
Polaris
LA NUIT DE L'INFO
2021

Liste des figures

Figure 1 : Cartographie des risques.....4

Figure 2 : plan d'action 5

Figure 3 : cycle de vie des données.....9

Figure 4 : Vue d'ensemble des risques.....22

Sommaire :

Validation **4**
Cartographie des risques **4**
Plan d'action **5**
Contexte **5**
Vue d'ensemble **5**
Données, processus et supports **7**
Principes fondamentaux **9**
Proportionnalité et nécessité **9**
Mesures protectrices des droits **10**
Risques **13**
Mesures existantes ou prévues **13**
Accès illégitime à des données **15**
Modification non désirées de données **17**
Disparition de données **18**
Vue d'ensemble des risques **22**

Validation

Cartographie des risques

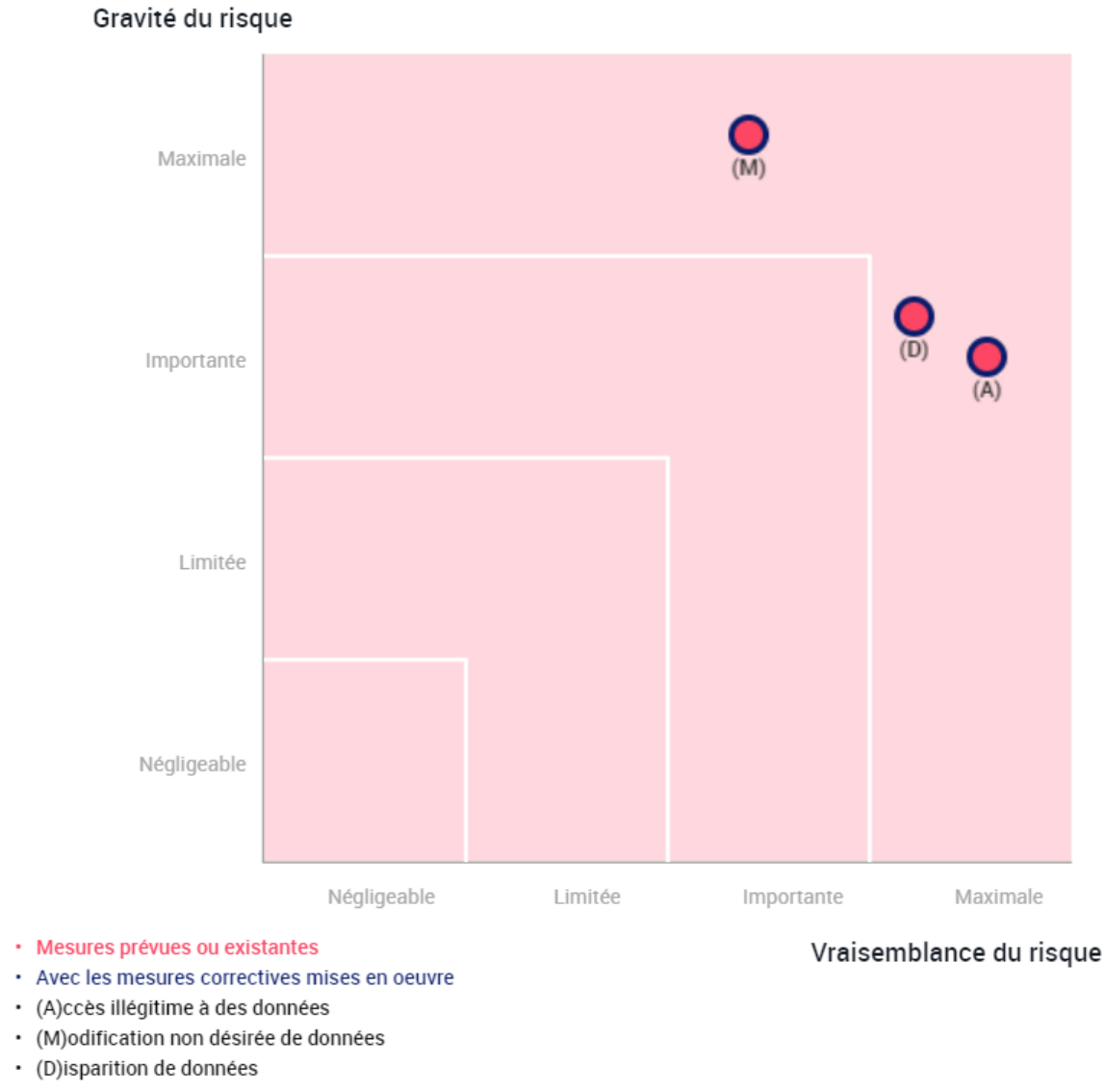

Figure 1 : Cartographie des risques

Validation

Plan d'action

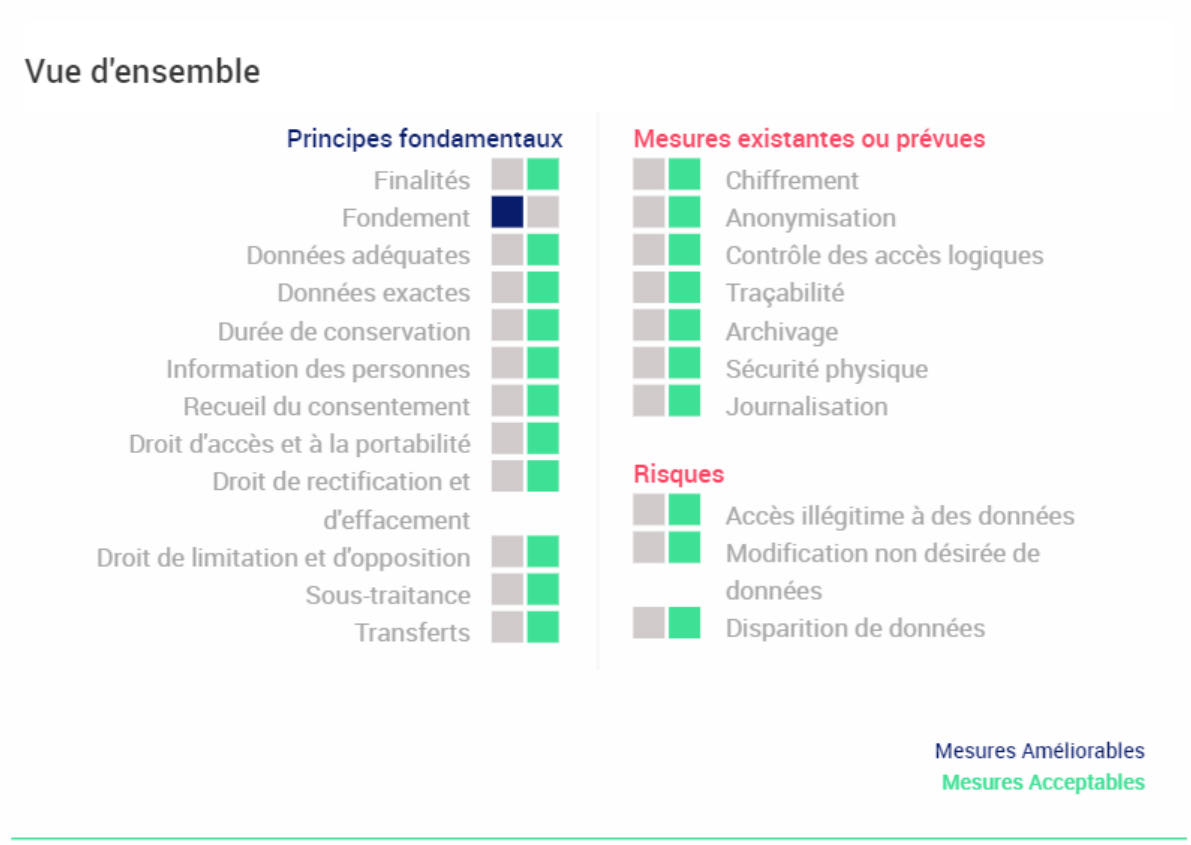

Figure 2 : plan d'action

Contexte

Vue d'ensemble

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

Le droit au respect de la vie privée est défini comme étant le droit à la protection de l'intimité de chaque naufragé contre toute intervention arbitraire d'une personne n'ayant aucun accès de privilégions.
Cette déclaration de respect de la vie privée décrit la façon dont nous gérons les données Personnelles que nous collectons par divers moyens tels que : formulaires, appels téléphoniques, Courriels et d'autres communications avec les naufragés.

Notre plateforme est subdivisée comme la suite:

-Espace administrateur : qui contient tous les données d 'audite, traçabilité, visualisation.
L'admin peut consulter toutes les nouveautés, accepter les demandes pour participer aux missions de sauvetage, visualiser les statistiques, et vérifier les demandes et les types d'intervenants.

-Espace de sauveteur : qui contient les données personnelles de chaque sauveur, le temps de chaque opération et les missions de sauvetage, toutes actualités sur l'états des bateaux, l'états des naufragés, reçu d'invitation pour participer dans la mission de sauvetage, (Exemples : lieu de sauvetage (dunkerquois).

-Espace des naufragés (remplie par les sauveteurs) contient leur nom, le numéro d'identifiant (s'il est possible), date de naissance de chaque naufragé, traits de visage, nationalité (s'il est possible), sexe, l'âge, lieu de naissance (s'il est possible), données sanitaire (atteint maladies chroniques, vacciné ou non ...).

-des personnes autorisées à visualiser certaines informations réparties comme suit :

- un journaliste qui a accès aux informations public (les statistiques disponibles sur le nombre de personnes sauvé (les morts et naufragés), intervalle d'âge)
- une association humanitaire qui a accès aux données sanitaire/médical en cas d'existence d'une maladie chronique ou accident au cours de la migration
-un policier qui a accès aux quelques information réduite donné par les naufragés La solution proposée assure les politiques de sécurité.

Quelles sont les responsabilités liées au traitement ?

Une donnée à caractère personnel est toute information sensible permettant directement ou indirectement d'identifier et classifier une personne : les informations personnelles, les données de localisation ou plusieurs Éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, Économique, culturelle ou sociale.

Le traitement de données de définit comme toute opération ou tout ensemble

d'opération Effectuées ou non à l'aide de procédés automatisés tels que la collecte, l'enregistrement, la Conversation, l'adaptation ou la modification, la consultation, l'utilisation....

Les données personnelles ne sont accessibles et traitées que par les personnes concernées par la mission de sauvetage car il n'est pas raisonnable d'accorder de tels droits de Façon non conditionnelle.
Ils sont sensibilisés à la confidentialité de ces données, à une utilisation légitime, garantir l'intégrité des données pour ne pas être altérer, ainsi qu'à la sécurité de ces données, et aussi la disponibilité des matériels et logiciels (les capteurs pour la signalisation, les antennes pour l'envoi et la réception des informations sensible et délicats , GPS , blackbox (s'il existe)) .

La confidentialité de données se fait par les algorithmes de chiffrement. Par exemple on utilise les algorithmes de chiffrement :

-Symétrique pour le cryptage des documents.

-Asymétrique pour l'échange de données.

- STEGANOGRAPHY pour cacher des informations sensible (par exemple photo, vidéo ...) pour éviter l'attention de toute interceptions et des actions malveillantes

La protection de la vie privée des naufragés a une importance cruciale.

Quels sont les référentiels applicables ?

Les référentiels applicables sont :
-**Les prestataires d'audit de la sécurité des systèmes d'information** pour protéger ces derniers.

-Les prestataires de détection des incidents visent à détecter les attaques informatiques afin de limiter les conséquences et de permettre une remédiation rapide.
-Les prestataires de réponse aux incidents de sécurité visent à réagir aux

attaques informatiques et interviennent lorsqu'une concordance de signaux permet de soupçonner ou d'attester une activité informatique malveillante au sein d'un système d'information.

Contexte

Données, processus et supports

Quelles sont les données traitées ?

Les données personnelles collectées peuvent inclure :
Coordonnées de naufragé, ou des personnes avec laquelle il migre : noms, adresse, e-mail et téléphone
-Sexe
- Nationalité
-Date et lieu de naissance de naufragé
-Composition et situation de famille
-Photos
-Numéro de la carte d'identité
-Dossier médical

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

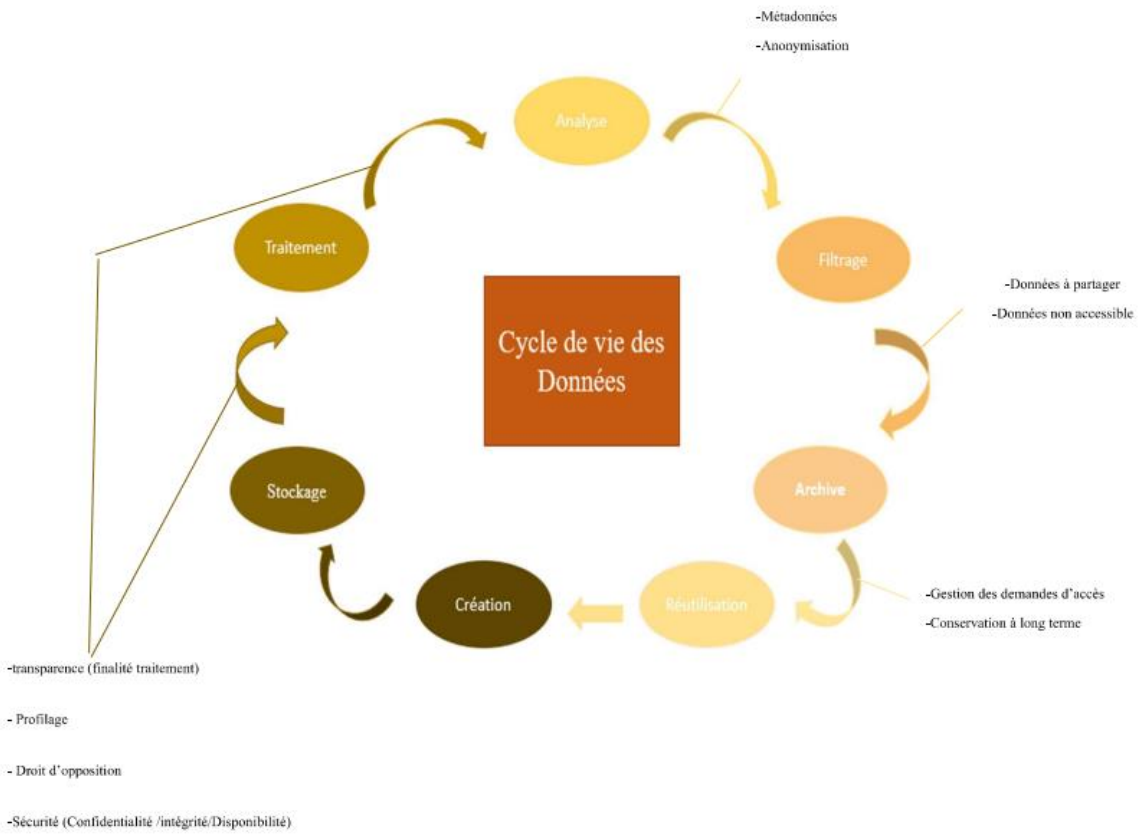

Figure 3 : cycle de vie des données

Quels sont les supports des données ?

Les supports de données :

-Blackbox

-Serveur cloud

-Carte à puce

-GPS

Principes fondamentaux

Proportionnalité et nécessité

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

Les données sont collectées pour des finalités déterminées et légitimes.
L'utilisation de ces données soit :

-Sur base de votre consentement.

-Parce que cela est nécessaire à l'exécution de la mission sauvetage.

-Afin d'établir la situation de naufragé en termes d'état sanitaire.

-Afin de justifier des dérogations à la situation administrative.

-Afin de réaliser une préanalyse de risque.

-Parce que le traitement est nécessaire à la sauvegarde des intérêts vitaux.

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

Les fondements de traitement :

-Droit d'accès aux données : Obtenir des informations sur le traitement des données à caractère personnel.

-Droit de rectification des données : Demander à faire rectifier les données personnelles si celles-ci sont erronées, inexactes ou incomplètes.

-Droit d'opposition à un traitement de données : opposer au traitement de données en motivant spécifiquement la demande.

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 sont collectées pour des finalités déterminés et légitimes.

Les données ont traité et les mesures de minimisation :

-Température, humidité, taux de particules, luminosité, données d'accéléromètre.

Les données sont-elles exactes et tenues à jour ?

Les sauveteurs peuvent modifier par l’application leurs données directement identifiantes à tout moment (adresse email, date de naissance, mot de passe ...)

Quelle est la durée de conservation des données ?

1er cas : Les données sont conservées tant que l'étudiant concerné n’en demande pas la suppression.

2éme cas : Les historiques vont être supprimées automatiquement si l'étudiant n'accède pas à l'application durant un mois.

Principes fondamentaux

Mesures protectrices des droits

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

Information des personnes concernées (traitement loyal et transparent)

Afin d'assurer la transparence et la pleine connaissance des conséquences de l'usage de l'application, pourrait informer ses utilisateurs sous forme de « pop-up » lors de l'activation de l'application, de manière concise, en des termes simples 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 .

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

Les données de naufragé seront disponibles si l'admin l'autorise par des procédures. Cette autorisation se fait par :

-Notification par mail.

-Notification par SMS.

-Notification par appel téléphonique.

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

L'administrateur de plateforme doit respecter l'intimité des naufragés par :

-Le droit d'accès : Ajout d'une liste ACL qui contienne des règles doivent être respectées

-Le droit à la portabilité offre à naufragés la possibilité de récupérer une partie des données dans un format lisible par une machine.

Libre de stocker ailleurs ces données portables ou les transmettre facilement d'un système à un autre, en vue d'une réutilisation à d'autres fins.

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

Les sauveurs peuvent exercer leurs droits de rectification et droit à l'effacement des données liée aux naufragés :

-En cas mis de modification ou suppression d'information : l'autorisation doit passer par la biométrie.

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

Droit à la limitation :

-Les coordonnées de naufragé doivent être renseignées pour le suivi.

-Pas de cookies droits à l'opposition :

La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière.

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

Sous-traitant :

BETA : Hébergement Cloud Privé (openstack,openshift, etc..).

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

Les données doivent être transférées d'une manière chiffrée par exemple :

- Utilisation de l'algorithme de diffie-hellman.

L'accès au réseau public doit passer par un proxy ou VPN pour assurer la transparence et l'anonymat.

Implémentation d'un firewall pour filtrer l'accès non autorisé.

Risques

Mesures existantes ou prévues

Chiffrement

Le principal objectif du chiffrement de données est de protéger la confidentialité des données Numériques tandis qu'elles sont stockées sur des systèmes informatiques et transmises via Internet ou d'autres réseaux.

Implémentation de Openssl, TLS, VPN... se passent par une phase de négociation et utilisation de l'algorithme de chiffrement asymétrique pour l'échange de clé public et privé.

Anonymisation

L'anonymisation est une action qui consiste à transformer des données personnelles de façon à ne plus permettre l'identification de la personne ciblée. Cette transformation doit être irréversible. C'est-à-dire qu'il ne doit pas exister de méthode directe ou indirecte permettant de rattacher les données à la personne concerné.

Cette technique est utile pour transmettre tout ou partie du jeu de données à un tiers qui a besoin de travailler sur les données réelles sans avoir besoin des données nominatives.

Les cas sont nombreux :

-Exploitation des données pour des traitements statistiques.

-Création d'un jeu de tests réalistes pour les environnements hors-production.

-Reconstruction du jeu de production sur un environnement pour étudier un incident.

Contrôle des accès logiques

Le contrôle d'accès logique est un système de contrôle d'accès aux systèmes d'information.
Il est généralement associé à un contrôle d'accès physique et permet de limiter le nombre d'utilisateurs du système d'information.
Le contrôle d'accès logique est divisé en trois éléments : l'authentification, l'autorisation et la traçabilité.
Ces étapes sont couvertes par AAA (Authentification, Autorisation

Comptabilité).
Le premier élément est de s'assurer que l'identité de l'entité demandant l'accès est connue de la base de données et de la prouver (par exemple, par un mot de passe connu de lui seul). Le second vérifie si l'entité a le droit d'utiliser les données après le premier.
Ce dernier permet de collecter des informations sur l'utilisation des données (durée de connexion, adresse IP de l'utilisateur, etc.).

Traçabilité

Étant un élément nécessaire pour effectuer les connexions des intervenants sur les équipements convenables et pour suivre leurs activités.
La traçabilité est aussi un outil de bonne gestion de production et d'une gestion des stocks rigoureuse. C'est notamment le cas de la mise en place d'un système code-barre pour les stocks de produits finis qui sert, éventuellement et le moins souvent possible, en cas de rappel mais qui sert surtout, tous les jours, pour une gestion des stocks efficace.

Aussi la traçabilité est une nécessité pour toute démarche de progrès : en effet, pour corriger une non-conformité, il faut pouvoir en retrouver l'origine et connaître les paramètres correspondants. Le lien entre le produit et les enregistrements est un élément essentiel de la démarche qualité.

Archivage

L'archivage est l'action d'archiver. C'est l'ensemble des techniques et moyens employés pour recueillir, classer, conserver et exploiter des documents jusqu'à leur destruction éventuelle.

Sécurité physique

La sécurité physique a trait à l'application de mesures de protection physiques et techniques pour prévenir l'accès illicite à des informations classifiées. L'officier de sécurité doit s'assurer que les mesures de protection répondent aux exigences établies.

Journalisation

La journalisation permet de récupérer rapidement un arrêt brutal du système.

Risques

Accès illégitime à des données

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

Apprécier les risques vie privée, traiter les risques, lancer un nouveau Traitement, ajouter et modifier des informations sensibles, qualifier le traitement.

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

* Porte dérobée ("backdoor") : Fonction d'un programme non autorisée et qui ne participe en rien aux objectifs officiels d'un programme.
* Cheval de Troie ("Trojan") Programme, jeu, commande ayant une fonction annoncée et en réalisant une autre (illicite) attaque classique s'exécute à l'insu de l'utilisateur.,
*Virus : Programme illicite qui s'insère dans des programmes légitimes appelés hôtes se reproduit automatiquement, se transmet, peut avoir des actions retardées se répand au travers d'internet, de disquettes, de clés USB.
* Lors d'un risque de MITM, un tiers intercepte une communication entre utilisateurs (ou machines).
* phishing : Les sites Web de phishing, également appelés sites usurpés, sont de fausses copies de sites Web réels que vous connaissez et en lesquels vous avez confiance. Les pirates créent ces sites falsifiés afin de vous tromper pour que vous saisissiez vos identifiants de connexion, qu'ils pourront ensuite utiliser pour se connecter aux comptes des sauveurs.

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

Les Risques politiques, Les risques liés à la portée, Les risques liés à l'échéancier et aux estimations d'efforts, Les risques dans les assomptions, Les risques liés aux dépendances, Les risques liés aux contraintes, Les risques liés à la technologie, Les risques liés aux critères d'acceptation, Les risques réglementaires, Les risques liés aux personnes, Les risques liés aux compétences et expertises.

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

Chiffrement, Anonymisation, Contrôle des accès logiques, Traçabilité, Archivage, Sécurité physique, Journalisation

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

Importante,

La gravité de risque permet d'obtenir une vision claire des traitements de données sensible à caractère personnel considérés.

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

Maximale,

La gravité de risque permet d'obtenir une vision claire des traitements de données sensible à caractère personnel considérés.

Risques

Modifications non désirées de données

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

Apprécier les risques vie privée., Qualifier le traitement., lancer un nouveau traitement., traiter les risques.

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

La gravité de risque permet d'obtenir une vision claire des traitements de données sensible à caractère personnel considérés.
*Virus : Programme illicite qui s'insère dans des programmes légitimes appelés hôtes se reproduit automatiquement, se transmet, peut avoir des actions retardées se répand au travers d'internet, de disquettes, de clés USB.
* Cheval de Troie ("Trojan") Programme, jeu, commande ayant une fonction annoncée et en réalisant une autre (illicite) attaque classique s'exécute à l'insu de l'utilisateur.
* Porte dérobée ("backdoor") : Fonction d'un programme non autorisée et qui ne participe en rien aux objectifs officiels d'un programme.
* Lors d'un risque de MITM, un tiers intercepte une communication entre utilisateurs (ou machines).
* phishing : Les sites Web de phishing, également appelés sites usurpés, sont de fausses copies de sites Web réels que vous connaissez et en lesquels vous avez confiance. Les pirates créent ces sites falsifiés afin de vous tromper pour que vous saisissiez vos identifiants de connexion, qu'ils pourront ensuite utiliser pour se connecter aux comptes des sauveurs.

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

Les risques liés à la portée., Les risques liés aux contraintes., Les risques liés aux compétences et expertises., Les risques liés aux personnes., Les risques liés à la technologie., Les risques liés aux critères d'acceptation., Risques politiques., Risques liés à la propriété intellectuelle.

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

Chiffrement, Anonymisation, Contrôle des accès logiques, Traçabilité, Archivage, Sécurité physique, Journalisation.

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

Maximale,
La gravité de risque est estimée par :

-L'analyse des données

-L'audit

-Les mesures de sécurité**…**

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

Importante, Les sources de risque sont différentes, ils proviennent de : logiciels, matériels, personnes...

Risques

Disparition de données

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

Apprécier les risques vie privée., lancer un nouveau traitement., Qualifier le traitement., traiter les risques.

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

* Cheval de Troie ("Trojan") Programme, jeu, commande ayant une fonction annoncée et en réalisant une autre (illicite) attaque classique s'exécute à l'insu de l'utilisateur.
* Lors d'un risque de MITM, un tiers intercepte une communication entre utilisateurs (ou machines).
* Porte dérobée ("backdoor") : Fonction d'un programme non autorisée et qui ne participe en rien aux objectifs officiels d'un programme.
* phishing : Les sites Web de phishing, également appelés sites usurpés, sont de fausses copies de sites Web réels que vous connaissez et en lesquels vous avez confiance. Les pirates créent ces sites falsifiés afin de vous tromper pour que vous saisissiez vos identifiants de connexion, qu'ils pourront ensuite utiliser pour se connecter aux comptes des sauveurs., *Virus : Programme illicite qui s'insère dans des programmes légitimes appelés hôtes se reproduit automatiquement, se transmet, peut avoir des actions retardées se répand au travers d'internet, de disquettes, de clés USB.

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

Les risques liés aux personnes., Les risques liés aux contraintes., Les risques liés à la portée., Les risques liés à la technologie., Risques politiques., Risques liés à la propriété intellectuelle., Les risques liés aux critères d'acceptation.

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

Chiffrement, Anonymisation, Contrôle des accès logiques, Traçabilité, Archivage, Sécurité physique, Journalisation.

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

Importante, La gravité du risque peut être estimé par les méthodes de chiffrement (chiffrement symétrique, asymétrique, STEGANOGRAPHY), identifier, évaluer et prioriser les risques relatifs aux activités.

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

Maximale,
Les sources de risques se diffèrent par :
Risques humains : malveillance, usurpation, ingénierie sociale, l'espionnage...

Risques technologiques : Menaces liés aux matériels, aux logiciels, à l'environnement.

Risques juridiques : Non-respect de la législation relative à la signature numérique et les conventions entre les états (responsable de migration) et les fournisseurs de cloud

Risques

Vue d'ensemble des risques

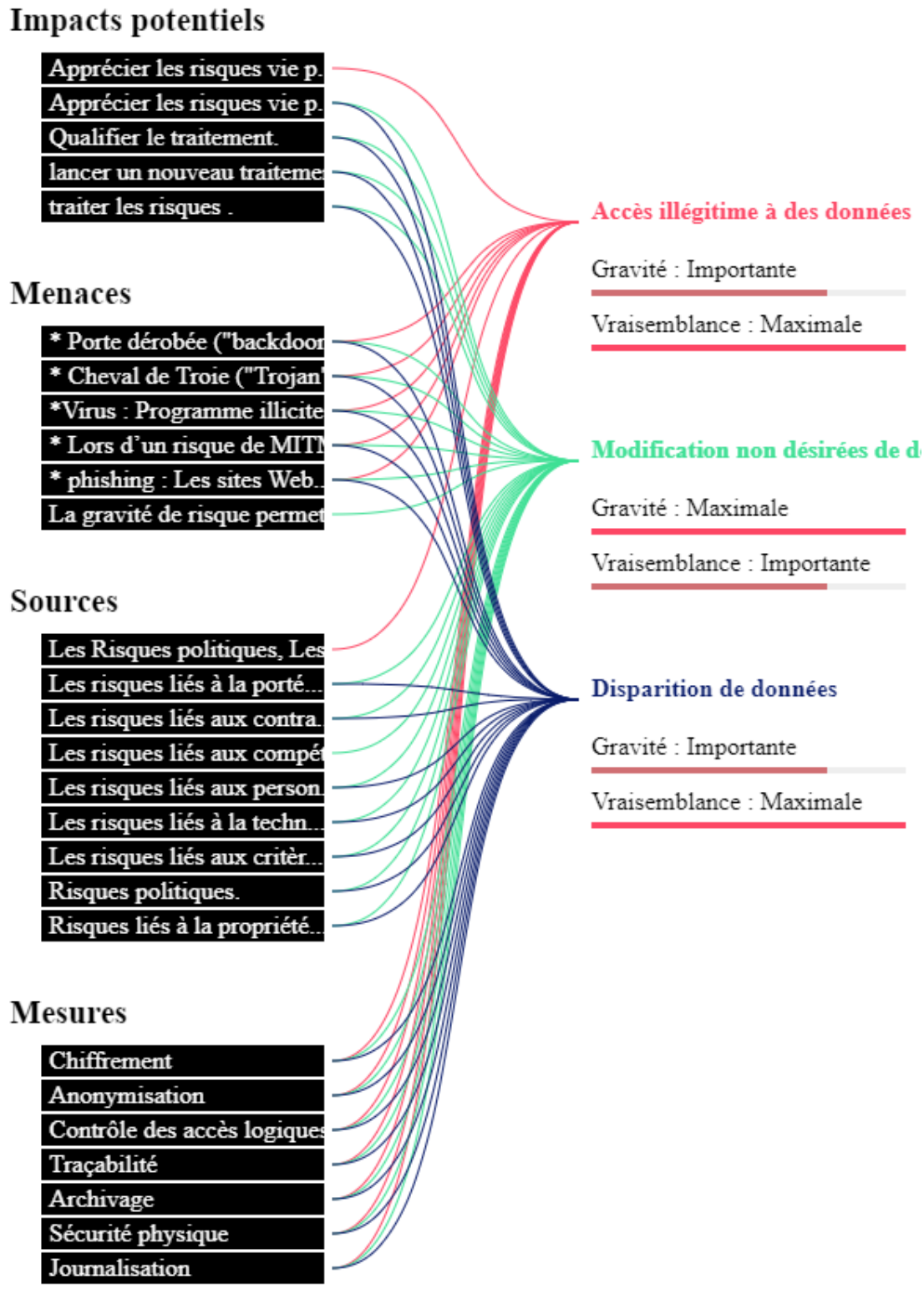

Figure 4 : Vue d'ensemble des risques