

# PIA Montre PrivateRun

Saisie :

Marine Duteil

Évaluation :

DPO de PrivateRun

Validation :

PDG de PrivateRun

Statut :

En cours

6%

## 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

DUTEIL Marine

#### Statut du DPD

Le traitement pourrait être mis en oeuvre.

## **Opinion du DPD**

Tout est bon

## **Recherche de l'avis des personnes concernées**

L'avis des personnes concernées a été demandé.

## **Noms des personnes concernées**

DUTEIL Marine

## **Statuts des personnes concernées**

Le traitement pourrait être mis en oeuvre.

## **Opinions des personnes concernées**

Tout est bon

# **Contexte**

## **Vue d'ensemble**

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

PrivateRun fait un traitement de données de géolocalisation issues d'activités de running ayant comme finalités d'un suivi personnalisé de l'activité sportive et de créer une communauté par cartographie anonyme.

Les enjeux sont le respect de la vie privée et la convivialité tout en obtenant des informations agrégées anonymes.

Le traitement repose sur un consentement explicite des utilisateurs tout en s'inscrivant dans une logique de service numérique personnalisé et communautaire.

### **Quelles sont les responsabilités liées au traitement ?**

Responsabilités liées au traitement des données :

- Utilisateurs : Ils doivent fournir un consentement éclairé et peuvent exercer leurs droits sur leurs données conformément à la législation en vigueur
- Responsable du traitement : Association Appliwebcourses surveille l'utilisation des données pour assurer la conformité aux politiques de confidentialité, de la protection des données et contribuer à leur élaboration.
- Sous-traitants : PrivateRun est chargée d'assurer la conformité avec les réglementations sur la protection des données et de collecter le consentement des utilisateurs.
- Sous-traitants: SuperCloudProvider fournit une infrastructure cloud pour le stockage et le

traitement des données à PrivateRun, garantissant la fiabilité, la disponibilité et la sécurité cloud.

## **Quels sont les référentiels applicables ?**

Les référentiels applicables sont le RGPD, les normes de sécurité informatique, les accords de confidentialité, les normes de protection et le code de conduite approuvés.

**Évaluation : Acceptable**

# **Contexte**

## **Données, processus et supports**

### **Quelles sont les données traitées ?**

Géolocalisation:

- Collectées: Coordonnées GPS, date, heure et vitesse
- Durée de conservation: 2 ans maximum après collecte
- Destinataires: Utilisateur, PrivateRun, AppliWebcourses

Données d'identification:

- Collectées: Nom, Prénom et date de naissance
- Durée de conservation: jusqu'à suppression du compte par l'utilisateur ou 2 ans après la dernière activité
- Destinataires: AppliWebCourses
- Accès restreint: PrivateRun

Données de compte:

- Collectées: adresse mail, identifiant et mot de passe
- Durée de conservation: jusqu'à suppression du compte par l'utilisateur ou 2 ans après la dernière activité
- Accès: uniquement aux administrateurs techniques de PrivateRun

Données agrégées et anonymisées:

- Collectées: trajectoires fusionnées, coordonnées GPS sans identifiant
- Durée de conservation: sans limite spécifique tant qu'elles sont anonymes
- Destinataires: Public, PrivateRun, AppliWebCourses

Données techniques:

- Collectées: logs de connexions, adresse IP, Informations sur l'appareil

- Durée de conservation: 12 mois
- Destinataire: PrivateRun

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

- Collecte: les données de course sont collectées depuis la montre connectée de l'utilisateur et via un formulaire de consentement pour les données personnelles
- Transmission: il y a une centralisation des données pour le traitement
- 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
- Suppression/ anonymisation: Les données GPS peuvent être conservées sous forme non identifiable. Les utilisateurs peuvent demander la suppression de leur données. Une suppression se fait après 2 ans d'inactivité

## **Quels sont les supports des données ?**

Du côté utilisateur:

- La montre connectée collecte et stock temporairement les données GPS
- Application mobile: transmission des données vers les serveurs

Supports distants:

- Serveur cloud: stock des données, traite et virtualise le site web
- Base de données: organisation des données utilisateur, authentification et parcours
- Serveur web: espace privé + page publique
- Système de sauvegarde: restauration possible en cas de défaillance

Personnes:

Les utilisateurs et les employés 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 ?**

Les deux finalités sont clairement définies en amont par le responsable du traitement et formellement énoncées dans le formulaire de consentement de chaque utilisateur. Les deux finalités répondent à un besoin concret des utilisateurs (suivi personnel de leur activité) et un objectif communautaire (visualisation globale sans atteinte à la vie privée).

**Évaluation : Acceptable**

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

Le traitement est licite, car il repose sur le consentement éclairé, libre et explicite des utilisateurs, recueilli conformément aux exigences du RGPD (article 6.1.a)

**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 sont collectées de manière minimisée : elles sont adéquates, pertinentes et limitées à ce qui est nécessaire pour atteindre les finalités prévues (F1 et F2). Le traitement respecte pleinement le principe de minimisation imposé par le RGPD.

- Le nom et prénom est utiles pour identifier personnellement le compte de l'utilisateur.
- Date de naissance permet de personnaliser les performances
- Adresse mail et mot de passe sont indispensables à la gestion sécurisée de l'accès personnel
- Coordonnées GPS, l'horodatage et la vitesse sont des données centrales pour tracer les parcours, calculer les performances et générer heatmaps
- Les données agrégées et anonymisées sont issues de traitement à des fins statistiques
- Logs de connexion et adresse IP sont utilisés uniquement pour la sécurité du service et la prévention des abus

**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 ?**

Les données collectées dans le cadre de l'utilisation du service PrivateRun sont conservées uniquement pendant la durée strictement nécessaire à la réalisation des finalités pour lesquelles elles ont été recueillies. La durée de conservation varie en fonction de la nature des données et des traitements associés, conformément au principe de limitation de la conservation prévu par l'article 5.1.e du RGPD.

- Données d'identification personnelles (nom, prénom, date de naissance, adresse e-mail) : conservées tant que le compte utilisateur est actif. En cas d'inactivité prolongée de plus de 2 ans, et sans réponse aux relances, le compte et les données associées sont supprimés.
- Données de connexion et de sécurité (identifiants, logs, adresses IP) : conservées pendant une durée maximale de 1 an à compter de la dernière connexion, à des fins de sécurité, de traçabilité et de gestion des accès.
- Données de géolocalisation associées à un utilisateur (positions, vitesses, horaires de parcours) : conservées pendant une durée de 2 ans après la dernière activité enregistrée, afin de permettre à l'utilisateur de consulter l'historique de ses performances. Ces données peuvent être supprimées à tout moment sur demande.
- Données géographiques anonymisées (traces GPS agrégées pour cartes de chaleur) : une fois anonymisées, ces données ne sont plus considérées comme des données personnelles. Elles peuvent être conservées sans limitation de durée à des fins statistiques, de visualisation publique ou d'analyse collective.
- Sauvegardes techniques : les sauvegardes automatiques du système, incluant les données personnelles, sont conservées pour une durée maximale de 30 jours avant suppression ou écrasement automatique, dans le cadre du plan de continuité d'activité.

**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**

## **Audits**

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

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

Possibilité de surveillance non autorisée, Risque de discrimination, 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 ?**

Utilisation abusive des données géolocalisées, 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 ?**

Faibles 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, Audits

**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 ?**

Piratage, Perte ou vol de données

### **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 ?**

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

### **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**

## Vue d'ensemble

### 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                 |
|  |  | Anonymisation               |
|  |  | Cloisonnement               |
|  |  | Contrôle des accès logiques |
|  |  | Audits                      |
|  |  | Archivage                   |
|  |  | Minimisation des données    |

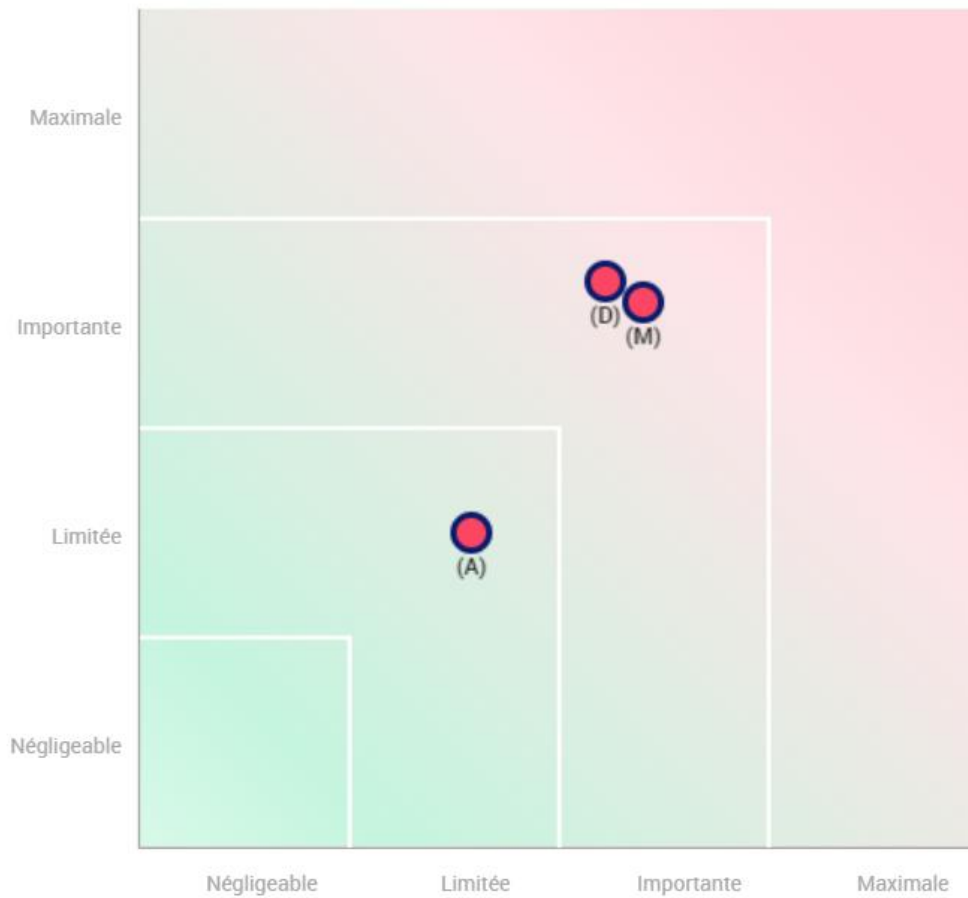
### Risques

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

Mesures Améliorables

Mesures Acceptables

## 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

## Impacts potentiels

Violation de la vie privée  
Perte de confiance  
Possibilité de surveillance...  
Risque de discrimination  
Risque de vol d'identité

## Menaces

Possibilité de surveillance...  
Risque de discrimination  
Piratage  
Perte ou vol de données  
Accès non autorisé  
Utilisation abusive des don  
Erreurs humaines

## Sources

Utilisation abusive des don  
Failles de sécurité dans le...  
Insuffisance des mesures de  
Manque de formation du pe  
Politiques de sécurité inad...  
Non-respect des réglementa

## Mesures

Chiffrement  
Anonymisation  
Cloisonnement  
Contrôle des accès logiques  
Audits  
Minimisation des données

### Accès illégitime à des données

Gravité : Limitée

Vraisemblance : Limitée

### Modification non désirées de d

Gravité : Importante

Vraisemblance : Importante

### Disparition de données

Gravité : Importante

Vraisemblance : Importante