# Analyse d'impact relative à la protection des données

*Privacy Impact Assessment (PIA)*

## ÉTUDE DE CAS « CAPTOO »

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

*Édition février 2018*

# Table des matières

# Avant-propos

**Ce document illustre un PIA** qui contient le minimum attendu en termes d'analyse, et qui a été mené par une société (fictive) sur un traitement (fictif) sans exploiter de bases de connaissances particulières.

La méthode de la CNIL est composée de trois guides, décrivant respectivement la démarche, des modèles utiles pour formaliser l'étude et des bases de connaissances (un catalogue de mesures destinées à respecter les exigences légales et à traiter les risques, et des exemples) utiles pour mener l'étude :

Ils sont téléchargeables sur le site de la CNIL :




https://www.cnil.fr/fr/PIA-privacy-impact-assessment

Conventions d'écriture pour l'ensemble de ces documents :

- le terme « **vie privée** » est employé comme raccourci pour évoquer l'ensemble des libertés et droits fondamentaux (notamment ceux évoqués dans le [RGPD], par les articles 7 et 8 de la [Charte-UE] et l'article 1 de la [Loi-I&L] : « vie privée, identité humaine, droits de l'homme et libertés individuelles ou publiques ») ;
- l'acronyme « **PIA** » est utilisé pour désigner indifféremment *Privacy Impact Assessment*, étude d'impact sur la vie privée (EIVP), analyse d'impact relative à la protection des données, et *Data Protection Impact Assessment* (DPIA) ;
- les libellés entre crochets ([libellé]) correspondent aux références bibliographiques.

**Attention : les modèles présentés dans ce guide constituent une aide à la mise en œuvre de la démarche. Il est tout à fait possible et même souhaitable de les adapter à chaque contexte particulier.**

# 1 Étude du contexte

## 1.1 Vue d'ensemble

### Présentation du (des) traitement(s) considéré(s)

| | |
|---|---|
| Description du traitement[1] | Captoo permet de mesurer différents éléments (données collectées pendant la nuit à l'aide de différents capteurs) pour connaître et comprendre l'environnement de l'utilisateur. |
| Finalités du traitement | Mesurer les paramètres du sommeil de l'utilisateur.<br>Amélioration de la qualité du sommeil de l'utilisateur. |
| Enjeux du traitement | Création d'un nouveau service, l'identification de causes de trouble du sommeil l'amélioration de la qualité de sommeil de l'utilisateur au cours du temps. |
| Responsable du traitement | DREAMLAND |
| Sous-traitant(s) | Hébergeur BETA situé aux États-Unis. |

### Recensement des référentiels applicables au traitement[2]

| Référentiels applicables au traitement | Prise en compte |
|---|---|
| Aucun référentiel spécifique | |
| | |
| | |

## 1.2 Données, processus et supports

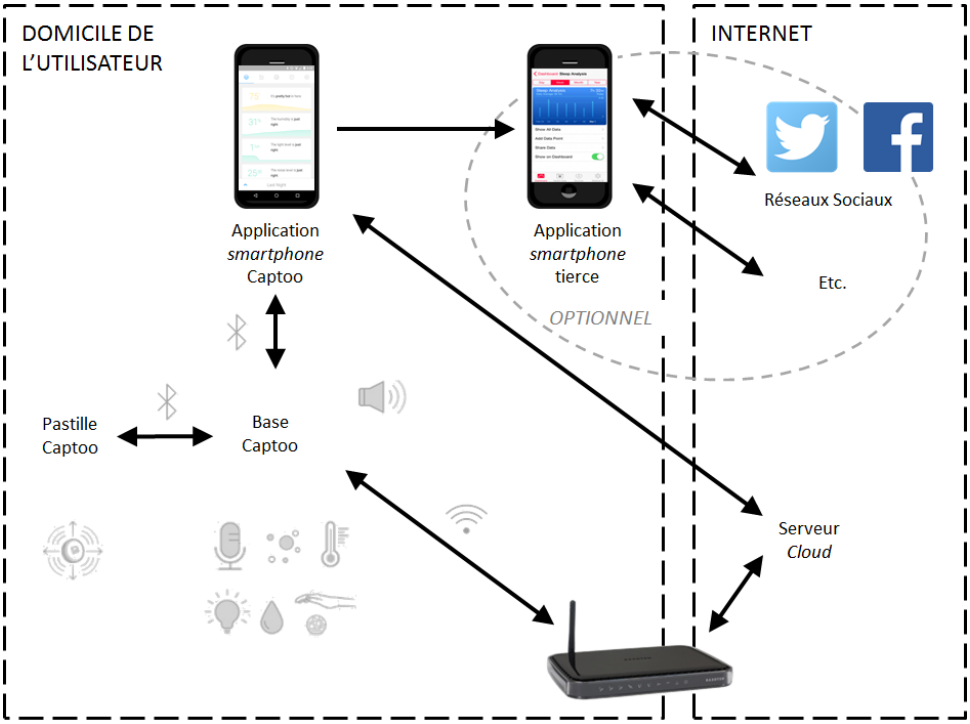
### Description des données[3], destinataires et durées de conservation

| Données | Destinataires | Durées de conservation |
|---|---|---|
| Fournies par l'utilisateur :<br>Adresse électronique, numéro de téléphone, date de naissance, genre, taille, poids | Dreamland, BETA, partenaires et affiliés | Jusqu'à la demande de suppression par l'utilisateur. |
| Provenant d'applications tierces (Twitter, Facebook) obtenues par lien avec le compte DREAMLAND | Dreamland, BETA, partenaires et affiliés | Jusqu'à la demande de suppression par l'utilisateur. |
| Données relevées :<br>Température, humidité, taux de particules, luminosité, | Réseaux sociaux, applications tierces, Dreamland, BETA, partenaires et affiliés | Jusqu'à la demande de suppression par l'utilisateur, les données audio sont conservées |

[1] Sa nature, sa portée, son contexte, *etc.*
[2] Voir article 35 (8) du [RGPD].
[3] Voir l'annexe **Erreur ! Source du renvoi introuvable.**.

| Données | Destinataires | Durées de conservation |
|---|---|---|
| son/bruit, heure de réveil, données d'accéléromètre | | 7 jours au plus dans le buffer de la base. |
| Données calculées :<br>Quantification de la qualité du sommeil, évaluation de la qualité de l'environnement de la chambre à coucher (niveau de bruit, température, humidité, air, etc.) | Réseaux sociaux, applications tierces, Dreamland, BETA, partenaires et affiliés | Jusqu'à la demande de suppression par l'utilisateur. |
| Données déduites :<br>vie sexuelle, données philosophiques, politiques, syndicales, relatives à la religion, relatives à la santé | Dreamland, BETA, partenaires et affiliés | Jusqu'à la demande de suppression par l'utilisateur. |

## Description des processus et supports[4]




| Processus | Description détaillée du processus | Supports des données concernés |
|---|---|---|
| Création du compte utilisateur | L'utilisateur crée un compte avec ses informations personnelles | Serveurs Cloud BETA, smartphone, applications tierces, Internet, WIFI, Bluetooth |
| Collecte des données liées au sommeil | Les capteurs Contenus dans la capsule Captoo (accrochée au matelas ou à l'oreiller) et la base (posée dans la chambre) relèvent les données | Pastille Captoo, Bluetooth<br>Base Captoo,<br>Internet, WIFI |

[4] Voir l'annexe **Erreur ! Source du renvoi introuvable.**.

| Processus | Description détaillée du processus | Supports des données concernés |
|---|---|---|
| | qui sont visualisées sur le smartphone de l'utilisateur via une application dédiée. | Smartphone |
| Envoi des données au serveur | Les données envoyées sur un serveur, qui les analyse et produit des données calculées, qui peuvent être consultées via la même application ; | Pastille Captoo, Bluetooth, Base Captoo, WIFI, Internet, Serveur BETA, Smartphone |
| Relai des informations vers des applications tierces | Les informations Captoo peuvent être relayées vers des applications tierces ou postées sur les réseaux sociaux (ex : publication de son score de sommeil). | Smartphone<br>Internet<br>Application réseaux Sociaux<br>Applications tierces |
| Amélioration de la qualité de service | Exploitation des données d'identification, relevées et calculées des utilisateurs DREAMLAND afin d'améliorer la qualité du service et d'effectuer des audits | Serveurs BETA |

# 2 Étude des principes fondamentaux

## 2.1 Évaluation des mesures garantissant la proportionnalité et la nécessité du traitement

### Explication et justification des finalités (art.5.1 (b)

| Finalités | Légitimité |
|---|---|
| Les données sont collectées pour **fournir le service demandé par l'utilisateur,** à savoir observer son sommeil, l'aider à identifier les causes de troubles et le réveiller au meilleur moment de son cycle. | La finalité de collecte aux fins de fourniture du service demandé par l'utilisateur est déterminée, explicite et légitime. |
| Des informations de connexion collectées par divers canaux (*cookies*, informations de fournisseurs internet, *etc.*) permettent aussi **d'effectuer des statistiques d'usage** sur le traitement Captoo. | Intérêt légitime. |
| Ces données sont susceptibles d'être conservées afin **d'alimenter des bases de données** possédées et maintenues par DREAMLAND, ses **affiliés et ses fournisseurs** de service. | Intérêt légitime. |
| | |

### Explication et justification du fondement (art.6)

| Critères de licéité | Applicable | Justification |
|---|---|---|
| La personne concernée a consenti[5] au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques. | | |
| Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci. | Oui | Le traitement est nécessaire à l'exécution du contrat auquel l'utilisateur est partie. |
| Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis. | | |
| Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique. | | |
| Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. | | |
| Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou | Non | Le fondement juridique correspondant à |

[5] Concernant le recueil du consentement de la personne et son information, voir le 2.2.

| Critères de licéité | Applicable | Justification |
|---|---|---|
| par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant[6]. | | l'exécution du contrat ne sera valable que pour la fourniture du service demandé par l'utilisateur et non pour le calculer des statistiques ou alimenter les bases de données des affiliés et fournisseurs de service de Dreamland.<br>Pour chacune des finalités, calcul de statistiques et alimentation des bases des affiliés et fournisseurs, correspondant chacune à la notion de « traitement », il conviendra de refaire un PIA et d'évaluer la possibilité de recourir à l'intérêt légitime en fonction des mesures de protection mises en place. |

[6] Ce point ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

## Explication et justification de la minimisation (adéquates, pertinentes, non excessives) des données (art.5 (c)

| Détail des données traitées | Catégories | Justification du besoin et de la pertinence des données | Mesures de minimisation |
|---|---|---|---|
| Température, humidité, taux de particules, luminosité, son/bruit, heure de réveil, données d'accéléromètre | Données relevées | Les données sont minimisées avant leur transmission au serveur *cloud* de BETA et seules ces données, nécessaires à la fourniture du service, sont conservées. | Les données de bruit provenant des captations audio ne sont pas enregistrées par défaut. Celles-ci sont collectées par tranches de 5 secondes et traitées dans la base Captoo pour détection de bruits caractéristiques tels que les ronflements. |
| Quantification de la qualité du sommeil, évaluation de la qualité de l'environnement de la chambre à coucher (niveau de bruit, température, humidité, air, etc.) | Données calculées à partir des relevés | Ce sont les données indicatrices de la qualité de sommeil du client livrables prévus par le contrat de service. | Seules les données prévues au contrat sont calculées. |
| Adresse électronique, numéro de téléphone, date de naissance, genre, taille, poids | Données courantes : données d'identification du compte | Données utilisées pour identifier le client et pour paramétrer les calculs de qualité de sommeil. | |

## Données exactes et tenus à jour (art.5.1 (d)

| Mesures pour la qualité des données | Justification |
|---|---|
| Les utilisateurs peuvent modifier leurs données directement identifiantes à tous moment (adresse email, taille, poids, date de naissance, *etc.*). | Par l'application ou en contactant Dreamland contact@captoo-dreamland.com. |
| | |
| | |

## Explication et justification des durées de conservation (art.5.1 (e)

| Types de données | Durée de conservation | Justification de la durée de conservation | Mécanisme de suppression à la fin de la conservation |
|---|---|---|---|
| Données courantes | Les données sont conservées tant que la personne concernée n'en demande pas la suppression. | | Sur demande (Dreamland contact@captoo-dreamland.com), les données sont rendues illisibles et les zones de stockage qui ont été utilisées sont effacées et écrasées. |
| Données archivées | | | |
| Traces fonctionnelles | | | |
| Journaux techniques (logs) | | | |

## Évaluation des mesures

| Mesures garantissant la proportionnalité et la nécessité du traitement | Acceptable / améliorable ? | Mesures correctives |
|---|---|---|
| Finalités : déterminées, explicites et légitimes | Améliorable<br>Cette finalité doit être distinguée de celle des transmissions de données aux affiliés ou de tout autre traitement à des fins de recherche ou d'éventuel profilage mis en œuvre par BETA et ses affiliés. Ces autres finalités sont rapidement évoquées, sans pour autant être explicite. | Afin d'éviter un usage incompatible ou un détournement de finalité, il conviendrait d'expliciter les autres finalités dans les documents portés à la connaissance des clients et de réitérer le PIA pour ces traitements. L'enjeu pour la vie privée des personnes diffère en fonction des finalités. |
| Fondement : licéité du traitement, interdiction du détournement de finalité | Améliorable<br>Ce fondement n'est valable que pour le traitement de données strictement nécessaire à la fourniture du service. Il ne sera pas valable pour la transmission de données à des tiers ou toute autre finalité de traitement accessoire, non nécessaire pour fournir le service. | Distinguer le service lui-même des autres finalités, au besoin faire un PIA pour chacune. |
| Minimisation des données : adéquates, pertinentes et limitées | Améliorable<br>La nécessité de la collecte de certaines données (informations personnelles comme la localisation, la date | Une distinction entre les données absolument nécessaires au fonctionnement du moniteur et de l'application |

| Mesures garantissant la proportionnalité et la nécessité du traitement | Acceptable / améliorable ? | Mesures correctives |
|---|---|---|
| | de naissance, l'âge, le poids, etc.) pour l'évaluation de la qualité du sommeil de l'utilisateur semble questionnable. Pour la localisation, il s'agirait de pouvoir intégrer les heures de lever et coucher du soleil ainsi que des informations d'ordre météorologique.<br>Il n'y a aucune garantie que les données agrégées pour partage avec des applications tierces soient effectivement anonymes (cf. remarques ci-dessus sur les finalités autres que le bon fonctionnement du service). | et celles non nécessaires doit être faite.<br><br>Suppression de la captation du son. Remplacement par le suivi du niveau sonore (en dB) au cours de la nuit. |
| Qualité des données : exactes et tenues à jour | Acceptable | |
| Durées de conservation : limitées | Améliorable<br>Aucune durée de conservation n'est fixée, les données peuvent donc être stockées indéfiniment dans les serveurs, à défaut de demande de suppression de l'utilisateur. | Une durée de conservation pour chaque catégorie de donnée doit être fixée en tenant compte de ce qui est strictement nécessaire au bon fonctionnement du service. Pour que la procédure d'effacement soit efficace, BETA doit distinguer entre les données présentes dans ses serveurs, celles présentes dans les serveurs de son sous-traitant et celles traitées en local dans le moniteur et le téléphone de l'utilisateur. |

## 2.2 Évaluation des mesures protectrices des droits des personnes des personnes concernées

### Détermination et description des mesures pour l'information des personnes (art.12)

Si le traitement bénéficie d'une exemption au droit d'information, prévue par l'article 32 de la [Loi-I&L] et les articles 12, 13 et 14 du [RGPD] :

| Dispense d'information des personnes concernées | Justification |
|---|---|
| | |

Dans le cas contraire :

| Mesures pour le droit à l'information | Modalités de mise en œuvre | Justification des modalités ou de l'impossibilité de leur mise en œuvre |
|---|---|---|
| Présentation des conditions d'utilisation/confidentialité. | Conditions Générales d'Utilisation. | L'information de l'utilisateur est faite dans les CGU. |
| Possibilité d'accéder aux conditions d'utilisation/confidentialité. | Dans le compte client. | Accès au compte client via l'application. |
| Conditions lisibles et compréhensibles. | Oui | |
| Existence de clauses spécifiques au dispositif. | Non | |
| Présentation détaillée des finalités des traitements de données (objectifs précis, croisements de données s'il y a lieu, etc.). | Notation de la qualité de sommeil de l'utilisateur en vue de l'améliorer. | Dans les CGU. |
| Présentation détaillée des données personnelles collectées. | Oui | Lors de la création du compte client via l'application. |
| Présentation des éventuels accès à des identifiants de l'appareil, en précisant si ces identifiants sont communiqués à des tiers. | Non | Pas de communication à des tiers. |
| Présentation des droits de la personne concernée (retrait du consentement, suppression de données, etc.). | Oui dans les CGU. | |
| Information sur le mode de stockage sécurisé des données, notamment en cas d'externalisation. | Le stockage est sécurisé. | La sécurité est gérée par BETA. |
| Modalités de contact de l'entreprise (identité et coordonnées) pour les questions de confidentialité. | Par mail, contact@captoo-dreamland.com | |
| Le cas échéant, information de la personne concernée de tout changement concernant | Dans les CGU. | Accessibles depuis le compte client via l'application. |

| Mesures pour le droit à l'information | Modalités de mise en œuvre | Justification des modalités ou de l'impossibilité de leur mise en œuvre |
|---|---|---|
| les données collectées, les finalités, les clauses de confidentialité. | | |
| Dans le cas de transmission de données à des tiers : | | |
| - présentation détaillée des finalités de transmission à des tiers ; | Non | |
| - présentation détaillée des données personnelles transmises ; | Non | |
| - indication de l'identité des entreprises tierces. | Non | La liste peut changer. |

## Détermination et description des mesures pour le recueil du consentement[7] (art.7)

| Mesures pour le recueil du consentement | Modalités de mise en œuvre | Justification des modalités ou de l'impossibilité de leur mise en œuvre |
|---|---|---|
| Consentement exprès à l'inscription. | Oui | La personne accepté les CGU lors de l'installation de l'application. |
| Consentement segmenté par catégorie de données ou types de traitement. | Non | Il n'y a qu'un traitement. |
| Consentement exprès avant le partage de données avec des tiers. | Oui | Le client décide de partager ou non ses données sur les réseaux sociaux. |
| Consentement présenté de manière compréhensible et adapté à la personne cible (notamment pour les enfants). | Non | Appareil destiné aux adultes. |
| Recueil du consentement des parents pour les mineurs de moins de 13 ans. | Non | Appareil destiné aux adultes. |
| Pour une nouvelle personne, mise en œuvre d'un nouveau recueil de consentement. | Non applicable | Si une nouvelle personne utilise l'appareil elle acceptera les CGU à l'installation de l'application. |
| Après une longue période sans utilisation, demande à la personne concernée de réaffirmer son consentement. | Non applicable | L'appareil est connecté en permanence et activé chaque nuit. |
| Si l'utilisateur a consenti au traitement de données particulières (par ex. sa localisation), l'interface signale clairement que ce traitement a lieu (icône, voyant lumineux). | Non | L'appareil s'active automatiquement. |

[7] Si la licéité du traitement repose sur le consentement.

| Mesures pour le recueil du consentement | Modalités de mise en œuvre | Justification des modalités ou de l'impossibilité de leur mise en œuvre |
|---|---|---|
| Si l'utilisateur change de contrat, les paramètres liés à son consentement sont maintenus. | Non Applicable | Il n'y a qu'un contrat. |

## Détermination et description des mesures pour les droits d'accès et à la portabilité (art.15 & art.20)

Si le traitement bénéficie d'une exemption au droit d'accès, prévue par les articles 39 et 41 de la loi [Loi-I&L] et les articles 15 et 20 du [RGPD] :

| Exemption du droit d'accès | Justification | Modalités de réponse aux personnes concernées |
|---|---|---|
| | | |

Dans le cas contraire :

| Mesures pour le droit d'accès | Données internes | Données externes | Justification |
|---|---|---|---|
| Possibilité d'accéder à l'ensemble des données personnelles de l'utilisateur, via les interfaces courantes. | Oui | Oui | Par l'application. |
| Possibilité de consulter, de manière sécurisée, les traces d'utilisation liées à la personne concernée. | Oui | Oui | Accès à l'historique par l'application. |
| Possibilité de télécharger une archive de l'ensemble des données à caractère personnel liées à la personne concernée. | Oui | Oui | Téléchargement d'une archive complète des données depuis l'application. |

Enfin, si le droit à la portabilité s'applique au traitement conformément à l'article 20 du [RGPD] :

| Mesures pour le droit à la portabilité | Données internes | Données externes | Justification |
|---|---|---|---|
| Possibilité de récupérer, sous une forme aisément réutilisable, les données personnelles qui ont été fournies par la personne concernée, afin de pouvoir les transférer à un service tiers. | Oui | Oui | Téléchargement d'une archive complète des données depuis l'application. |

## Détermination et description des mesures pour les droits de rectification et d'effacement (art.16 & art.17)

Si le traitement bénéficie d'une exemption au droit de rectification et d'effacement, prévue par l'article 41 de la [Loi-I&L] et l'article 17 du [RGPD] :

| Exemption des droits de rectification et d'effacement | Justification | Modalités de réponse aux personnes concernées |
|---|---|---|
| | | |

Dans le cas contraire :

| Mesures pour les droits de rectification et d'effacement | Données internes | Données externes | Justification |
|---|---|---|---|
| Possibilité de rectifier les données personnelles | Oui | Oui | Les données utilisateur peuvent être modifiées par l'utilisateur directement mais la modification des données collectées ne peut se faire qu'en écrivant à contact@captoo-dreamland.com. |
| Possibilité de supprimer les données personnelles | Oui | Oui | Les utilisateurs peuvent effacer leurs données (en particulier en quittant le service) en écrivant à contact@captoo-dreamland.com. |
| Indication des données personnelles qui seront conservées malgré tout (contraintes techniques, obligations légales, etc.) | Non | Non | Les données seront supprimées à la demande de l'utilisateur. |
| Mise en œuvre du droit à l'oubli pour les mineurs | Non | Non | Non applicable, produit destiné aux adultes |
| Indications claires et étapes simples pour effacer les données avant de mettre l'appareil au rebut | Oui | Oui | Les utilisateurs peuvent effacer leurs données (en particulier en quittant le service) en écrivant à contact@captoo-dreamland.com. |
| Conseils fournis pour remise à zéro en cas de vente de l'appareil | Non | Non | Il n'est pas prévu de pouvoir revendre l'appareil |

| | | | |
|---|---|---|---|
| Possibilité d'effacer les données en cas de vol de l'appareil | Oui | Oui | Les utilisateurs peuvent effacer leurs données (en particulier en quittant le service) en écrivant à contact@captoo-dreamland.com. |

## Détermination et description des mesures pour les droits de limitation du traitement et d'opposition (art.18 & art.21)

Si le traitement bénéficie d'une exemption au droit de limitation et d'opposition, prévue par l'article 38 de la [Loi-I&L] ou l'article 21 du [RGPD] :

| Exemption des droits de limitation et d'opposition | Justification | Modalités de réponse aux personnes concernées |
|---|---|---|
| | | |

Dans le cas contraire :

| Mesures pour les droits de limitation et d'opposition | Données internes | Données externes | Justification |
|---|---|---|---|
| Existence de paramètres « Vie privée » | Oui | Oui | Les coordonnées de la personne doivent être renseignées pour le suivi |
| Invitation à changer les paramètres par défaut | Non | Non | Il n'y a pas de valeur par défaut |
| Paramètres « Vie privée » accessibles pendant l'inscription | Oui | Oui | Tous les paramètres sont accessibles à l'inscription |
| Paramètres « Vie privée » accessibles après l'inscription | Oui | Oui | Les utilisateurs peuvent modifier leurs données (en particulier en quittant le service) en écrivant à contact@captoo-dreamland.com |
| Existence d'un dispositif de contrôle parental pour les enfants de moins de 13 ans | Non | Non | Le produit est destiné aux adultes |
| Conformité en matière de traçage (Cookies, Publicité, etc.) | Oui | Oui | Pas de cookies |
| Exclusion des enfants de moins de 13 ans des traitements de profilage automatisé | Oui | Oui | Le produit est destiné aux adultes |

| | | | |
|---|---|---|---|
| Exclusion effective de traitement des données de l'utilisateur en cas de retrait du consentement | Oui | Oui | Les utilisateurs peuvent effacer leurs données (en particulier en quittant le service) en écrivant à contact@captoo-dreamland.com |

## Détermination et description des mesures pour la sous-traitance (art. 28)

| Nom du sous-traitant | Finalité | Périmètre | Référence du contrat | Conformité art.28[8] |
|---|---|---|---|---|
| BETA | Hébergement Cloud Privé | Hébergement de toutes les données | DL-001 | |
| | | | | |
| | | | | |

## Détermination et description des mesures pour le transfert de données en dehors de l'Union européenne (chap.5)

| Données | France | UE | Pays reconnu adéquat par l'UE | Autre pays | Justification et encadrement (clauses contractuelles types, règles internes d'entreprise) |
|---|---|---|---|---|---|
| Toutes | | | | USA | BETA est situé aux Etats-Unis |
| | | | | | |
| | | | | | |

## Évaluation des mesures

| Mesures protectrices des droits des personnes concernées | Acceptable / améliorable ? | Mesures correctives |
|---|---|---|
| Information des personnes concernées (traitement loyal et transparent) | Améliorable<br>Placer l'information dans les CGU risque de la noyer parmi d'autres aspects. L'information n'est pas complète s'agissant des aspects | Afin d'assurer la transparence et la pleine connaissance des conséquences de l'usage de l'application, Dreamland pourrait informer ses utilisateurs sous forme de « pop up » lors de l'activation de l'application, de manière concise, en des termes simples |

[8] Un contrat de sous-traitance doit être conclu avec chacun des sous-traitants, précisant l'ensemble des éléments prévus à l'art. 28 du [RGPD] : durée, périmètre, finalité, des instructions de traitement documentées, l'autorisation préalable en cas de recours à un sous-traitant, mise à disposition de toute documentation apportant la preuve du respect du [RGPD], notification immédiate de toute violation de données, *etc.*

| Mesures protectrices des droits des personnes concernées | Acceptable / améliorable ? | Mesures correctives |
|---|---|---|
| | décrits dans les mesures correctives ci-dessous. | et clairs, et par l'utilisation d'icônes, de l'identité et des coordonnées du responsable de traitement, des finalités de chaque traitement et de tout traitement ultérieur, de leur base juridique respective, des destinataires des données (la mention de partenaires et affiliés est trop large), de la durée de conservation, de la manière d'exercer les droits d'accès, de rectification, d'opposition, d'effacement, le droit à la portabilité, le droit à la limitation du traitement, les coordonnées du délégué à la protection des données (s'il a été nommé).<br>Une information sur le transfert de données hors UE est requise. |
| Recueil du consentement | Améliorable<br>Le traitement est basé sur un contrat, mais il est nécessaire d'expliciter les sous finalités. | Afin d'éviter un usage incompatible ou un détournement de finalité, il conviendrait d'expliciter les autres finalités dans les documents portés à la connaissance des clients et de réitérer le PIA pour ces traitements. L'enjeu pour la vie privée des personnes diffère en fonction des finalités. |
| Exercice des droits d'accès et à la portabilité | Améliorable<br>Les données accessibles depuis l'application ne sont pas les seules données détenues par Dreamland.<br>Celles-ci peuvent comprendre les données de connexion (IP, horodatage des connexions au service et.) collectées dans le cadre du fonctionnement du service, un éventuel profil restitué de manière incomplète par l'appli, etc. | Identifier les données soumises à portabilité et définir le format « structuré couramment utilisé et lisible par une machine » permettant d'automatiser leur transmission.<br><br>S'assurer de la complétude des informations fournies depuis les différents supports de données, lors de la réponse à une demande d'exercice du droit d'accès. |

| Mesures protectrices des droits des personnes concernées | Acceptable / améliorable ? | Mesures correctives |
|---|---|---|
| | L'utilisateur doit être en mesure de les récupérer que ce soit, dans leur intégralité, par son droit d'accès, ou partiellement en demandant une portabilité (le service étant fourni sur la base d'un contrat) | |
| Exercice des droits de rectification et d'effacement | Améliorable.<br>Les utilisateurs peuvent rectifier leurs données (informations sur l'utilisateur, mais pas les données collectées à l'aide de capteurs) et demander la suppression des informations, mais sans savoir sur quelles données portent précisément ce droit.<br>De plus l'entourage de l'utilisateur susceptible d'être concerné par les données collectées ne peut s'opposer au système. | A chaque évolution du service et de ses sous-finalités, Dreamland devrait initier une procédure de révision de la pertinence des données collectées pour signaler, au moyen d'une icône, les données qui ne sont plus absolument nécessaires à l'exécution du service et dont la personne peut demander l'effacement, si Dreamland ne l'a pas déjà fait.<br>Un accusé de réception devrait être adressé pour confirmer la prise en compte des demandes. Un message de sensibilisation pourrait également être envoyé à l'utilisateur pour l'inviter à avertir son entourage de l'activation de l'application. |
| Exercice des droits de limitation du traitement et d'opposition | Améliorable.<br>Attention, dans le cas présent, la seule finalité étudiée est celle de la fourniture du service basé sur l'exécution du contrat ; les données collectées sur la base de ce fondement ne font pas l'objet du droit d'opposition prévu à l'article 21 du RGPD.<br><br>Le droit à la limitation du traitement permettra en revanche à la personne concernée de signaler un | Les suites à donner à l'identification d'un problème de licéité, d'exactitude des données, de pertinence, etc. doivent être documentées et permettre de répondre à chaque demande de limitation du traitement. |

| Mesures protectrices des droits des personnes concernées | Acceptable / améliorable ? | Mesures correctives |
|---|---|---|
| | problème au niveau du traitement de ses données et à Dreamland de suspendre leur traitement le temps de vérifier le bien-fondé de la demande (par exemple). | |
| Sous-traitance : identifiée et contractualisée | Améliorable.<br>BETA agissant en tant que sous-traitant, elle ne peut traiter les données que selon les instructions et pour le compte de Dreamland, dans un cadre établi par écrit. | Un contrat de sous-traitance doit être conclu entre les 2 sociétés précisant l'ensemble des éléments prévus à l'art. 28 (durée, périmètre, finalité, des instructions de traitement documentées, l'autorisation préalable en cas de recours à un sous-traitant, mise à disposition de toute documentation apportant la preuve du respect du règlement, notification immédiate de toute violation de données, etc.) |
| Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne | Améliorable.<br>Aucun encadrement du transfert des données collectées depuis les moniteurs vers les serveurs de l'hébergeur aux États-Unis ne semble être prévu. | Dreamland doit s'assurer d'encadrer le transfert par des « garanties appropriées » (cf. liste d'instrument art. 46). Il sera également nécessaire de signer un contrat avec ce sous-traitant aux US.<br><br>NB : avant l'entrée en application du RGPD le 25 mai 2018, Dreamland devra faire une déclaration normale sur le site de la CNIL en renseignant l'annexe transfert |

# 3 Étude des risques liés à la sécurité des données

## 3.1 Évaluation des mesures

### Description et évaluation des mesures contribuant à traiter des risques liés à la sécurité des données (art.32)

| Mesures portant spécifiquement sur les données du traitement | Modalités de mise en œuvre ou justification sinon | Acceptable / améliorable ? | Mesures correctives |
|---|---|---|---|
| Chiffrement | Toutes les connexions, entre la base Captoo, la pastille Captoo, le serveur cloud de BETA et le smartphone de l'utilisateur, se font en SSL via le protocole https. | Améliorable.<br>Il est recommandé d'utiliser la version de TLS la plus à jour possible et non SSL. | TLS devrait être employé pour l'utilisation du protocole https. |
| Anonymisation | Non applicable | | |
| Cloisonnement des données (par rapport au reste du système d'information) | La solution cloud de BETA choisie par Dreamland offre un cloisonnement vis-à-vis des données des autres clients du service. | Améliorable.<br>Il n'est pas indiqué si les données des utilisateurs sont isolées entre elles dans les serveurs utilisés par Captoo. Par ailleurs, il n'est pas précisé si les instances sur lesquels les serveurs s'exécutent sont dédiés (ce qui est vraisemblable) ou si ces instances sont susceptibles d'être réutilisées par des tiers. | Il conviendrait de préciser la manière dont les données sont cloisonnées. |
| Contrôle des accès logiques | Par identifiant et mot de passe. Il est de la responsabilité de l'utilisateur de maintenir la confidentialité de ses informations de connexion. | Améliorable.<br>Il incombe toutefois à Dreamland de garantir la bonne gestion de ces informations. | Il conviendrait de préciser la politique de gestion des mots de passe. |
| Traçabilité (journalisation) | Tous les accès aux données à caractère personnel font l'objet d'une journalisation et | Améliorable.<br>Manque de précision. | Il conviendrait de préciser les informations journalisées, leurs durées de |

| Mesures portant spécifiquement sur les données du traitement | Modalités de mise en œuvre ou justification sinon | Acceptable / améliorable ? | Mesures correctives |
|---|---|---|---|
| | les journaux sont audités | | conservation, l'architecture de journalisation, la fréquence et la procédure d'audit des journaux, et si des procédures de détection des accès frauduleux et/ou suspects sont mises en œuvre. |
| Contrôle d'intégrité | Toutes les connexions, entre la base Captoo, la pastille Captoo, le serveur cloud de BETA et le smartphone de l'utilisateur, se font en SSL via le protocole https. | Améliorable<br>Les données pourraient être altérées après leur transfert. | Chaque modification pourrait être horodatée et la date de dernière modification conservée dans l'application pour être vérifiée à la reconnexion. En cas de différence l'utilisateur recevrait une alerte. |
| Archivage | Les données sont conservées tant que la personne concernée n'en demande pas la suppression. Sur demande, les données sont rendues illisibles et les zones de stockage qui ont été utilisées sont effacées et écrasées. Les données audio enregistrées (des tranches de signal de 5s) devraient à terme être conservées dans le buffer de la base Captoo, pour au plus 7 jours, afin que l'utilisateur puisse les rejouer. | Améliorable.<br>Aucune durée de conservation n'est fixée, les données peuvent donc être stockées indéfiniment dans les serveurs, à défaut de demande de suppression de l'utilisateur. | Une durée de conservation pour chaque catégorie de donnée doit être fixée en tenant compte de ce qui est strictement nécessaire au bon fonctionnement du service. Pour que la procédure d'effacement soit efficace, Dreamland doit distinguer entre les données présentes dans ses serveurs, celles présentes dans les serveurs de son sous-traitant et celles traitées en local dans le |

| Mesures portant spécifiquement sur les données du traitement | Modalités de mise en œuvre ou justification sinon | Acceptable / améliorable ? | Mesures correctives |
|---|---|---|---|
| | | | moniteur et le téléphone de l'utilisateur. |
| Sécurité des documents papier | Non applicable | | |

## Description et évaluation des mesures générales de sécurité

| Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre | Modalités de mise en œuvre ou justification sinon | Acceptable / améliorable ? | Mesures correctives |
|---|---|---|---|
| Sécurité de l'exploitation | La maintenance des serveurs est couverte par le contrat avec BETA. La maintenance des logiciels et des terminaux est réalisée par Dreamland. | Acceptable | |
| Lutte contre les logiciels malveillants | La sécurité des serveurs est couverte par le contrat avec BETA. | Acceptable | |
| Gestion des postes de travail | La sécurité des postes de travail est garantie par la politique de sécurité de Dreamland. | Acceptable | |
| Sécurité des sites web | Les mesures de sécurité mises en œuvre lors de l'utilisation d'un serveur cloud de BETA sont décrites dans sa politique de sécurité. | Acceptable | |
| Sauvegardes | Effectuée dans le serveur de BETA. | Améliorable<br>Manque de précision. | Préciser la politique de sauvegarde de BETA. |
| Maintenance | La maintenance des serveurs est couverte par le contrat avec BETA. La maintenance des logiciels et des terminaux est réalisée par Dreamland. La base Captoo et la pastille Captoo font l'objet d'une garantie d'un an. | Acceptable | |
| Sécurité des canaux informatiques (réseaux) | Les réseaux suivants sont mis en œuvre :<br>- réseau privé du client ;<br>- Internet ;<br>- réseau privé BETA. | Améliorable.<br>Le réseau privé du client est à sa charge, toutefois un rappel des bonnes pratiques de sécurité pourrait être fait. | Rappeler les bonnes pratiques concernant les réseaux domestiques dans la documentation produit. |

| Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre | Modalités de mise en œuvre ou justification sinon | Acceptable / améliorable ? | Mesures correctives |
|---|---|---|---|
| Surveillance | Les mesures de sécurité mises en œuvre lors de l'utilisation d'un serveur *cloud* de BETA sont décrites dans sa politique de sécurité. | Acceptable | |
| Contrôle d'accès physique | Les mesures de contrôle d'accès mises en œuvre par BETA pour l'accès à leurs infrastructures sont décrites dans sa politique de sécurité. | Acceptable | |
| Sécurité des matériels | Les mesures de sécurité physique mises en œuvre lors de l'utilisation d'un serveur *cloud* de BETA sont décrites dans sa politique de sécurité. | Acceptable | |
| Éloignement des sources de risques | La politique de sécurité de BETA mentionne l'attention portée aux risques naturels dans le choix de l'implantation de leurs datacenters. | Acceptable | |
| Protection contre les sources de risques non humaines | Les mesures de sécurité physique mises en œuvre lors de l'utilisation d'un serveur *cloud* de BETA sont décrites dans sa politique de sécurité (détection d'incendies, alimentation électrique, surveillance de la température, maintenance préventive, déstockage matériel, *etc.*). | Acceptable | |

## Description et évaluation des mesures organisationnelles (gouvernance)

| Mesures organisationnelles (gouvernance) | Modalités de mise en œuvre ou justification sinon | Acceptable / améliorable ? | Mesures correctives |
|---|---|---|---|
| Organisation | L'accès des employés de Dreamland aux données à caractère personnel nécessite une autorisation. | Améliorable. Manque de précision. | Il conviendrait de préciser la manière dont les habilitations sont gérées. |
| Politique (gestion des règles) | BETA dispose d'une charte informatique. | Améliorable | Dreamland devrait en rédiger une également. |
| Gestion des risques | Aucune mesure prévue [*Indiquez ici si les risques que les traitements font peser sur la vie privée des personnes concernées sont étudiés pour les nouveaux traitements, si c'est systématique ou non, et le cas échéant, selon quelle méthode.* *Précisez s'il existe, au niveau de l'organisme, une cartographie des risques sur la vie privée.*] | Améliorable | Une procédure de gestion de projet intégrant l'étude systématique des risques que font peser le traitement sur la vie privée des personnes concernées devrait être rédigée. |
| Gestion des projets | Les tests sont effectués sur des données anonymes. | Acceptable | |
| Gestion des incidents et des violations de données | Il n'existe pas de procédure *en ce qui concerne la gestion ds violations de données à caractère personnel.* | Améliorable | Mettre en place une procédure de gestion des violations des données personnelles |
| Gestion des personnels | Aucune mesure prévue [*Indiquez ici les mesures de sensibilisation prises à l'arrivée d'une personne dans sa fonction.* *Indiquez les mesures prises au départ des personnes accédant aux données.*] | Améliorable | Prévoir des sessions de sensibilisation du personnel. Préciser les mesures prises en cas de départ d'un salarié dans la procédure de gestion du personnel. |
| Relations avec les tiers | Les modalités d'accès aux données sont précisées dans le contrat de sous-traitance avec BETA | Acceptable | |

| Mesures organisationnelles (gouvernance) | Modalités de mise en œuvre ou justification sinon | Acceptable / améliorable ? | Mesures correctives |
|---|---|---|---|
| Supervision | Des audits sont réalisés. | Améliorable.<br>Manque de précision. | Il conviendrait de préciser les conditions de réalisation des audits internes. |

## 3.2 Appréciation des risques : les atteintes potentielles à la vie privée

### Analyse et estimation des risques

| Risque | Principales sources de risques | Principales menaces | Principaux impacts potentiels | Principales mesures réduisant la gravité et la vraisemblance | Gravité | Vraisemblance |
|---|---|---|---|---|---|---|
| Accès illégitime à des données | Employé<br>Attaquant<br>Entourage | Consultation/vol des données sur le serveur<br>Usurpation d'un compte (via un smartphone) | Conséquences d'une communication d'informations potentiellement sensibles (discrimination, menaces, agressions, perte d'emploi, perte d'accès à des services, etc.)<br>Phishing<br>Publicité ciblée | Minimisation<br>Durées de conservation<br>Contrôle d'accès logique des utilisateurs<br>Chiffrement de flux (SSL)<br>Sécurité de l'exploitation (authentification des équipements)<br>Surveillance (cloud privé)<br>Organisation (habilitation des employés)<br>Traçabilité (journalisation des accès)<br>Supervision (audits)<br>Notification de la violation aux personnes concernées et prescription de mesures préventives adaptées | Importante | Maximale |
| Modification non désirée de données | Employé<br>Entourage<br>Attaquant | Altération des données sur le serveur | Détérioration de la qualité du service | Sauvegarde du serveur cloud<br>Chiffrement de flux (SSL)<br>Sécurité de l'exploitation (authentification des équipements) | Limitée | Limitée |

| Risque | Principales sources de risques | Principales menaces | Principaux impacts potentiels | Principales mesures réduisant la gravité et la vraisemblance | Gravité | Vraisemblance |
|---|---|---|---|---|---|---|
| | | | | Surveillance (cloud privé)<br>Contrôle d'accès logique des utilisateurs<br>Organisation (habilitation des employés)<br>Traçabilité (journalisation des accès)<br>Supervision (audits)<br>Notification de la violation aux personnes concernées et prescription de mesures préventives adaptées | | |
| Disparition de données | Utilisateur<br>Entourage<br>Employé<br>Attaquant<br>Sinistre | Suppression de données (via l'application ou le serveur)<br>Détérioration de serveurs<br>Dégradation physique d'un matériel (par exemple lavage machine de la pastille Captoo avec taie d'oreiller, casse de la base Captoo, etc.) | Nécessité de recréer un compte d'utilisation<br>Perte de l'historique et de la personnalisation du service<br>Détérioration de la qualité du service | Surveillance (cloud privé)<br>Sécurité des matériels (protection physique des serveurs cloud)<br>Maintenance (garantie pour la base et la pastille Captoo)<br>Sauvegarde du serveur cloud<br>Archivage (conservation locale et temporaire des données)<br>Contrôle d'accès logique des utilisateurs<br>Organisation (habilitation des employés) | Limitée | Limitée |

| Risque | Principales sources de risques | Principales menaces | Principaux impacts potentiels | Principales mesures réduisant la gravité et la vraisemblance | Gravité | Vraisemblance |
|---|---|---|---|---|---|---|
| | | | | Gestion des postes de travail (authentification forte des employés)<br>Traçabilité (journalisation des accès) | | |

## Évaluation des risques

| Risques | Acceptable / améliorable ? | Mesures correctives | Gravité résiduelle | Vraisemblance résiduelle |
|---|---|---|---|---|
| Accès illégitime à des données | Améliorable.<br>Des données pourraient encore être volées par un employé de Dreamland, ou consultées par l'entourage usurpant le compte via le *smartphone* dans le but de caractériser une situation relevant de la vie privée des personnes (par exemple un adultère). | - Préciser, et le cas échéant adapter, la manière dont les enregistrements audio sont réalisés, sauvegardés et restitués aux utilisateurs ;<br>- mettre en œuvre des mesures de chiffrement des données stockées en base ;<br>- préciser à l'utilisateur les bonnes pratiques à suivre lors de la mise au rebut des matériels ;<br>- mettre en place une charte d'utilisation des moyens informatiques et un engagement de confidentialité pour | Importante | Négligeable |

| Risques | Acceptable / améliorable ? | Mesures correctives | Gravité résiduelle | Vraisemblance résiduelle |
|---|---|---|---|---|
| | | les employés de Dreamland. | | |
| Modification non désirée de données | Acceptable.<br>Un utilisateur peut voir ses données de sommeil faussées suite à l'hébergement d'une personne dans sa chambre à coucher et observer une détérioration de la qualité du service.<br>Le risque semble acceptable au regard de la gravité (limitée) et de la vraisemblance (limitée) résiduelles, compte tenu des mesures existantes ou prévues. | Non applicable. | Limitée | Négligeable |
| Disparition de données | Acceptable.<br>Un utilisateur voit les données relatives à son sommeil supprimées par maladresse par un employé de Dreamland et perd ainsi tout l'historique d'utilisation et de personnalisation du service.<br>Le risque semble acceptable au regard de la gravité (limitée) et de la vraisemblance (limitée) résiduelles, compte tenu des mesures existantes ou prévues. | Non applicable | Limitée | Négligeable |

# 4 Validation du PIA

## 4.1 Préparation des éléments utiles à la validation

### Élaboration de la synthèse relative à la conformité au [RGPD] des mesures permettant de respecter les principes fondamentaux

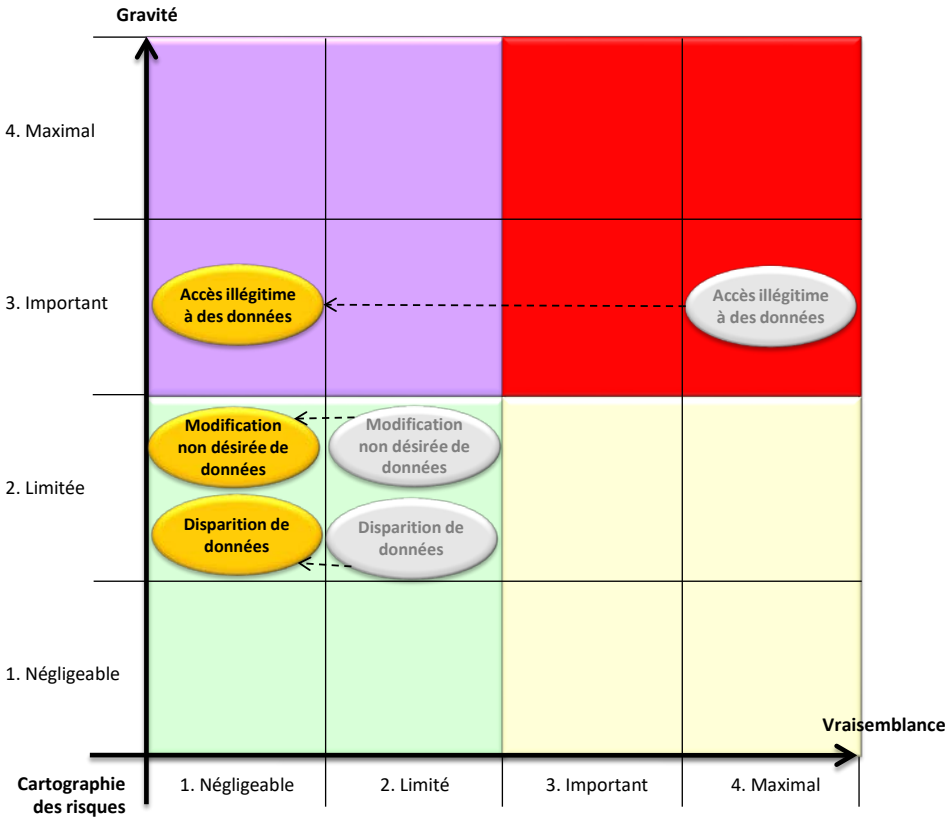
| Légende | | | | |
|---|---|---|---|---|
| Symbole : | ●●● | ●○○ | ○●○ | ○○● |
| Signification : | Non applicable | Insatisfaisant | Amélioration prévue | Satisfaisant |

| Mesures permettant de respecter les principes fondamentaux | Évaluation |
|---|---|
| Mesures garantissant la proportionnalité et la nécessité du traitement | |
| Finalités : déterminées, explicites et légitimes | ○●○ |
| Fondement : licéité du traitement, interdiction du détournement de finalité | ○●○ |
| Minimisation des données : adéquates, pertinentes et limitées | ○●○ |
| Qualité des données : exactes et tenues à jour | ○●○ |
| Durées de conservation : limitées | ○●○ |
| Mesures protectrices des droits des personnes des personnes concernées | |
| Information des personnes concernées (traitement loyal et transparent) | ○●○ |
| Recueil du consentement | ○●○ |
| Exercice des droits d'accès et à la portabilité | ○●○ |
| Exercice des droits de rectification et d'effacement | ○●○ |
| Exercice des droits de limitation du traitement et d'opposition | ○●○ |
| Sous-traitance : identifiée et contractualisée | ○●○ |
| Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne | ○●○ |

## Élaboration de la synthèse relative à la conformité aux bonnes pratiques des mesures des mesures contribuant à traiter les risques liés à la sécurité des données

| Mesures contribuant à traiter les risques liés à la sécurité des données | Évaluation |
|---|---|
| Mesures portant spécifiquement sur les données du traitement | |
| Chiffrement | ○●○ |
| Anonymisation | ●●● |
| Cloisonnement des données (par rapport au reste du système d'information) | ○●○ |
| Contrôle des accès logiques des utilisateurs | ○●○ |
| Traçabilité (journalisation) | ○●○ |
| Contrôle d'intégrité | ○●○ |
| Archivage | ○●○ |
| Sécurité des documents papier | ●●● |
| Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre | |
| Sécurité de l'exploitation | ○○● |
| Lutte contre les logiciels malveillants | ○○● |
| Gestion des postes de travail | ○○● |
| Sécurité des sites web | ○○● |
| Sauvegardes | ○●○ |
| Maintenance | ○○● |
| Sécurité des canaux informatiques (réseaux) | ○●○ |
| Surveillance | ○○● |
| Contrôle d'accès physique | ○○● |
| Sécurité des matériels | ○○● |
| Éloignement des sources de risques | ○○● |
| Protection contre les sources de risques non humaines | ○○● |
| Mesures organisationnelles (gouvernance) | |
| Organisation | ○●○ |
| Politique (gestion des règles) | ○●○ |
| Gestion des risques | ○●○ |
| Gestion des projets | ○○● |
| Gestion des incidents et des violations de données | ○●○ |
| Gestion des personnels | ○●○ |
| Relations avec les tiers | ○○● |
| Supervision | ○●○ |

## Élaboration de la cartographie des risques liés à la sécurité des données


Gravité
4. Maximal
3. Important
2. Limitée
1. Négligeable
Accès illégitime à des données
Accès illégitime à des données
Modification non désirée de données
Modification non désirée de données
Disparition de données
Disparition de données
Vraisemblance
Cartographie des risques
1. Négligeable
2. Limité
3. Important
4. Maximal

## Élaboration du plan d'action[9]

| Mesures complémentaires demandées | Responsable | Terme | Difficulté | Coût | Avancement |
|---|---|---|---|---|---|
| Distinguer la finalité de fourniture du service des autres finatlités | Marketing Dreamland | Trimestre | Moyenne | Nul | En cours |
| Minimiser les données :<br>- Distingure les données indispensables au traitement des autres<br>- Suppression de la captation du son. Remplacement par le suivi du niveau sonore (en dB) au cours de la nuit | R&D Dreamland | Trimestre | Moyenne | Moyen | En cours |
| Définir des durées de conservation | DPD, Marketing et R&D Dreamland, hébergeur BETA | Trimestre | Elevée | Moyen | En cours |
| Mettre en place une pop-up d'information | DPD et R&D Dreamland | Mois | Faible | Moyen | Non démarré |
| Exercice des droits d'accès et à la portabilité :<br>- Identifier les données soumises à la portabilité<br>- Définir le format « structuré couramment utilisé et lisible par une machine »<br>- S'assurer de la complétude des données fournies en réponse à une demande d'exercice du droit d'accès | DPD et R&D Dreamland | Mois | Moyenne | Moyen | Non Démarré |
| Exercice des droits de rectification et d'effacement :<br>- Rédiger une procédure de révision de lapertinence des données collectées | DPD et R&D Dreamland | Trimestre | Faible | Moyen | Non Démarré |

[9] Voir l'annexe **Erreur ! Source du renvoi introuvable.**.

| Mesures complémentaires demandées | Responsable | Terme | Difficulté | Coût | Avancement |
|---|---|---|---|---|---|
| - Mise en place d'icônes indiquant les données qui ne sont plus nécessaires<br>- Mise en place d'une procédure d'accusé de réception des demandes | | | | | |
| Procédure de limitation du traitement | DPD et R&D Dreamland | Trimestre | Elevée | Moyen | Non démarré |
| Encadrer la sous-traitance (vérifier la conformité avec l'article 28 du RGPD) | DPD et service juridique Dreamland | Mois | Moyen | Nul | Non démarré |
| Encadrer les transferts hors UE par des « garanties appropriées » conformément à l'article 46 du RGPD | DPD et service juridique Dreamland | Mois | Moyen | Nul | Non Démarré |
| Passage en TLS 1.2 | DSI Dreamland | Mois | Moyenne | Nul | Terminé |
| Revoir la documentation produit :<br>- Cloisonnement des données<br>- Gestion des mots de passe<br>- Traçabilité<br>- Bonnes pratiques de configuration d'un réseau WIFI | DSI Dreamland | Trimestre | Moyenne | Nul | En cours |
| Contrôle d'intégrité : horodatage des modifications | R&D Dreamland | Mois | Moyenne | Moyen | En cours |
| Fournir la politique de sauvegarde de BETA | DSI Dreamland | Mois | Faible | Nul | En cours |
| Formaliser la politique de gestion des habilitations | RSSI Dreamland | Mois | Faible | Nul | Terminé |
| Rédiger une charte informatique | DPD Dreamland | Mois | Faible | Nul | Terminé |
| Rédiger la procédure de gestion de projet incluant l'étude systématique des risques sur la vie privée | DPD Dreamland | Mois | Faible | Nul | En cours |

| Mesures complémentaires demandées | Responsable | Terme | Difficulté | Coût | Avancement |
|---|---|---|---|---|---|
| Rédiger une procédure de gestion des incidents et violations de données | DPD et RSSI Dreamland | Trimestre | Faible | Nul | En cours |
| Sessions de sensibilisation des personnels | DPD et RH Dreamland | Année | Moyen | Moyen | En cours |
| Formaliser les procédures d'audits | RSSI Dreamland | Mois | Faible | Nul | En cours |

## Formalisation du conseil de la personne en charge des aspects « Informatique et libertés »[10]

Le 25/03/2017, le délégué à la protection des données de Dreamland a rendu l'avis suivant concernant la conformité du traitement et le PIA mené :

L'analyse menée montre qu'avec la mise en place des plans d'actions préconisés, la protection de la vie privée des personnes est garantie de manière acceptable.

[Signature]

## Formalisation de l'avis des personnes concernées ou de leurs représentants[11]

Les personnes concernées ont été consultées et ont émis l'avis suivant sur la conformité du traitement au vu du PIA mené :

Le panel de clients interrogé lors de l'étude de marché est majoritairement intéressé par le produit et accepte ses modalités d'utilisation.

[10] Voir l'article 35 (2) du [RGPD].
[11] Voir l'article 35 (9) du [RGPD].

## 4.2 Validation formelle

### Formalisation de la validation

Le 31/03/2017, le directeur général de Dreamland valide le PIA du traitement Captoo, au vu du PIA mené, en sa qualité de responsable du traitement.

Le traitement a pour finalité d'améliorer la qualité de sommeil de l'utilisateur grâce à une connaissance et compréhension de son environnement. L'enjeu de ce traitement est d'identifier les causes de trouble du sommeil à l'aide de différents capteurs, afin d'améliorer la qualité de sommeil de l'utilisateur au cours du temps.

Les mesures prévues pour respecter les principes fondamentaux de la protection de la vie privée et pour traiter les risques sur la vie privée des personnes concernées sont en effet jugées acceptables au regard de cet enjeu. La mise en œuvre des mesures complémentaires devra toutefois être démontrée, ainsi que l'amélioration continue du PIA.

[Signature]