spécifient leur consentement pour le traitement de leurs données. Ce formulaire inclut des informations sur les données collectées, les finalités du traitement et les modalités de stockage et de traitement. Les utilisateurs ont la possibilité d'accepter ou de refuser chaque finalité de traitement proposée.

Évaluation : Acceptable

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

Les personnes concernées peuvent exercer leur droit d'accès et de portabilité en demandant à PrivateRun une copie de leurs données personnelles stockées et en demandant le transfert de ces données vers un autre service ou système.

Évaluation : Acceptable

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

Les personnes concernées peuvent exercer leur droit de rectification et leur droit à l'effacement (droit à l'oubli) en contactant PrivateRun pour demander la correction ou la suppression des données incorrectes, inappropriées ou obsolètes les concernant. PrivateRun doit alors prendre les mesures nécessaires pour rectifier ou supprimer ces données conformément aux exigences légales en matière de protection des données.

Évaluation : Acceptable

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

Les personnes concernées peuvent exercer leur droit de limitation et leur droit d'opposition en contactant PrivateRun

pour demander la restriction du traitement de leurs données personnelles ou pour s'opposer à certains types de traitement, tels que la diffusion de leurs données de manière anonyme dans le cadre de l'affichage des cartes de chaleur. PrivateRun est tenu de respecter ces demandes, sauf si des motifs légitimes impérieux prévalent sur les droits et libertés de la personne concernée.

Évaluation : Acceptable

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

Les obligations des sous-traitants doivent être clairement définies dans un contrat conforme à la législation sur la protection des données. Ce contrat doit préciser les responsabilités, les exigences en matière de sécurité des données, et les conditions de traitement des données personnelles. Les sous-traitants doivent s'engager à respecter toutes les obligations légales et à ne pas utiliser les données à d'autres fins que celles convenues avec PrivateRun.

Évaluation : Acceptable

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

Pour garantir la protection des données lors de leur transfert en dehors de l'Union européenne, PrivateRun doit s'assurer qu'elles bénéficient d'un niveau de protection équivalent à celui assuré dans l'UE. Cela peut être réalisé en utilisant des mécanismes de transfert approuvés, comme les clauses contractuelles types de la Commission européenne ou les règles d'entreprise contraignantes.

Évaluation : Acceptable

Risques
Mesures existantes ou prévues

Chiffrement

PrivateRun assure la confidentialité et l'intégrité des données en utilisant un cryptage des données en transit et au repos. L'accès aux données est strictement contrôlé par des mécanismes d'authentification robustes, et les activités sont surveillées pour détecter toute anomalie. Des mises à jour régulières sont effectuées pour maintenir la sécurité des systèmes.

Évaluation : Acceptable

Risques
Accès illégitime à des données

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

Si un risque survient chez PrivateRun, les utilisateurs pourraient subir des impacts tels que la violation de la vie privée, des risques pour la sécurité, une confidentialité compromise et des préjudices financiers.

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

Principales menaces sont : Piratage informatique Vol ou perte de la montre connectée Erreurs

humaines Défaillance technique Attaques par phishing

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

Sources de risques : Failles de sécurité Perte ou vol de la montre Erreurs humaines Attaques de pirates Non-respect des normes de protection des données

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

Chiffrement

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

Importante, L'estimation de la gravité du risque dépend des impacts potentiels et des mesures prévues. Les impacts potentiels incluent les conséquences sur la vie privée et la confiance des utilisateurs, tandis que les mesures prévues comprennent les protocoles de sécurité et les mécanismes de protection des données. Une analyse combinée de ces facteurs permet d'évaluer la gravité du risque.

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

Limitée, La vraisemblance du risque dépend des menaces, des sources de risques et des mesures de sécurité mises en place.

Évaluation : Acceptable

Risques

Modification non désirées de données

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

Les principaux impacts potentiels sur les utilisateurs pourraient inclure : Violation de la vie privée Risques pour la sécurité Perte de contrôle sur les informations personnelles Utilisation abusive des données Altération de l'intégrité des données

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

Les principales menaces incluent : Violation de la confidentialité. Piratage des serveurs. Accès non autorisé. Défaillance du système.

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

Les sources de risques possibles comprennent : Vulnérabilités dans le logiciel de PrivateRun. Failles de sécurité sur les serveurs de SuperCloudProvider. Mauvaise gestion des identifiants et des accès. Erreurs humaines lors du traitement des données. Attaques de pirates informatiques.

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

Chiffrement

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

Limitée, La gravité du risque est modérée à élevée, selon la sensibilité des données collectées et l'efficacité des mesures de protection mises en place.

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

Limitee,

La vraisemblance du risque dépend des mesures de sécurité. Si elles sont robustes, le risque est faible à modéré. Sinon, il peut être modéré à élevé.

Évaluation : Acceptable

Risques

Disparition de données

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

Le principal impact pourrait être une violation de la vie privée et un risque pour la sécurité des utilisateurs.

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

Les principales menaces qui pourraient permettre la réalisation du risque comprennent les violations de la vie privée des utilisateurs, les fuites de données personnelles, les cyberattaques visant les serveurs de stockage et les risques liés à la sécurité des données lors du transfert entre la montre connectée et les serveurs cloud.

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

Les principales sources de risques : comprennent Vulnérabilités dans le logiciel de la montre connectée. Attaques contre les serveurs cloud. Insuffisances dans la protection des données. Défaillances du consentement utilisateur., Les principales sources de risques comprennent : Vulnérabilités dans le logiciel de la montre connectée. Attaques contre les serveurs cloud. Insuffisances dans la protection des données. Défaillances du consentement utilisateur.

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

Chiffrement

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

Limitée,

La gravité du risque dépend de la sensibilité des données collectées et du potentiel d'impact sur la vie privée des utilisateurs. Les mesures de sécurité prévues, telles que le cryptage des données et le consentement explicite des utilisateurs, contribueront à atténuer ce risque.

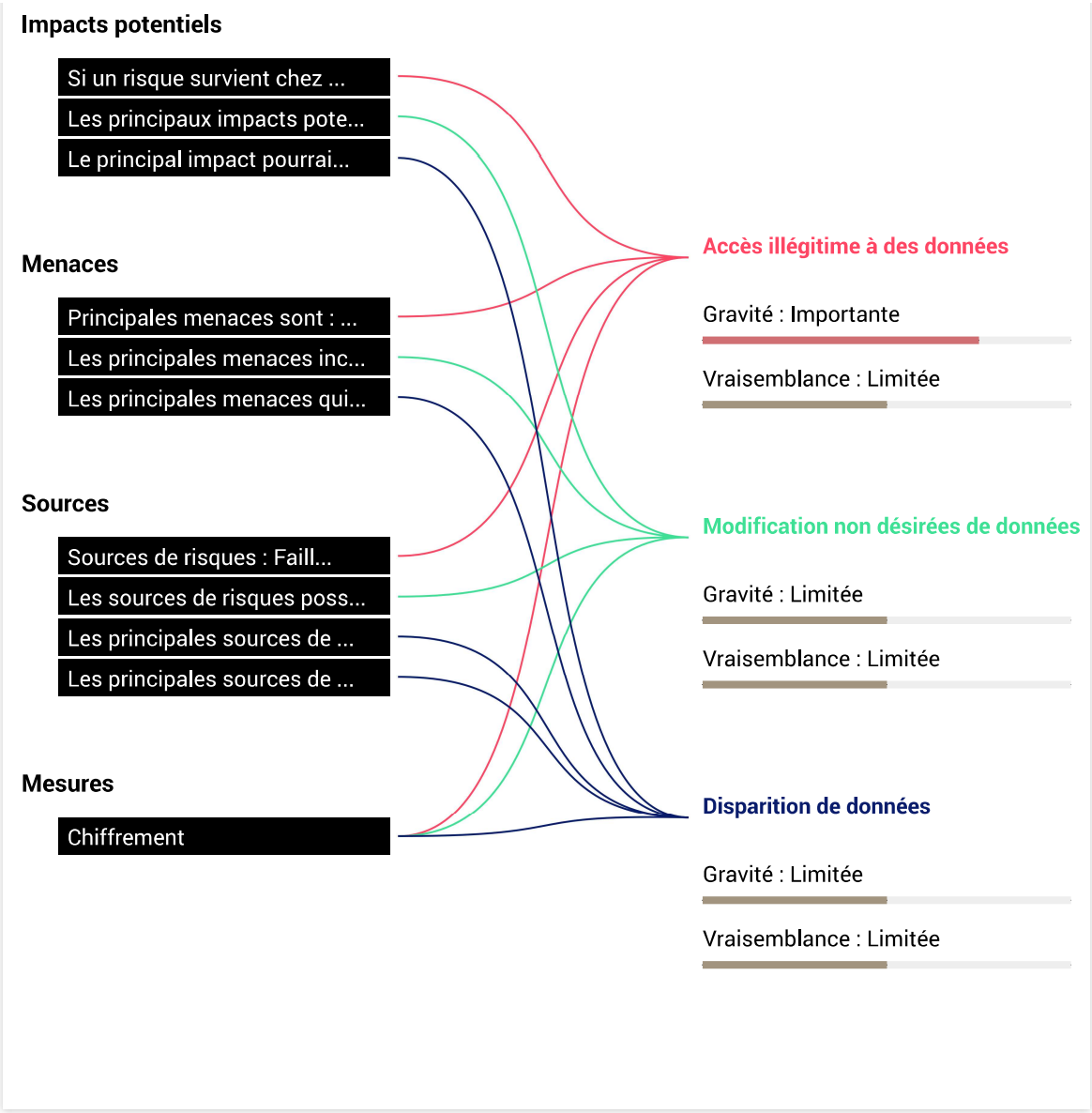
Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Limitée, La vraisemblance du risque dépend de la sécurité des mesures prises par PrivateRun. Les menaces comme les cyberattaques peuvent augmenter ce risque, mais des mesures telles que le cryptage des données peuvent le réduire.

Évaluation : Acceptable

Risques

Vue d'ensemble des risques


Impacts potentiels
Si un risque survient chez ...
Les principaux impacts pote...
Le principal impact pourrai...
Menaces
Principales menaces sont : ...
Les principales menaces inc...
Les principales menaces qui...
Sources
Sources de risques : Faill...
Les sources de risques poss...
Les principales sources de ...
Les principales sources de ...
Mesures
Chiffrement
Accès illégitime à des données
Gravité : Importante
Vraisemblance : Limitée
Modification non désirées de données
Gravité : Limitée
Vraisemblance : Limitée
Disparition de données
Gravité : Limitée
Vraisemblance : Limitée