PIA Montre PrivateRun

Saisie :
Anthony AFONSO
Clément ARKI
Évaluation :
DPO de PrivateRun
Validation :
PDG de PrivateRun
Statut :
En cours
0%

Validation

Cartographie des risques

Validation

Plan d'action

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

M. DPO

Statut du DPD

Le traitement pourrait être mis en oeuvre.

Recherche de l'avis des personnes concernées

L'avis des personnes concernées a été demandé.

Noms des personnes concernées

M. DPO

Statuts des personnes concernées

Le traitement pourrait être mis en oeuvre.

Contexte

Vue d'ensemble

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

PrivateRun a développé un système nommé "Gestion des données de course", intégré à leur application. La finalité est qu'il vise à garantir le stockage, l'analyse et le partage sécurisés des données de course des utilisateurs de montres connectées.

- Les enjeux sont le respect de la vie privée et la convivialité
- Le contexte et d'intégré à l'application PrivateRun pour les utilisateurs de montre connectées
- Les conctionnalités sont l'acquisiation des données, stockage sécurisé, analyse pour afficher les traces de coruse privées de gérérer des cartes de chaleur anonymes, consentement utilisateur
- Le traitement des données est réalisé dans le strct respect du consentement utilisateur
- Le traitement des données est conforme au consentement utilisateur, assurant une gestion sécurisée tout en préservant la confidentialité

Quelles sont les responsabilités liées au traitement ?

Responsabilités liées au traitement des données :

- Responsable du traitement : PrivateRun est chargée d'assurer la conformité avec les réglementations sur la protection des données et de collecter le consentement des utilisateurs.
- Utilisateurs : Ils doivent fournir un consentement éclairé et peuvent exercer leurs droits sur leurs données conformément à la législation en vigeur
- Sous -traitants : Ils doivent respecter les instructions de PrivateRun et mettre en oeuvre des mesures de sécurité adéquates pour protéger les données
- Co-responsable: En partageant la responsabilité, toutes les parties doivent garantir la conformité légale en matière de protection des données

Quels sont les référentiels applicables ?

Les référentiels applicatbles sont :

- Le RGPD (avec la CNIL)
- Les normes de sécurité informatique (ex : ISO 27001)
- Les accord de confidentialité
- Les normes de protection
- Codes de conduite approuvés : Lignes directrices spécifiques pour le traitement des données

Évaluation : Acceptable

Contexte

Données, processus et supports

Quelles sont les données traitées ?

Géolocalisation :

Collectées : Position, vitesse, date et heure.
- Conservation : Localement sur la montre et sur les serveurs de PrivateRun la durée dépend des préférences de l'utilisateur et des politiques de rétention.

Données personnelles :

- Collectées : Nom, prénom, date de naissance.
- Conservation : Sur les serveurs de PrivateRun, durée dépend de l'utilisation du service et des exigences légales.

Destinataires et accès :

- Utilisateurs : Accès à leurs données de géolocalisation via l'application PrivateRun.
- PrivateRun : Accès à toutes les données collectées pour fournir ses services.
- SuperCloudProvider : Accès aux données sur ses serveurs selon le contrat avec PrivateRun.
- Utilisateurs autorisés : Accès à leurs propres données via la partie privée du site web avec login, et accès à des données anonymisées dans la partie publique.

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

Cycle de vie des données :

- Collecte : Les données de course sont collectées depuis la montre connectée de l'utilisateur et via un formulaire de consentement pour les données personnelles.

- Stockage : Les données sont stockées localement sur la montre et sur les serveurs de PrivateRun hébergés par SuperCloudProvider.

- Traitement : Les données sont traitées sur les serveurs pour générer des cartes de chaleur et d'autres analyses.

- Accès : Les utilisateurs accèdent à leurs propres données via l'application et à des données anonymisées sur le site web public. Les utilisateurs autorisés peuvent accéder à leurs données privées sur le site web.

- Archivage et destruction : Les données peuvent être archivées pour conservation ou détruites selon les politiques de rétention de PrivateRun et les demandes des utilisateurs.

Quels sont les supports des données ?

Supports des données :

Systèmes informatiques : Logiciels sur les montres et serveurs pour la collecte, le stockage et le traitement des données.

Serveurs : Serveurs de PrivateRun chez SuperCloudProvider pour stocker et traiter les données.

Réseau : Transfert des données entre montres, serveurs et cloud.

Personnes : Utilisateurs et personnel de PrivateRun.

Support papier : Formulaire de consentement utilisateur.

Évaluation : Acceptable

Principes fondamentaux

Proportionnalité et nécessité

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

Oui, les objectifs du traitement des données sont bien définis, clairs et légitimes. Ils sont explicitement indiqués dans le formulaire de consentement, permettant aux utilisateurs d'autoriser PrivateRun à traiter leurs données pour afficher leurs traces de course de manière privée (F1) ou anonyme (F2), en accord avec les services proposés et les principes de protection de la vie privée.

Évaluation : Acceptable

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

Le traitement des données est fondé sur le consentement des utilisateurs, recueilli via un formulaire signé, où les utilisateurs autorisent explicitement PrivateRun à traiter leurs données personnelles. Ce consentement constitue le fondement légal du traitement, conformément aux principes de la réglementation sur la protection 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) ?

Les données collectées par PrivateRun, telles que le nom, prénom, date de naissance et géolocalisation, sont nécessaires pour les finalités du traitement. Chaque donnée est essentielle pour identifier les utilisateurs, personnaliser l'expérience et suivre leurs trajets de course. Elles sont adéquates, pertinentes et limitées à ce qui est strictement nécessaire pour atteindre les objectifs du traitement, respectant ainsi le principe de minimisation des données.

Évaluation : Acceptable

Les données sont-elles exactes et tenues à jour ?

PrivateRun garantit la qualité des données en les validant lors de leur acquisition, en les stockant de manière sécurisée sur leurs serveurs avec des sauvegardes régulières, et en les mettant à jour selon les nouvelles trajectoires enregistrées par les utilisateurs.

Évaluation : Acceptable

Quelle est la durée de conservation des données ?

La durée de conservation des données dépend de leur utilisation. Les données de géolocalisation sont conservées tant que l'utilisateur utilise le service, tandis que les données personnelles sont conservées jusqu'à ce que leur usage devienne inutile ou que l'utilisateur retire son consentement, en l'absence d'obligation légale spécifique.

Évaluation : Acceptable

Principes fondamentaux

Mesures protectrices des droits

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

Les personnes concernées sont informées du traitement de leurs données par PrivateRun via un formulaire de consentement, qui précise les types de données collectées, les finalités du traitement, les moyens de stockage et de présentation, ainsi que leur droit de retirer leur consentement à tout moment.

Évaluation : Acceptable

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

Les utilisateurs concernés donnent leur consentement pour le traitement de leurs données via un formulaire signé, dans lequel PrivateRun précise les types de données collectées, les finalités du traitement, ainsi que les moyens de stockage et de présentation des données.

Évaluation : Acceptable

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

Les utilisateurs peuvent contacter PrivateRun pour exercer leur droit d'accès afin de consulter leurs données personnelles et les télécharger dans un format structuré et couramment utilisé s'ils souhaitent les transférer à un autre responsable du traitement.

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 contacter PrivateRun pour exercer leur droit de rectification afin de mettre à jour leurs données personnelles inexactes ou incomplètes. De plus, elles peuvent également demander l'effacement de leurs données, y compris leurs traces de géolocalisation, en envoyant une demande à PrivateRun.

Évaluation : Acceptable

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

Les personnes concernées peuvent exercer leurs droits de limitation et d'opposition en contactant PrivateRun selon les procédures définies par le RGPD.

Évaluation : Acceptable

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

Les obligations des sous-traitants sont clairement définies dans des contrats, des codes de conduite ou des certifications, établissant leurs responsabilités spécifiques en matière de traitement des données.

Évaluation : Acceptable

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

En cas de transfert de données hors de l'UE, des mesures équivalentes garantissent la protection des données, soit par reconnaissance de la conformité du pays tiers, soit par des clauses contractuelles spécifiques.

Évaluation : Acceptable

Risques

Mesures existantes ou prévues

Chiffrement

Le chiffrement est utilisé pour sécuriser les données collectées à partir des montres connectées des utilisateurs, ainsi que lors de leur transmission vers les serveurs de PrivateRun et leur stockage.

Évaluation : Acceptable

Anonymisation

L'anonymisation est utilisée pour masquer les données personnelles des utilisateurs lors de l'affichage des traces de tous les coureurs sur le site web de PrivateRun, conformément à la finalité F2.

Évaluation : Acceptable

Cloisonnement

Les données des utilisateurs sont cloisonnées pour assurer une séparation entre les finalités F1 et F2. Cela est réalisé en stockant les données de manière distincte sur le serveur, avec des autorisations d'accès restreintes.

Évaluation : Acceptable

Contrôle des accès logiques

Les profils utilisateurs sont définis selon les besoins d'accès et les actions autorisées, puis attribués en fonction de ces critères.

Évaluation : Acceptable

Journalisation

Les événements sont journalisés pour assurer la traçabilité des actions effectuées sur les données. La durée de conservation de ces traces est déterminée en fonction des exigences légales et des besoins opérationnels de l'entreprise.

Évaluation : Acceptable

Archivage

Les données personnelles sont archivées électroniquement avec des mesures de sécurité appropriées, conformément aux exigences légales. La durée de conservation est déterminée par les obligations légales et les besoins opérationnels, avec une politique de gestion des archives en place.

Évaluation : Acceptable

Minimisation des données

Les données sensibles sont collectées de manière minimale, limitant ainsi la quantité d'informations personnelles stockées.

Évaluation : Acceptable

Risques

Accès illégitime à des données

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

Violation de la vie privée, Risque de vol d'identité, Perte de confiance, Possibilité de surveillance non autorisée, Risque de discrimination

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

Piratage, Perte ou vol de données, Accès non autorisé, Utilisation abusive des données géolocalisées, Erreurs humaines

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

Failles de sécurité dans le logiciel, Insuffisance des mesures de sécurité, Manque de formation du personnel, Politiques de sécurité inadéquates, Non-respect des réglementations en matière de protection des données

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

Chiffrement, Anonymisation, Cloisonnement, Contrôle des accès logiques

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

Limitée,

Car les mesures prévues telles que le chiffrement, l'anonymisation, le cloisonnement et le contrôle des accès logiques sont en place pour atténuer les impacts potentiels.

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

Limitée,

Car les mesures prévues, telles que le chiffrement, l'anonymisation, le cloisonnement et le contrôle des accès logiques, sont bien conçues pour contrer les menaces et les sources de risques identifiées.

Évaluation : Acceptable

Risques

Modification non désirées de données

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

Perte de confiance, Possibilité de surveillance non autorisée, Risque de vol d'identité

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

Accès non autorisé, Perte ou vol de données, Piratage, Utilisation abusive des données géolocalisées

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

Failles de sécurité dans le logiciel, Insuffisance des mesures de sécurité, Manque de formation du personnel

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

Chiffrement, Contrôle des accès logiques, Journalisation

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

Importante,

La gravité du risque est jugée "importante" en raison des impacts potentiels importants sur la confidentialité et la sécurité des données, malgré les mesures prévues pour atténuer ces risques.

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

Importante,

La vraisemblance du risque est jugée "Importante" en raison des nombreuses menaces et sources de risques identifiées, malgré les mesures prévues pour atténuer ces risques.

Évaluation : Acceptable

Risques

Disparition de données

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

Violation de la vie privée, Perte de confiance, Risque de discrimination

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

Perte ou vol de données, Piratage

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

Non-respect des réglementations en matière de protection des données, Insuffisance des mesures de sécurité, Manque de formation du personnel

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

Contrôle des accès logiques, Chiffrement, Anonymisation, Minimisation des données

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

Importante,

La gravité du risque est considérée comme importante en raison des impacts significatifs sur la vie privée des utilisateurs, malgré la mise en place de mesures de sécurité.

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

Importante,

La vraisemblance du risque est importante en raison de nombreuses menaces et sources de risques, malgré les mesures prévues.

Évaluation : Acceptable

Risques

Vue d'ensemble des risques