Modèle :	Manuel de Référence G2S - V 1.0 du 16/02/2016
Type :	G - Modèle Guide
Référent du modèle :	A Sarr (ASA – aissatou.sarr@almerys.com – 06.86.42.88.59)

Manuel de Référence

Fiche Réflexe

Contrôle de conformité à l'utilisation de données personnelles préalable à tous projets

Objet / Synthèse *	Cette Fiche Réflexe doit être utilisée en amont d'un projet. Il vous est demandé dans celle-ci d'effectuer une description précise du projet afin d'évaluer la proportionnalité entre la finalité du traitement et l'utilisation des données à caractère personnel. Elle a pour objectif de définir si des démarches de mise en conformité sont à effectuer auprès des autorités de protection des données (CNIL), le type de démarche et les délais avant d'avoir la possibilité d'utiliser ces données.
Client	-
Projet	-

Niveau de diffusion *	D2 - Interne G2S Group
Liste de Diffusion	Collaborateurs
Localisation * (GED ou réseau)	https://www.ged.almerys.com/nuxeo/nxdoc/default/a43878c3-7e2b-4795-96d4-d4fac869fffa/view_documents

Version *	Date *	Modifications *	Rédacteur *
V1.0	17/03/2016	Création	Aïssatou SARR (ASA)
V2.0	16/05/2016	Modification	Aïssatou SARR (ASA)
V3.0	29/11/2016	Modification	Aïssatou SARR (ASA)
V4.0	20/01/2017	Modification	Aïssatou SARR (ASA)

Date de péremption	31/12/2017
Responsable d'actualisation	Aïssatou SARR (ASA)
Identifiant du document	-

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

Documents de Références

Libellé	Adresse GED ou WIKI ou Chemin réseau ou *insertion du document*

Glossaire

Terme / Acronyme	Définition
DCP	Données à Caractère Personnel
CNIL	Commission Nationale de l'Informatique et des Libertés
RT	Responsable de Traitement
ART	Article
CIL	Correspondant Informatique et Libertés
C	Confidentialité
I	Intégrité
D	Disponibilité

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

Sommaire

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

1. Introduction

1.1. Objet

Protection des Données à Caractère Personnel

« L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques » (ART 1 de la loi du 6 janvier 1978).

1.2. Application

« *La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles. »* (ART 2-1 de la loi du 6 janvier 1978).

1.3. Définitions

Qu'est-ce qu'une données à caractère personnel ?

« Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. » (ART 2-2)

Par exemple : le nom, prénom, date de naissance, adresse, login, mot de passe, numéro de téléphone, géolocalisation, adresses IP, photographies, Numéro d'Inscription au Répertoire de l'INSEE (NIR), etc…

Qu'est-ce qu'un traitement de données à caractère personnel ?

« Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment :

- *La collecte*
- *L'enregistrement*
- *L'organisation*
- *La conservation*
- *L'adaptation*
- *La modification*
- *L'extraction*
- *La consultation*
- *L'utilisation*
- *La communication par transmission*
- *La diffusion ou toute autre forme de mise à disposition*
- *Le rapprochement*
- *L'interconnexion*
- *Le verrouillage*
- *L'effacement*
- *La destruction »* (ART2-3)

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

1.4. Objectifs

Avoir une conformité totale avec la loi Informatique et Libertés du 06 janvier 1978 et plus globalement assurer la protection des données à caractère personnel et/ou sensibles collectées dans le cadre des traitements et services d'almerys, ce quelle que soit la responsabilité d'almerys vis-à-vis du traitement (responsable de traitement ou sous-traitant).

Cette fiche permet d'évaluer la nécessité ou pas d'effectuer des démarches auprès de la CNIL. Celles-ci peuvent être plus ou moins longues (immédiate, 6 mois, 1 an) selon le traitement mis en œuvre et bien sûr ces démarches doivent être faites avant la mise en place du traitement.

L'objectif est donc d'anticiper tous blocages que l'on pourrait avoir, afin que le projet se déroule sans problèmes de conformité avec la loi Informatique et libertés.

1.5. Existant

Lorsque le service existe déjà, il a normalement fait l'objet d'un audit de façon à l'inscrire sur le registre des traitements almerys.

1.6. Point Clé

Il faut garder à l'esprit que la donnée à caractère personnel et/ou sensible ne nous appartient pas, elle est la propriété exclusive de la personne concernée.

1.7. Mode d'emploi

Retourner la fiche réflexe ci-dessous au CIL, en préfixant le nom du fichier et le nom du projet avec la date (format JJ/MM/AAAA).

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

2. Identifier le(s) service(s) concerné(s)

- Nom du ou des services organisationnels chargés de la conception *(Pôle/Direction)* :
  - …
  - …
- Responsable du projet *(Prénom/Nom)* :
- Date de mise en production *(JJ/MM/AAAA)* :
- Nouveau traitement ou modification d'un traitement existant :

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

3. Questions macro

3.1. Définir le cadre d'utilisation du traitement

Quel est le cadre d'utilisation de mon traitement ? Pourquoi doit-il être mis en projet ?

- Quels clients
- Le contexte
- Etc…

3.2. Définir la finalité du traitement

Quelle est la ou les finalités du traitement du projet ?

Expliquer la finalité du traitement, c'est à dire :

- Pourquoi ce traitement a été mis en place ?
- Que fait le traitement ?
- En quoi le projet nécessite l'utilisation de données personnelles ?

Y-a-t-il des sous-finalités dans mon traitement ?

3.3. Expliquer le traitement

Quel type de traitement va être appliqué aux données à caractère personnel et ou sensibles ?

Expliquer quel est le type de traitement appliqué aux données à caractère personnel et ou sensibles :

- La collecte
- L'enregistrement
- L'organisation
- La conservation
- L'adaptation
- La modification
- L'extraction
- La consultation
- L'utilisation
- La communication par transmission
- La diffusion ou toute autre forme de mise à disposition
- Le rapprochement
- L'interconnexion
- Le verrouillage
- L'effacement
- La destruction

3.4. Définir les destinataires

Qui aura accès aux données à caractère personnel ? En interne (ex : l'exploitation applicative, le support, etc…) ou en Externe (ex : le client, des partenaires, des fournisseurs, etc…)

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

4. Définition du besoin

Après avoir décrit le service ci-dessus, il s'agit maintenant de se poser les bonnes questions sur la pertinence du traitement et de ses modalités d'application.

4.1. Quelles sont les données personnelles indispensables à la mise en œuvre du projet ?

Veuillez lister précisément toutes les données à caractère personnel nécessaires au projet.

Exemple : Nom, prénom, adresse, géolocalisation…

4.2. Les données collectées sont-elles nécessaires ?

Il faut comprendre ici : la collecte de ces données est-elle licite, nécessaire, suffisante et justifiée dans le cadre de la finalité du traitement.

Expliquer brièvement en quoi ces données sont nécessaires.

4.3. Mise en œuvre

Qui sera chargé de la mise en œuvre du traitement (nom, prénom et coordonnées) ?

En interne : Point de contact en cas de besoin

En externe : Permet de savoir s'il on utilise des sous-traitants et le cas échéant vers qui le CIL doit-il s'orienter pour avoir plus d'informations.

4.4. Quels seront les applicatifs ou les produits impactés ?

Lors de la mise en place du projet, des Mises en Productions (MEP) vont être nécessaires. Cette question permet de définir quels vont être les applicatifs, produits, etc. qui seront impactés par le projet.

Cela permet de savoir notamment, quelles sont les MEP qui vont nécessiter un transfert de la Fiche Réflexe afin que la MEP puisse être validée.

Par exemple, le Projet X va nécessiter une modification d'AGAPS, ADELE, le site des PEC, etc.

Il faudra donc fournir aux DDA/RSA la Fiche Réflexe validée du Projet X pour qu'ils l'intègrent dans leur package de MEP.

4.5. Mon projet nécessite-t-il de collecter des données sensibles ?

Une donnée à caractère sensible est une donnée pouvant générer une discrimination sur la personne concernée (santé, pratiques sexuelles, pratiques religieuses, etc.)
Attention la CNIL interdit de collecter ou de traiter des données sensibles qui font apparaître, directement ou indirectement,

- **Les origines raciales, ou ethniques**

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

- **Les opinions politiques,**
- **Philosophiques ou religieuses,**
- **L'appartenance syndicale**
- **Les données de santé (code acte, pathologies, soins, etc…)**

Il convient d'être très prudent et très attentif sur la nécessité de collecter de telles données.
La CNIL veille tout particulièrement à la réelle nécessité et proportionnalité de telles collectes et aux mesures de protection et d'information qui sont mises autour.

CAS PARTICULIER DU NNI ou du NIR : JE NE L'UTILISE QUE SI LE TRAITEMENT LE JUSTIFIE DANS UN CADRE REGLEMENTAIRE ET JURIDIQUE PRECIS DONC UNIQUEMENT DANS LE CAS DE TRAITEMENTS LIES A LA SANTE ET SUR BESOIN LICITE ET NECESSAIRE. Pas de clé dans les bases de données basée sur les NNI, à proscrire absolument.

Veuillez lister les données sensibles (notamment de santé) nécessaires.

4.6. Dois-je collecter des données pour les logs ?

Il s'agit ici de données tracées. Elles ne doivent être récupérées pour des logs, si et seulement s'il n'est pas possible de faire autrement dans le cadre de la finalité du traitement.

4.7. Vais-je faire des interconnexions ?

L'interconnexion c'est lorsque que l'on utilise deux traitements ayant des finalités différentes, que l'on croise afin de mettre en place un nouveau traitement indépendant des deux autres.

ATTENTION : L'INTERCONNEXION NECESSITE UNE DEMANDE D'AUTORISATION A LA CNIL (voir 4.13)

4.8. Dois-je informer le propriétaire de la collecte de ses données ?

Généralement oui. Une mention CNIL suffit dans la majeure partie des cas. Elle doit être visible et non sur un lien obscur.
Attention à la collecte de données de santé, il est nécessaire de demander le consentement explicite du propriétaire de la donnée.

Toutefois, si nous sommes sous-traitants, ce n'est pas à nous de prévenir le propriétaire des données mais au Responsable de Traitement (le client).

4.9. Quelle sera la durée de conservation des données ?

Cette durée doit toujours être justifiée, établie et indiquée, quel que soit le traitement.
D'une manière générale, les données ne doivent être conservées que le temps nécessaire au traitement, après elles doivent être :

- **soit archivées,**
- **soit purgées,**
- **soit anonymisées.**

Si des données sont récupérées dans des logs (voir paragraphe 4.4), cette question s'applique aussi.

Si la durée de conservation se base sur un fondement légal, veuillez l'indiquer.

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

4.10. Comment ou quel mécanisme d'archivage vais-je mettre en place ?

Veuillez indiquer quel logiciel d'archivage sera utilisé.

4.11. Comment vais-je assurer la confidentialité des données ?

Dans tous les cas, l'appropriation par un tiers non autorisé des données à caractère personnel et/ou sensible peut nuire au propriétaire de la donnée.

Donc j'assure la confidentialité des données.

Mécanisme : (anonymisation, chiffrage, cryptage, etc…)

Veuillez décrire le procédé utilisé.

4.12. Comment assurer l'application du droit des personnes ?

Comme précisé plus haut, les données à caractère personnel et/ou sensible sont la propriété exclusive de la personne concernée. Il est donc nécessaire et justifié que ces données soient disponibles sur demande de l'intéressé.

Conformément aux articles 38, 39 et 40 de la loi n° 78-17 du 6 janvier 1978 la personne concernée dispose d'un droit d'accès, de modification, de rectification et de suppression (droit à l'oubli) pour raison légitime de ses données personnelles.

Il faut donc inscrire le nom de la personne qui se chargera de ce droit d'accès. Elle sera la personne vers laquelle le CIL pourra se tourner en cas de demande de droit d'accès aux données.

4.13. Comment est assurée l'intégrité des données ?

La donnée à caractère personnel et/ou sensible doit dans tous les cas être intègre !

Quels sont les moyens utilisés pour respecter l'intégrité, la confidentialité et la sécurité des données ?

Par exemple : liste restreinte de personnes ayant accès aux données, données chiffrées, etc…

4.14. Vais faire appel à un sous-traitant ou à une entreprise externe ?

Si oui, veuillez décrire l'entreprise sollicitée, les actions qu'elles auront à mener, leurs périmètres d'action, etc…

4.15. Vais-je transférer ces données vers un pays tiers ?

Le transfert vers des pays tiers nécessite des mécanismes de sécurité (confidentialité et intégrité des données).
De plus, hors Union Européenne il faut une demande d'autorisation auprès de la CNIL.
Ce transfert doit être justifié dans le cadre de la finalité du traitement.

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

La demande d'autorisation de la CNIL est un processus long, donc s'il y a transfert il faut le faire savoir le plus tôt possible afin que l'on obtienne l'autorisation le plus RAPIDEMENT possible AVANT de pouvoir mettre le traitement en œuvre.

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

5. Etude d'Impact sur la Vie Privée (EIVP) ou Privacy Impact Assessment (PIA)

5.1. Définitions :

La Loi informatique et libertés (article 34), impose aux responsables de traitement de « *prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données* ».
Chaque responsable doit donc identifier les risques engendrés par son traitement avant de déterminer les moyens adéquats pour les réduire.

Un PIA (Privacy Impact Assessment) ou étude d'impacts sur la vie privée (EIVP) repose sur deux piliers :

- les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés. Ils ne peuvent faire l'objet d'aucune modulation, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
- la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données personnelles.

Remplissez le tableau ci-dessous en vous aidant des informations que vous trouverez à partir du 5.2. Ce tableau vous permettra d'effectuer l'Etude d'Impact sur la Vie Privée (EIVP).

Niveaux	Descriptions génériques des impacts (directs et indirects)	Impacts corporels	Impacts matériels	Impacts moraux
1. Négligeable				
2. Limitée				
3. Importante				
4. Maximale				

5.2. Les échelles d'impact

Il est demandé ici d'effectuer une analyse d'impact du projet sur la vie privée. Pour vous aider voici une échelle d'impact avec des exemples permettant d'estimer la gravité des évènements redoutés, mettez en rouge les éléments pouvant concerner le projet et complétez avec les informations manquantes :

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels	Exemples d'impacts matériels	Exemples d'impacts moraux
1. Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront	- Absence de prise en charge adéquate d'une personne non autonome (mineur, personne sous tutelle) - Maux de tête passagers	- Perte de temps pour réitérer des démarches ou pour attendre de les réaliser - Réception de courriers non sollicités (ex. : *spams*) - Réutilisation de données publiées sur des sites	- Simple contrariété par rapport à l'information reçue ou demandée - Peur de perdre le contrôle de ses données - Sentiment d'atteinte à la vie privée sans préjudice réel ni

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

	sans difficulté		Internet à des fins de publicité ciblée (information des réseaux sociaux réutilisation pour un mailing papier) - Publicité ciblée pour des produits de consommation courants	objectif (ex : intrusion commerciale) - Perte de temps pour paramétrer ses données - Non-respect de la liberté d'aller et venir en ligne du fait du refus d'accès à un site commercial (ex : alcool du fait d'un âge erroné)
2. Limitée	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	- Affection physique mineure (ex. : maladie bénigne suite au non respect de contre-indications) - Absence de prise en charge causant un préjudice minime mais réel (ex : handicap) - Diffamation donnant lieu à des représailles physiques ou psychiques	- Paiements non prévus (ex. : amendes attribuées de manière erronée), frais supplémentaires (ex. : agios, frais d'avocat), défauts de paiement - Refus d'accès à des services administratifs ou prestations commerciales - Opportunités de confort perdues (ex. : annulation de loisirs, d'achats, de vacances, fermeture d'un compte en ligne) - Promotion professionnelle manquée - Compte à des services en ligne bloqué (ex. : jeux, administration) - Réception de courriers ciblés non sollicités susceptible de nuire à la réputation des personnes concernées - Élévation de coûts (ex. : augmentation du prix d'assurance) - Données non mises à jour (ex. : poste antérieurement occupé) - Traitement de données erronées créant par exemple des dysfonctionnements de comptes (bancaires, clients, auprès d'organismes sociaux, etc.) - Publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel (ex : publicité grossesse, traitement pharmaceutique) - Profilage imprécis ou abusif	- Refus de continuer à utiliser les systèmes d'information (*whistleblowing*, réseaux sociaux) - Affection psychologique mineure mais objective (diffamation, réputation) - Difficultés relationnelles avec l'entourage personnel ou professionnel (ex. : image, réputation ternie, perte de reconnaissance) - Sentiment d'atteinte à la vie privée sans préjudice irrémédiable - Intimidation sur les réseaux sociaux
3. Importante	Les personnes concernées pourraient connaître	- Affection physique grave causant un préjudice à long	- Détournements d'argent non Indemnisé - Difficultés financières non	- Affection psychologique grave (ex. : dépression, développement d'une phobie)

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

	des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives	terme (ex. : aggravation de l'état de santé suite à une mauvaise prise en charge, ou au non-respect de contre-indications) - Altération de l'intégrité corporelle par exemple à la suite d'une agression, d'un accident domestique, de travail, etc.	temporaires (ex. : obligation de contracter un prêt) - Opportunités ciblées, uniques et non récurrentes, perdues (ex. : prêt immobilier, refus d'études, de stages ou d'emploi, interdiction d'examen) - Interdiction bancaire - Dégradation de biens - Perte de logement - Perte d'emploi - Séparation ou divorce - Perte financière à la suite d'une escroquerie (ex. : après une tentative d'hameçonnage - *phishing*) - Bloqué à l'étranger - Perte de données clientèle	- Sentiment d'atteinte à la vie privée et de préjudice irrémédiable - Sentiment de vulnérabilité à la suite d'une assignation en justice - Sentiment d'atteinte aux droits fondamentaux (ex. : discrimination, liberté d'expression) - Victime de chantage - *Cyberbullying* et harcèlement moral
4. Maximale	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter	- Affection physique de longue durée ou permanente (ex. : suite au non-respect d'une contre-indication) - Décès (ex. : meurtre, suicide, accident mortel) - Altération définitive de l'intégrité physique	- Péril financier - Dettes importantes - Impossibilité de travailler - Impossibilité de se reloger - Perte de preuves dans le cadre d'un contentieux - Perte d'accès à une infrastructure vitale (eau, électricité)	- Affection psychologique de longue durée ou permanente - Sanction pénale - Enlèvement - Perte de lien familial - Impossibilité d'ester en justice - Changement de statut administratif et/ou perte d'autonomie juridique (tutelle)

5.3. Les menaces :

Veuillez présenter ici les potentielles et hypothétiques menaces :

Menaces	Sources de risques	Mesures	Vraisemblance	Justification

Voici des exemples de différentes sources de menaces possibles :
Les supports peuvent être :

- utilisés de manière inadaptée : les supports sont utilisés hors de leur cadre d'utilisation prévu, voire détournés, sans être modifiés ni endommagés ;
- observés : les supports sont observés ou espionnés sans être endommagés ;

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

- surchargés : les limites de fonctionnement des supports sont dépassées, ils sont surchargés, surexploités ou utilisés dans des conditions ne leur permettant pas de fonctionner correctement ;
- détériorés : les supports sont endommagés, partiellement ou totalement ;
- modifiés : les supports sont transformés ;
- perdus : les supports sont perdus, volés, vendus ou donnés, de telle sorte qu'il n'est plus possible d'exercer les droits de propriété.

Voici des menaces génériques exhaustives, indépendantes et appliquées aux spécificités de la protection de la vie privée :

Menaces qui peuvent mener à un accès illégitime aux DCP :

Critères touché	Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
C	Matériels	Utilisés de manière inadaptée	Utilisation de clefs USB ou disques inappropriés à la sensibilité des informations, utilisation ou transport d'un matériel sensible à des fins personnelles, le disque dur contenant les informations est utilisé pour une fin non prévue (par exemple pour transporter d'autres données chez un prestataire, pour transférer d'autres données d'une base de données à une autre, etc.)	Utilisable en dehors de l'usage prévu, disproportion entre le dimensionnement des matériels et le dimensionnement nécessaire (par exemple : disque dur de plusieurs To pour stocker quelques Go de données)
C	Matériels	Observés	Observation d'un écran à l'insu de son utilisateur dans un train, photographie d'un écran, géolocalisation d'un matériel, captation de signaux électromagnétiques à distance	Permet d'observer des données interprétables, émet des signaux compromettants
C	Matériels	Modifiés	Piégeage par un keylogger, retrait d'un composant matériel, branchement d'un appareil (ex. : clé USB) pour lancer un système d'exploitation ou récupérer des données	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions) via des connecteurs (ports, slots), permet de désactiver des éléments (port USB)
C	Matériels	Perdus	Vol d'un ordinateur portable dans une chambre d'hôtel, vol d'un téléphone portable professionnel par un pickpocket, récupération d'un matériel ou d'un support mis au rebut, perte d'un support de stockage électronique	Petite taille, attractif (valeur marchande)
C	Logiciels	Utilisé de manière inadaptée	Fouille de contenu, croisement illégitime de données, élévation de privilèges, effacement de traces, envoi de *spams* depuis la messagerie, détournement de fonctions réseaux	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées
C	Logiciels	Observés	Balayage d'adresses et ports réseau, collecte de données de configuration, étude d'un code source pour déterminer les défauts exploitables, test des réponses d'une base de données à des requêtes malveillantes	Possibilité d'observer le fonctionnement du logiciel, accessibilité et intelligibilité du code source
C	Logiciels	Modifiés	Piégeage par un keylogger logiciel, contagion par un code malveillant, installation d'un outil de prise de contrôle à distance, substitution d'un composant par un autre lors d'une mise à jour, d'une opération de maintenance ou d'une installation (des bouts de codes ou applications sont installés ou remplacés)	Modifiable (améliorable, paramétrable), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes), ne fonctionne pas correctement ou conformément aux attentes
C	Canaux informatiques	Observés	Interception de flux sur le réseau Ethernet, acquisition de données sur un réseau wifi	Perméable (émission de rayonnements parasites ou non), permet d'observer des données interprétables
C	Personnes	Observées	Divulgation involontaire en conversant, écoute d'une salle de réunion avec un matériel d'amplification sensorielle	Peu discret (loquace, sans réserve), routinier (habitudes facilitant l'espionnage récurrent)
C	Personnes	Détournées	Influence (hameçonnage, filoutage, ingénierie sociale, corruption), pression (chantage, harcèlement moral)	Influençable (naïf, crédule, obtus, faible estime de soi, faible loyauté), manipulable (vulnérable aux pressions sur soi ou son entourage)

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

C	Personnes	Perdues	Débauchage d'un employé, changement d'affectation, rachat de tout ou partie de l'organisation	Faible loyauté vis-à-vis de l'organisme, faible satisfaction des besoins personnels, facilité de rupture du lien contractuel
C	Documents papiers	Observés	Lecture, photocopie, photographie	Permet d'observer des données interprétables
C	Documents papiers	Perdues	Vol de dossiers dans les bureaux, vol de courriers dans la boîte aux lettres, récupération de documents mis au rebut	Portable
C	Canaux papier	Observés	Lecture de parapheurs en circulation, reproduction de documents en transit	Observable

Menaces qui peuvent mener à une modification non désirées des DCP :

Critères touché	Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
I	Matériels	Modifiés	Ajout d'un matériel incompatible menant à un dysfonctionnement, retrait d'un matériel indispensable au fonctionnement correct d'une application	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions) via des connecteurs (ports, slots), permet de désactiver des éléments (port USB)
I	Logiciels	Utilisé de manière inadaptée	Modifications inopportunes dans une base de données, effacement de fichiers utiles au bon fonctionnement, erreur de manipulation menant à la modification de données	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées
I	Logiciels	Modifiés	Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre	Modifiable (améliorable, paramétrable), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes), ne fonctionne pas correctement ou conformément aux attentes
I	Canaux informatiques	Utilisé de manière inadaptée	*Man in the middle* pour modifier ou ajouter des données à un flux réseau, rejeu (réémission d'un flux intercepté)	Permet d'altérer les flux communiqués (interception puis réémission, éventuellement après altération), seule ressource de transmission pour le flux, permet de modifier les règles de partage du canal informatique (protocole de transmission qui autorise l'ajout de nœuds)
I	Personnes	Surchargées	Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences	Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail, compétences inappropriées à la fonction Incapacité à s'adapter au changement
I	Personnes	Détournées	Influence (rumeur, désinformation)	Influençable (naïf, crédule, obtus)
I	Documents papier	Modifiés	Modification de chiffres dans un dossier, remplacement d'un document par un faux	Falsifiable (support papier au contenu modifiable)
I	Canaux papier	Modifiés	Modification d'une note à l'insu du rédacteur, changement d'un parapheur par un autre, envoi multiple de courriers contradictoires	Permet d'altérer les documents communiqués, seule ressource de transmission pour le canal, permet la modification du circuit papier

C : Confidentialité
I : Intégrité
D : Disponibilité

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite

5.4. La vraisemblance des menaces

L'échelle suivante va vous permettre d'estimer la vraisemblance des menaces :

La vraisemblance traduit la possibilité qu'un risque se réalise. Elle est essentiellement estimée au regard des vulnérabilités des supports concernés et de la capacité des sources de risques à les exploiter, compte tenu des mesures existantes, prévues ou complémentaires (qu'il convient de mentionner en tant que justification).

1. Négligeable : il ne semble pas possible que les sources de risques retenues puissent réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge et code d'accès).

2. Limité : il semble difficile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge).

3. Important : il semble possible pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans les bureaux d'un organisme dont l'accès est contrôlé par une personne à l'accueil).

4. Maximal : il semble extrêmement facile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papier stockés dans le hall public de l'organisme).

SANS AUTORISATION DE LA CNIL ON NE PEUT PAS UTILISER LES DONNEES PERSONNELLES

LA FICHE REFLEXE DOIT ETRE REMPLIE CHAQUE FOIS QU'UN PROJET DOIT ETRE MIS EN ŒUVRE, ET CE AVANT L'UTILISATION DES DONNEES.

LE CORRESPONDANT INFORMATIQUE ET LIBERTES RESTE A VOTRE DISPOSITION POUR VOUS AIDER A REMPLIR CETTE FICHE OU POUR TOUT AUTRE QUESTION :

correspondant.pro.dp@almerys.com

****** Fin du document ******

© G2S Group - Propriété exclusive de G2S Group. Reproduction interdite