Aperçu de l'analyse

INFORMATIONS GÉNÉRALES

éditer

100%

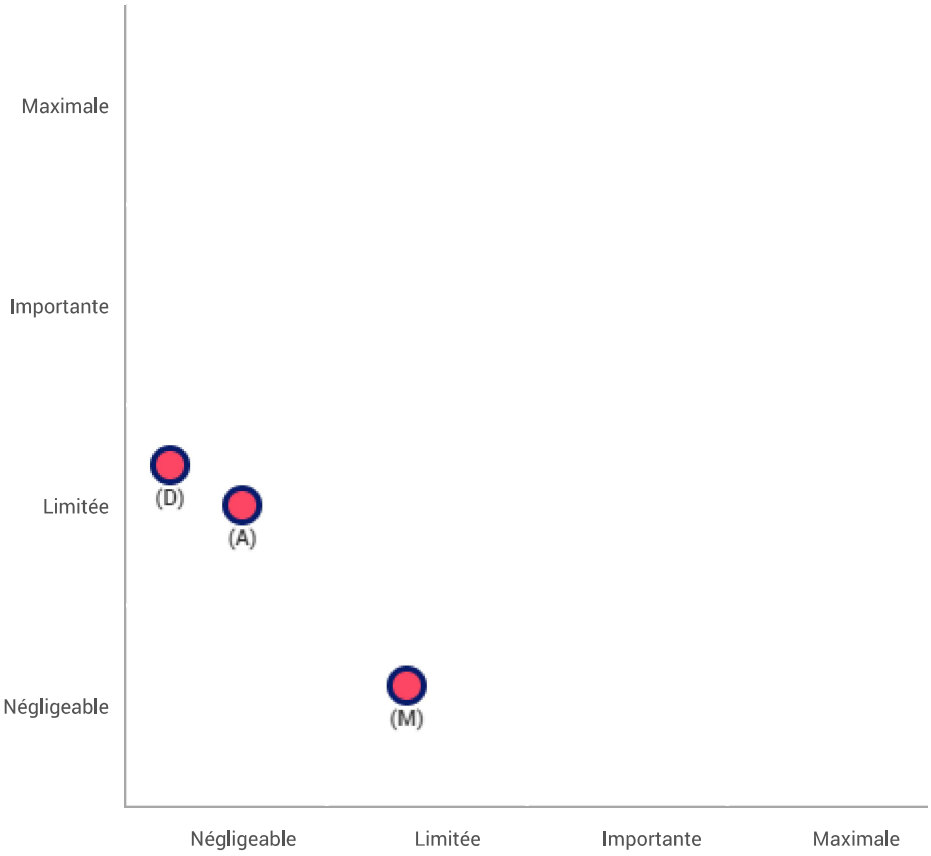
Aperçu

Saisie :	MARCHAND Nicolas	**Statut :**	Validation
Évaluation :	MARCHAND Nicolas		simple
Validation :	MARCHAND Nicolas		

Validation

Cartographie des risques

Gravité du risque



Vraisemblance du risque

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

21/09/2021

Validation

Plan d'action

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
Contrôle des accès logiques
Journalisation
Archivage
Sécurisation de l'exploitation
Sauvegarde des données
Maintenance
Sécurisation des canaux informatiques
Sécurité physique
Gestion des personnels

Risques

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

Mesures améliorables

Mesures acceptables

Principes fondamentaux

Aucun plan d'action enregistré.

Mesures existantes ou prévues

Aucun plan d'action enregistré.

Risques

Aucun plan d'action enregistré.

Validation

Avis du DPD et des personnes concernées

Nom du DPD

MARCHAND

Statut du DPD

Le traitement pourrait être mis en oeuvre.

Opinion du DPD

OK

Recherche de l'avis des personnes concernées

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

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

Multitude de client concernés

Contexte
Vue d'ensemble

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

Permettre aux utilisateurs de LoGeAs Web d'accéder à leurs données
Suivre l'activité liée au logiciel

Quelles sont les responsabilités liées au traitement ?

Le responsable de traitement est Logeas Informatique, qui agit pour le compte des structures clientes du logiciel LoGeAs WEB.

La societé Prosoluce est sous-traitant dans le cadre de l'hébergement de notre serveur dans l'une de ses baies en data-center. Remarque : Prosoluce n'a pas accés à la machine vituelle qui héberge les données

Quels sont les référentiels applicables ?

- Charte informatique Logeas Informatique
- NF 203 et NF 552
- Contrat cadre EPUdF-Logeas
- Conditions générales de vente

Évaluation : Acceptable

Contexte
Données, processus et supports

Quelles sont les données traitées ?

Etat-civil : Nom et prénom, adresse, téléphone, email, profession, fonction dans l'entité
Données de connexion : Informations d'horodatage et action (piste d'audit)

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

1. Création de la fiche de la personne, par l'assistance logeas (cas de la mise en place d'un nouvel administrateur) ou par le/les administrateurs de la base.
2. Envoi d'une invitation pour activer et mettre à jour le profil créé ainsi que pour créer son mot de passe
3. Vie du compte : mise à jour par l'utilisateur et/ou l'administrateur (pas d'intervention sur les données par Logeas)
4. Cloture et archivage du compte suite à la fin de contrat et/ou retrait des droits et/ou demande

de l'utilisateur.

Quels sont les supports des données ?

Les données sont stockées dans une base de données cryptée sur un serveur virtuel porté par un serveur physique situé dans un data-center Toulousain dans une baie Prosoluce.

Évaluation : Acceptable

Principes fondamentaux

Proportionnalité et nécessité

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

- donner accés à la base du client à ses utilisateurs/administrateur
- réaliser l'assistance sur le logiciel
- informer les utilisateurs des évolutions, problématiques liées au logiciel
- comuniquer afin de sensibiliser/former les utilisateurs

Évaluation : Acceptable

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

Excéution d'un contrat et des obligations liées

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) ?

Etat civil : Necessaire pour communiquer avec l'utilisateur
Données de connexion : obligations liées aux marques NF

Évaluation : Acceptable

Les données sont-elles exactes et tenues à jour ?

Les données étant sous le contrôle de l'utilisateur (propriétaire) elles sont réputées l'être ...

Évaluation : Acceptable

Quelle est la durée de conservation des données ?

Durée d'éxécution du contrat (fin d'hébergement des données de la structure et/ou retrait par l'administrateur du profil), puis archivage

Évaluation : Acceptable

Principes fondamentaux

Principes fondamentaux

Mesures protectrices des droits

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

Conditions générales de vente et contrat

Évaluation : Acceptable

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

sans objet

Évaluation : Acceptable

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

Contact par mail ou courrier à l'assistance et/ou recours auprés de l'administrateur de la base.

Évaluation : Acceptable

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

Modification direct de leur profil
Droit à l'effacement par mail ou courrier à l'assistance et/ou recours auprés de l'administrateur de la base.

Évaluation : Acceptable

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

Pas de droit de limitation mis en place

Évaluation : Acceptable

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

Oui via le contrat de sous traitance avec prosoluce

Évaluation : Acceptable

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

Pas de transfert hors UE

Évaluation : Acceptable

Risques

Mesures existantes ou prévues

Chiffrement

La base de données SQLLite utilisée par le logiciel en ligne MonEspace sont cryptées grâce à l'algorithme AES au travers de la bibliothèque "SynCrypto". La version implémentée par Synopse est le mode AES-OFB explicite avec dérivation IV rapide et réduction de mot de passe PBKDF2 éprouvée.

Pour plus d'information : https://synopse.info/files/html/api-1.18/SynCrypto.html

Évaluation : Acceptable

Contrôle des accès logiques

Les utilisateurs doivent mettre en place des mots de passe de plus de 8 caractéres et les changer tous les deux ans minimum.
Les mots de passe sont cryptés avant d'être stockés en base de données (algorithme SHA256).

Évaluation : Acceptable

Journalisation

Chaque accés à la plateforme MonEspace est enregistré dans une piste d'audit ainsi que toutes les modifications faites sur les profils, les droits ...

Évaluation : Acceptable

Archivage

Lors de la demande de ne plus avoir accés à la plate-forme MonEspace le profil de l'utilisateur est archivé.
Seuls les adminstrateurs de Logeas informatique ont accés aux données archivées.

Évaluation : Acceptable

Sécurisation de l'exploitation

La gestion de la plate-forme MonEspace est décrite dans le cadre de nos certifications qualité au travers de procédures disponibles sur la partie "certification" de notre wiki.
L'accés physique à la machine n'est pas possible (machine virtuelle), l'accés se faisant via une connexion à distance limitée par mot de passe

Évaluation : Acceptable

Sauvegarde des données

Les données sont sauvegardées chaque nuit sur le serveur (zip complet) puis synchronisées sur un poste de sauvegarde situé dans nos locaux (disque crypté) selon deux processus distincts.
Enfin le poste de sauvegarde fait l'objet d'une sauvegarde incrémentielle sur un nas distinct.

La procedure est décrite sur https://logeas.wiki.logeas.fr/doku.php?id=clientlourd:administration:transversal:sauvegarde

Évaluation : Acceptable

Évaluation : Acceptable

Maintenance

Les serveurs font l'objet d'un suivi par notre responsable réseau.
La version windows est systématiquement mise à jour.

Évaluation : Acceptable

Sécurisation des canaux informatiques

Les échanges se font via une connexion de type https.

Évaluation : Acceptable

Sécurité physique

Le data-center posséde un accés sécurisé

Évaluation : Acceptable

Gestion des personnels

Les personnels de logeas Informatique signent une charte informatique et plusieurs clauses de confidentialité sont incluses dans le contrat de travail.

Des formations et de la sensiblisation aux problématiques de sécurité sont régulièrement organisées

Évaluation : Acceptable

Risques

Accès illégitime à des données

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

Fuite de données non sensible ni banquaire

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

Accés avec un code de l'assistance à l'ensemble de la base, Piratage du serveur puis décryptage de la base

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

Hackeur

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

Chiffrement, Contrôle des accès logiques, Maintenance, Gestion des personnels, Sécurisation de l'exploitation

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

Limitée. Pas de données sensible ni banquaire, volume de donnée faible

Limitée, Pas de données sensible ni bancaire, volume de donnée faible

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

Négligeable, Les mesures prise en compte limite le risque

Évaluation : Acceptable

Risques

Modification non désirées de données

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

L'utilisateur n'a plus accés aux bases Logeas WEB de son compte, Les informations issu de Logeas informatique ne lui parviennent pas

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

Erreur humaine, Malveance, Malveillance, Erreur logiciel

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

Humaine

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

Contrôle des accès logiques, Journalisation, Sauvegarde des données, Gestion des personnels

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

Négligeable,

Le risque ne porte pas atteinte aux données mais à l'accés qui peut être facilement remis en place via l'assistance.

En cas de corruption importante les sauvegarde peuvent être facilement rermise en place.

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

Limitée, .

Évaluation : Acceptable

Risques

Disparition de données

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

Non accés au données du client

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

Erreur humaine, Crash serveur, Malveillance

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

Humaine, Hackeur

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

Sauvegarde des données

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

Limitée, Chaine de sauvegarde importante limitant le risque

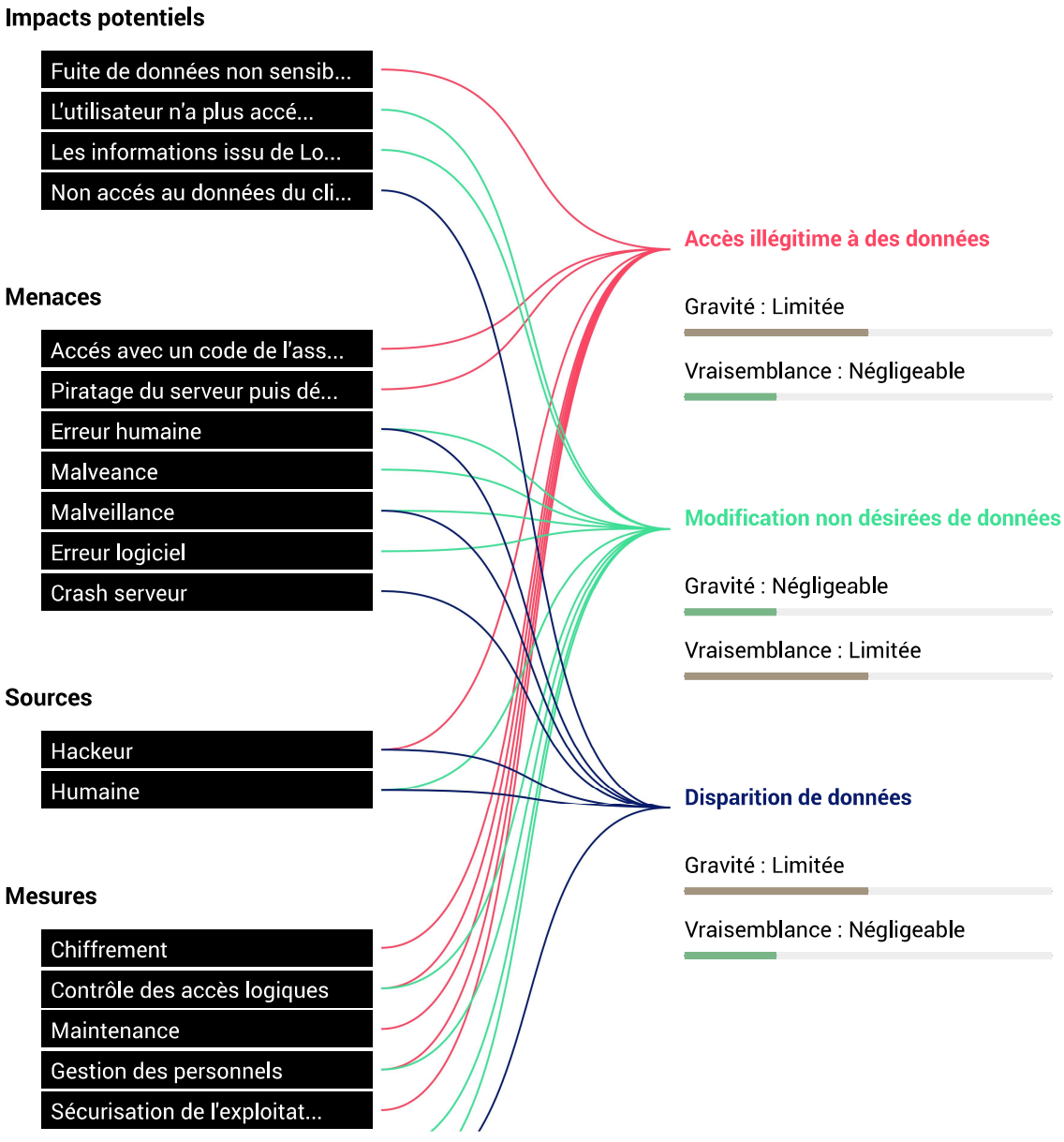
Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Négligeable, Les données sont facilement reconstituable

Évaluation : Acceptable

Risques

Vue d'ensemble des risques




Journalisation
Sauvegarde des données