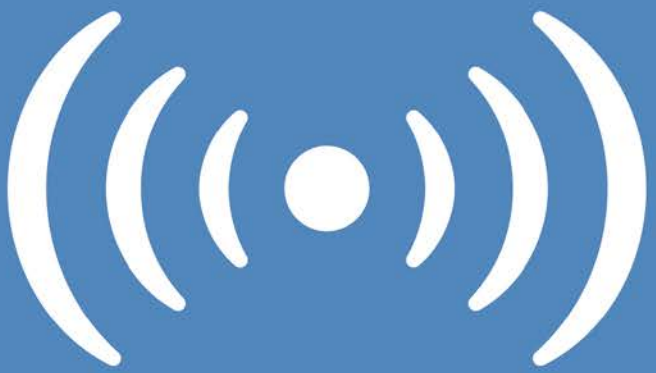
Analyse d'impact relative à la protection des données

Privacy Impact Assessment (PIA)

APPLICATION AUX OBJETS CONNECTÉS



CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Édition février 2018

Table des matières

Avant-propos

Ce document est une déclinaison des guides PIA de la CNIL au secteur spécifique des objets connectés.

Théoriquement mené par un responsable de traitement ou un fournisseur, un PIA a pour objectif de construire et de démontrer la mise en œuvre des principes de protection de la vie privée afin que les personnes concernées conservent la maîtrise de leurs données à caractère personnel.

Le fonctionnement itératif de cette méthode doit permettre de garantir une utilisation raisonnée et fiable de ces données dans le traitement.

Ce document est basé sur la méthode PIA de la CNIL

La méthode comporte trois guides, décrivant respectivement la démarche, les éléments pour formaliser l'étude et un guide de bonne pratiques pour la protection de la vie privée :

Ils sont téléchargeables sur le site de la CNIL et seront utiles pour remplir ce document :

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

Ce document a la structure d'un rapport de PIA, qui est le livrable du PIA[1].

Certaines parties de ce document [zones grisées] sont renseignées à titre d'exemple, en se basant sur un produit générique fictif composé d'un jouet interactif servant également de *babyphone*, d'une application mobile et d'un service en ligne, dont les données personnelles sont stockées chez un hébergeur tiers et qui fait appel à des prestataires (interactivité, analyse des usages, régie publicitaire).

Également, des notes apportent des conseils ou soulignent des points de vigilance liés au contexte particulier des objets connectés.

Enfin, des encarts [zones beiges] apportent un accompagnement méthodologique au fil du document et permettent de renseigner les évaluations prévues.

[1] Voir les lignes directrices du G29 sur les PIA (en anglais).

1 Étude du contexte

Généralement réalisée par la maîtrise d'ouvrage[2], avec l'aide d'une personne en charge des aspects « Informatique et libertés »[3].

Objectif : obtenir une vision claire des traitements de données personnelles considérés.

1.1 Vue d'ensemble du traitement

- Présenter **le produit** considéré, sa **nature**, sa **portée**, son **contexte**, ses **finalités** et ses **enjeux**[4] de manière synthétique.
- Identifier le **responsable du traitement** et les éventuels **sous-traitants**.
- Recenser les **référentiels applicables** au traitement, utiles ou à respecter[5], notamment les codes de conduite approuvés (cf. art. 40 du [RGPD]) et certifications en matière de protection des données (cf. art. 42 du [RGPD])[6].

1.1.1 Description du produit

Le modèle de tableau ci-dessous peut être utilisé pour décrire le produit de manière synthétique.

Pour illustrer son utilisation, il est renseigné à partir d'un exemple de jouet fictif, qui servira tout au long du document.

Description du produit	L'appareil est un jouet disposant d'un micro, d'une caméra et de boutons pour des fonctions basiques (*power*, *action*, *reset*). Il se connecte en Wifi et communique avec une application mobile dédiée, hébergée sur un *smartphone* ou une tablette, et avec un service en ligne.
Finalités du traitement	Fournir une interactivité à l'enfant, à travers la possibilité de dialogue avec le jouet (questions/réponses en langage naturel par reconnaissance vocale). Permettre à l'enfant de communiquer en ligne (envoi de messages vocaux, de textes et de photos) avec ses amis et/ou ses parents. Remonter des informations aux parents (dispositif de surveillance).
Enjeux du traitement	Créer une nouvelle classe de jouets destinés aux enfants et à leurs parents, en tirant partie de la connectivité, tout en respectant le cadre légal et la sécurité des données personnelles.
Responsable du traitement	Société *Fab* (fabricant)
Sous-traitant(s)	Société *Héb* (hébergeur), Société *Int* (moteur d'interactivité), Société *AnaPub* (analyse d'usages et régie publicitaire)

[2] Il s'agit des métiers. Elle peut être déléguée, représentée ou sous-traitée.
[3] Correspondant Informatique et libertés, délégué à la protection des données, ou autre.
[4] Répondre à la question « Quels sont les bénéfices attendus (pour l'organisme, pour les personnes concernées, pour la société en général, *etc.*) ? ».
[5] Selon les cas, ils serviront notamment à démontrer le respect de principes fondamentaux, à justifier des mesures ou à prouver qu'elles correspondent à l'état de l'art.
[6] Autres exemples : politique de sécurité, normes juridiques sectorielles, etc.

1.1.2 Référentiels sectoriels applicables au traitement[7]

Vous trouverez ci-dessous un tableau permettant de détailler les référentiels sectoriels applicables à votre traitement[8] ainsi que les modalités de leur prise en compte.

Référentiels applicables au traitement	Prise en compte

1.2 Données, processus et supports

- Délimiter et décrire le périmètre de manière détaillée :
  - les **données** personnelles concernées, leurs **destinataires**[9] et **durées de conservation** ;
  - une description des **processus** et des **supports** de données pour l'ensemble du cycle de vie des données (depuis leur collecte jusqu'à leur effacement).

1.2.1 Données traitées

Vous trouverez ci-dessous un tableau permettant de lister de manière détaillée les données traitées et les personnes qui y accèdent.

Pour illustrer son utilisation, il est renseigné avec les données de notre exemple de jouet fictif.

Données à caractère personnel	Catégories	Destinataires	Personnes pouvant y accéder
Informations sur l'utilisateur : prénom, date de naissance, genre, adresse électronique, numéro de téléphone	Données courantes : données d'identification	Société *Héb*	Personnels habilités des Sociétés *Fab* et *Héb*
Données renseignées dans une application tierce (Twitter, Facebook, *etc.*), obtenues par lien avec le compte utilisateur	Données courantes : données d'identification	Société *Héb*	Personnels habilités des Sociétés *Fab* et *Héb*
Données relevées : textes/messages, sons, images, mouvements, température, humidité Journaux d'usage de l'appareil, de l'application mobile et du service en ligne	Données courantes : habitudes de vie Données perçues comme sensibles : image et voix (permettant des traitements biométriques) Données sensibles (au sens du GDPR) : données liées à des mineurs	Société Héb + Sociétés *Int* et *AnaPub*	Personnels habilités des Sociétés *Fab* et *Héb* + Personnels habilités des Sociétés *Int* et *AnaPub*

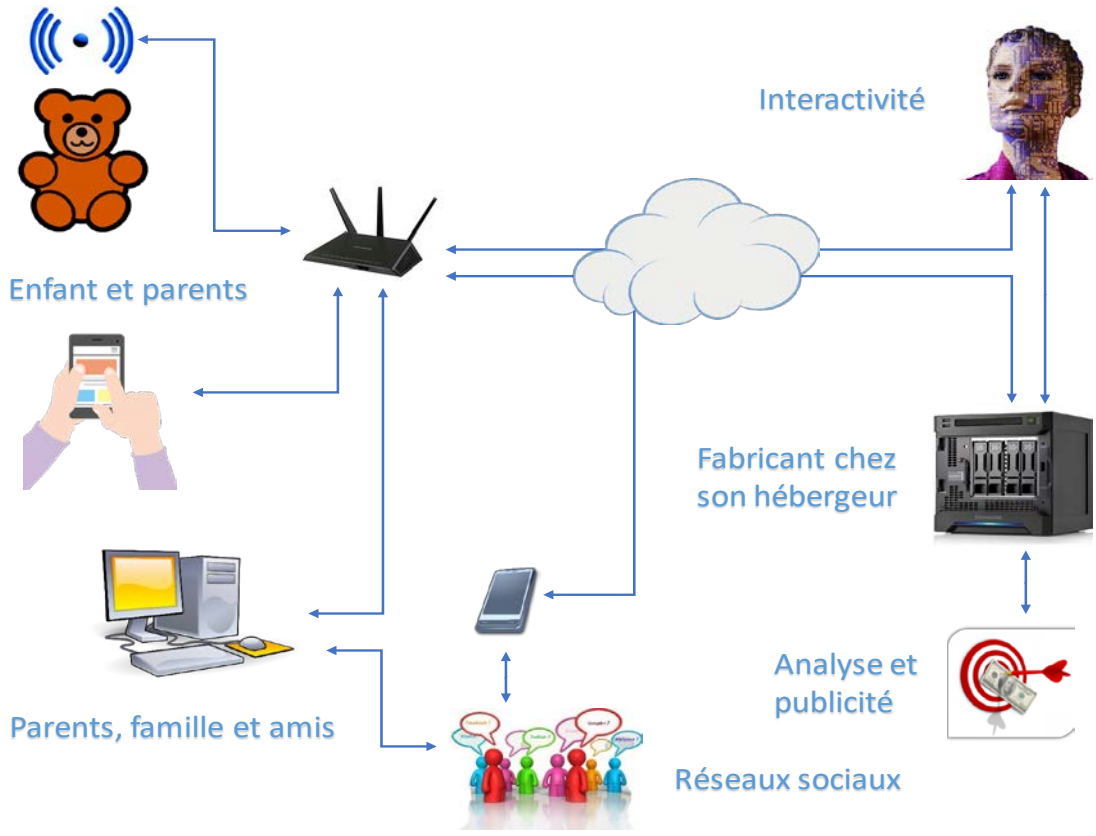
[7] Voir article 35 (8) du [RGPD].
[8] Par ex., un code de conduite, une certification, une politique générale de sécurité, un *PIA Framework*, etc.
[9] Définition de « destinataire » - voir article 4(9) du RGPD.

Données à caractère personnel	Catégories	Destinataires	Personnes pouvant y accéder
Données calculées : réponses aux questions des enfants et identification des centres d'intérêts pour aider à la pertinence des réponses Analyse des usages et publicités ciblées	Données courantes : habitudes de vie Données sensibles (au sens du RGPD) : données liées à des mineurs	Sociétés *Int* et *AnaPub* + Société *Héb*	Personnels habilités des Sociétés *Int* et *AnaPub* + Personnels habilités des Sociétés *Fab* et *Héb*

1.2.2 Cycle de vie des données et processus

Vous devez ici représenter et décrire le fonctionnement général du produit, avec un schéma des flux de données et la description détaillée des processus mis en œuvre.

À titre d'exemple, vous trouverez ci-dessous le schéma de fonctionnement de notre jouet fictif.



Vous trouverez ci-dessous un tableau permettant de lister de manière détaillée les processus de traitement de données mis en œuvre.

Pour illustrer son utilisation, il est renseigné avec notre exemple de jouet fictif.

Processus	Description détaillée du processus
1. Enregistrer un compte	L'utilisateur fournit des données d'identification à l'ouverture de son compte
2. Capter les données	Des données sont relevées via des capteurs
3. Transférer vers le mobile	Les données sont transférées vers l'application mobile, directement par l'appareil ou à travers les serveurs *cloud*
4. Saisir des données	Des données sont saisies dans l'application mobile
5. Stocker dans le mobile	Les données sont stockées dans l'application mobile
6. Envoyer les données aux serveurs	Les données sont envoyées aux serveurs *cloud*, par l'appareil directement ou par l'application mobile
7. Générer l'interactivité	Le moteur d'interactivité dans le *cloud* génère les données de réponse, en se basant sur les dialogues précédents et la détection des centres d'intérêt
8. Envoyer des données au jouet	Les données d'interactivité sont renvoyées à l'appareil, directement ou à travers l'application mobile
9. Conserver les données sur les serveurs	Les données captées et calculées sont stockées sur les serveurs *cloud*
10. Analyser les données	Des algorithmes d'analyse des données sont exécutés sur les serveurs *cloud* pour produire des statistiques d'usage ainsi qu'un ciblage publicitaire
11. Consulter les données des serveurs *cloud*	Une partie des données captées et calculées peuvent être consultées via l'application mobile ou sur un espace Internet personnel
12. Partager des données	Certaines données peuvent être relayées vers des applications tierces ou postées sur des réseaux sociaux

1.2.3 Supports des données

Vous trouverez ci-dessous un tableau permettant de lister de manière détaillée les supports des données. Pour illustrer son utilisation, il est renseigné avec notre exemple de jouet fictif.

Systèmes informatiques[10] sur lesquels reposent les données	Autres supports[11]
- Appareil (caméra, micro, haut-parleur, capteurs de mouvement, température, humidité) - *Smartphone/tablette/ordinateur* de l'utilisateur - Application mobile/navigateur - Réseau Wifi - Internet - Serveurs *cloud* de *Héb*, *Int et AnaPub*	- Utilisateur - Locaux de l'utilisateur - Locaux de *Fab* et *Héb* - Personnels de *Fab* et *Héb* - Locaux de *Int* et *AnaPub* - Personnels de *Int* et *AnaPub*

Attention : toute la partie 1 « Contexte » devra être relue par le CIL ou le DPD afin de s'assurer qu'elle est exhaustive et reflète bien la réalité du terrain.

Cette relecture est d'autant plus nécessaire que cette partie décrit des éléments structurants pour les chapitres suivants.

[10] Décomposables en matériels (et supports de données électroniques), logiciels et canaux informatiques.
[11] Décomposables en personnes, supports papier et canaux de transmission papier.

2 Étude des principes fondamentaux

Généralement réalisée par la maîtrise d'ouvrage, puis évaluée par une personne en charge des aspects « Informatique et libertés ».

Objectif : bâtir le dispositif de conformité aux principes de protection de la vie privée.

Les principes fondamentaux de la protection de la vie privée qui doivent être pris en compte sont les suivants : finalité(s) de collecte des données déterminées et explicites, licéité du traitement, minimisation des données, qualité des données, durées de conservation limitées, information des personnes, recueil de leur consentement, possibilité d'accès direct à leurs données, portabilité de leurs données, possibilité de rectification et de suppression de leurs données sur demande, possibilité de s'opposer au traitement ou de le limiter, encadrement de la sous-traitance et des transfert de données en dehors de l'Union européenne.

- Expliciter et justifier les **choix effectués** et décrire les **mesures retenues** (existantes ou prévues) **pour respecter ces exigences légales** (nécessitant d'expliquer comment il est prévu de les mettre en œuvre).
- Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer la manière dont chaque point est prévu, explicité et justifié, conformément au [RGPD].
- Le cas échéant, revoir leur description ou proposer des mesures complémentaires.

Note : Vous trouverez au §2.3 un tableau pour récapituler la justification de l'ensemble de ces points et y consigner leur évaluation et les éventuelles mesures correctives.

2.1 Mesures garantissant la proportionnalité et la nécessité du traitement

2.1.1 Finalités : déterminées, explicites et légitimes[12]

Vous trouverez ci-dessous un tableau permettant de détailler les finalités de traitement des données et justifier leur légitimité[13].

Finalités	Légitimité

Note : penser à expliciter les finalités de partage avec des tiers, notamment pour la publicité et les « offres partenaires », ainsi que les finalités de traitement de données pour l'amélioration du service.

Note : penser à expliciter les modalités particulières du traitement, en précisant notamment les croisements de données s'il y a lieu.

[12] Voir article 5.1 (b) du [RGPD].

[13] Sur la légitimité de la finalité, voir l'avis WP 203 du G29 - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Attention[14] : en raison de la vulnérabilité générale d'un enfant et compte tenu du fait que les données à caractère personnel doivent être traitées de manière loyale et licite, les responsables d'un traitement ciblant les enfants devraient respecter de façon encore plus stricte les principes de limitation de la finalité.

Plus particulièrement, les responsables du traitement ne devraient pas utiliser les données de l'enfant à des fins de profilage (par ex. pour de la publicité ciblée), que ce soit directement ou indirectement, dans la mesure où une telle pratique n'entre pas dans la sphère de compréhension d'un enfant et dépasse dès lors les limites d'un traitement loyal.

2.1.2 Fondement : licéité du traitement, interdiction du détournement de finalité[15]

Vous trouverez ci-dessous la liste des critères de licéité. Un traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

Critères de licéité	Applicable	Justification
La personne concernée a consenti[16] 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		
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 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[17]		

Note : dans le cas d'une obligation légale ou d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, préciser dans la justification le fondement légal du traitement dans le droit de l'Union européenne ou de l'État membre auquel le responsable du traitement est soumis.

Note : il peut y avoir plusieurs fondements pour un traitement : par exemple, un contrat lié à l'achat du produit pour son utilisation dans sa finalité principale et un consentement pour ses finalités secondaires (amélioration du service, marketing, *etc.*) qui sera recueilli lors de l'activation du produit.

[14] Voir l'avis 02/2013 du G29 sur les applications destinées aux dispositifs intelligents.
[15] Voir article 6 du [RGPD].
[16] Concernant le recueil du consentement de la personne et son information, voir le chapitre 2.2.
[17] Ce point ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions

Attention : si les données sont traitées à une fin autre que celle pour laquelle elles ont été collectées et que le traitement n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union européenne ou d'un État membre, il est nécessaire de déterminer si cette autre fin est compatible avec la finalité initiale de collecte, en tenant compte, entre autres :

- de l'existence éventuelle d'un lien entre la finalité du traitement et la finalité initiale de collecte des données ;
- du contexte de collecte initiale, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;
- de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données ou des données relatives à des condamnations pénales et à des infractions[18] ;
- des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;
- de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

2.1.3 Minimisation des données : adéquates, pertinentes et limitées[19]

Il est important de réduire la gravité des risques en minimisant le nombre de données à caractère personnel qui seront traitées, en se limitant au strict nécessaire au regard de la finalité définie (ne pas les collecter sinon). Ensuite, il est également possible de minimiser les données elles-mêmes, par des mesures destinées à réduire leur sensibilité (cf. annexe 1 - Liste de mesures de minimisation des données).

Vous trouverez ci-dessous un tableau permettant de lister les données traitées, réduites au strict nécessaire, accompagnées de la justification du besoin et des éventuelles mesures de minimisation complémentaires.

Pour illustrer son utilisation, il est renseigné avec les données tirées de notre exemple de jouet fictif.

Types de données	Catégories de données	Détail des données traitées	Justification du besoin et de la pertinence des données	Mesures de minimisation
Données courantes	État-civil, identité, données d'identification	Prénom, date de naissance, genre, adresse électronique, numéro de téléphone, lien avec un compte de réseau social	Éléments nécessaires à la création d'un profil permettant de communiquer	Pas de nom de famille Remplacement de la date de naissance par l'âge ou une tranche d'âge Stockage séparé des données identifiantes, dans une base chiffrée
	Vie personnelle (habitudes de vie, situation familiale, hors données sensibles ou dangereuses, *etc.*)	Textes/messages, sons, images, mouvements, température, humidité Réponses aux questions des enfants, identification des centres d'intérêts pour aider à la pertinence des réponses, publicités ciblées	Éléments faisant partie des fonctions de communication	

[18] Voir articles 9 et 10 du [RGPD].
[19] Voir article 5.1 (c) du [RGPD].

Types de données	Catégories de données	Détail des données traitées	Justification du besoin et de la pertinence des données	Mesures de minimisation
	Vie professionnelle (CV, scolarité formation professionnelle, distinctions, *etc.*)	Non collectées		
	Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, *etc.*)	Non collectées		
	Données de connexion (adresses IP, journaux d'événements, *etc.*)	Traces applicatives Logs techniques	Besoins de sécurité et de vérifier le respect des CGU	Pseudonymisation pour l'exploitation statistique
	Données de localisation (déplacements, données GPS, GSM, *etc.*)	Localisation du *smartphone* intégrée dans les photos (si l'option est activée)	Inutile	Retrait des informations de localisation avant envoi des photos
Données perçues comme sensibles	Numéro de sécurité sociale (NIR)	Non collecté		
	Données biométriques	Données brutes : voix et photographies	Éléments faisant partie des fonctions de communication	
	Données bancaires	Non collectées		
Données sensibles [20]	Opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, données de santé, origine raciales ou ethniques, relatives à la santé ou à la vie sexuelle	Non collecté mais peuvent apparaître directement ou indirectement dans les données textes, audios et vidéos	Éléments faisant partie des fonctions de communication	
	Infractions, condamnations, mesures de sécurité	Non collecté		

Notes : penser à bien justifier la collecte de certaines données (localisation, date de naissance, âge, poids, *etc.*) et à bien faire la distinction entre les données anonymes et pseudonymes.

[20] Voir notamment les articles 9 et 10 du [RGPD]. Des restrictions d'usage et des formalités particulières sont à prendre en compte.

Conseil : éviter les champs de saisie en texte libre (ex : zones « commentaires »), en raison du risque que les utilisateurs y consignent des informations ne respectant pas les principes de minimisation. On préférera donc des champs de saisie à base de listes déroulantes. Si on ne peut éviter la saisie de texte libre, une sensibilisation des utilisateurs devra être faite quant à l'usage de ces champs, vis-à-vis des conditions générales du service et vis-à-vis de la loi (pas de propos injurieux, pas de données sensibles non déclarées, *etc.*).

Attention : pour un traitement concernant des personnes mineures, les données sont globalement considérées comme sensibles selon le [RGPD].

Attention[21] : en raison de la vulnérabilité générale d'un enfant et compte tenu du fait que les données à caractère personnel doivent être traitées de manière loyale et licite, les responsables d'un traitement ciblant les enfants devraient respecter de façon encore plus stricte les principes de minimisation des données et de limitation de la finalité.

Les responsables du traitement devraient s'abstenir plus spécifiquement de collecter des données relatives aux parents ou aux membres de la famille de l'enfant, telles que des informations financières ou des catégories particulières d'information comme des données médicales.

2.1.4 Qualité des données : exactes et tenues à jour[22]

Vous trouverez ci-dessous un tableau permettant de détailler les mesures de respect de la qualité des données, mises en œuvre sur l'appareil, l'application mobile et l'espace personnel, ainsi qu'une justification sur les modalités ou l'impossibilité de mise en œuvre.

Mesures pour la qualité des données	Appareil	Application mobile	Espace personnel	Justification
Vérification régulière de l'exactitude des données personnelles de l'utilisateur				
Invitation de l'utilisateur à contrôler et, si nécessaire, mettre à jour ses données				
Traçabilité des modifications des données				

2.1.5 Durées de conservation : limitées[23]

Une durée de conservation doit être définie pour chaque type de données et justifiée par les besoins du traitement et/ou des contraintes légales. On distingue ainsi les données courantes et les données archivées dont l'accès sera restreint aux seuls acteurs concernées.

Un mécanisme de suppression doit être implémenté pour archiver les données courantes ou purger les données archivées à la fin de leur période de conservation. Les traces fonctionnelles devront également être purgées, tout comme les logs techniques qui ne pourront pas être conservés indéfiniment.

Notes : En réduisant la quantité de données traitées et disponibles, l'archivage et la purge permettent de limiter les impacts en cas de vol ou de diffusion accidentelle de la base de données.

Afin de s'assurer de l'effectivité de ces durées de conservation, il est conseillé de mettre en place un mécanisme automatique basé sur la date de création des données ou de leur dernier usage.

[21] Voir l'avis 02/2013 du G29 sur les applications destinées aux dispositifs intelligents.
[22] *Voir article 5.1 (d) du* [RGPD]. *L'exigence de qualité porte également sur le lien entre les données qui identifient les personnes et les données qui les concernent.*
[23] Voir article 5.1 (e) du [RGPD], à défaut d'une autre obligation légale imposant une conservation plus longue.

Attention : Pour les données sensibles, pour les données à risques élevé, il conviendra d'utiliser des outils d'effacement sécurisés rendant les données irrécupérables.

Les durées de conservation, leur justification et les mécanismes de purge peuvent être présentés dans le tableau ci-dessous.

Types de données	Durée de conservation	Justification de la durée de conservation	Mécanisme de suppression à la fin de la conservation
Données courantes			
Données archivées			
Traces fonctionnelles			
Journaux techniques (*logs*)			

2.2 Mesures protectrices des droits des personnes des personnes concernées

2.2.1 Information des personnes concernées (traitement loyal et transparent)[24]

Si le traitement bénéficie d'une exemption au droit d'information, prévue par les articles 12, 13 et 14 du [RGPD], vous le justifierez ci-dessous.

Dispense d'information des personnes concernées	Justification

Dans le cas contraire, vous trouverez ci-dessous une liste de mesures destinées à assurer l'information des utilisateurs (ou de leurs parents)[25].

Vous y détaillerez leur mise en œuvre (de préférence en joignant des copies d'écrans et extraits de documents) sur l'appareil, l'application mobile et l'espace personnel, ainsi qu'une justification sur les modalités ou sur l'impossibilité de leur mise en œuvre.

Mesures pour le droit à l'information	Appareil	Application mobile	Espace personnel	Justification
Présentation, lors de l'initialisation du dispositif, des conditions d'utilisation/confidentialité				
Possibilité d'accéder aux conditions d'utilisation/confidentialité après l'initialisation				
Conditions lisibles et compréhensibles				
Existence de clauses spécifiques au dispositif				
Présentation détaillée des finalités des traitements de données (objectifs précis, croisements de données s'il y a lieu, *etc.*)				

[24] Voir articles 12, 13 et 14 du [RGPD].
[25] Voir sur le site de la CNIL : « Editeurs de sites pour enfants : n'oubliez pas vos obligations ! ».

Mesures pour le droit à l'information	Appareil	Application mobile	Espace personnel	Justification
Présentation détaillée des données personnelles collectées				
Présentation des éventuels accès à des identifiants de l'appareil, du *smartphone*/tablette ou de l'ordinateur, en précisant si ces identifiants sont communiqués à des tiers				
Présentation des droits de l'utilisateur (retrait du consentement, suppression de données, *etc.*)				
Information de l'utilisateur si l'application est susceptible de fonctionner en arrière-plan				
Information sur le mode de stockage sécurisé des données, notamment en cas d'externalisation				
Information sur les protections d'accès à l'appareil				
Modalités de contact de l'entreprise (identité et coordonnées) pour les questions de confidentialité				
Information sur la possibilité de définir des directives relatives au sort des données post-mortem				
Le cas échéant, information de l'utilisateur de tout changement concernant 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				
- présentation détaillée des données personnelles transmises				
- indication de l'identité des organismes tiers				

Attention : dans le cas de transmission de données à des organismes tiers au responsable du traitement (filiales, affiliés, intragroupe, partenaires, *etc.*), il est nécessaire de fournir la liste des destinataires (dans une rubrique d'information dédiée), en précisant les catégories de données transmises et la finalité du transfert, et en fournissant un lien hypertexte vers la politique de protection des données des destinataires respectifs. Il faut également prévoir un processus interne permettant de mettre à jour cette liste en cas de modification.

Attention[26] : les développeurs d'applications, en collaboration avec les magasins d'applications et les fabricants de systèmes d'exploitation et de dispositifs, devraient présenter les informations utiles de manière simple, dans un langage adapté à un jeune âge, éventuellement par un message sonore.

[26] Voir l'avis 02/2013 du G29 sur les applications destinées aux dispositifs intelligents.

Recommandation : placer un « *QR Code* » d'information sur l'objet et responsabiliser les utilisateurs (ou leurs parents) pour qu'ils informent les tiers que leurs données sont susceptibles d'être collectées (par ex. les autres enfants conversant avec l'appareil ou présents sur les photos partagées).

2.2.2 Recueil du consentement, le cas échéant : exprès

Si le traitement est fondé sur le consentement de la personne, le responsable de traitement doit être en mesure de démontrer qu'il a bien recueilli ce consentement. La personne concernée doit avoir la possibilité de retirer son accord à tout moment et de façon simple[27].

Si la licéité du traitement[28] repose sur le consentement, vous trouverez ci-dessous une liste de mesures destinées à assurer le recueil du consentement des utilisateurs (ou de leurs parents)[29], le rappel et la réaffirmation de leur consentement, ainsi que le maintien des paramètres liés à celui-ci.

Vous y détaillerez leur mise en œuvre sur l'appareil, l'application mobile et l'espace personnel, ainsi qu'une justification sur les modalités ou l'impossibilité de mise en œuvre.

Mesures pour le recueil du consentement	Appareil	Application mobile	Espace personnel	Justification
Consentement exprès lors de l'initialisation				
Consentement segmenté par catégorie de données ou types de traitement				
Consentement exprès avant le partage de données avec d'autres utilisateurs				
Consentement présenté de manière simple, compréhensible et adaptée à l'utilisateur cible (notamment pour les enfants)				
Recueil du consentement des parents pour les mineurs de moins de 13 ans				
Pour un nouvel utilisateur, mise en œuvre d'un nouveau recueil de consentement				
Après une longue période sans utilisation, demande à l'utilisateur de réaffirmer son consentement				
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)				
Si l'utilisateur change d'appareil, de *smartphone* ou d'ordinateur, s'il réinstalle l'application mobile ou efface ses *cookies*, les paramètres liés à son consentement sont maintenus				

Attention[30] : le RGPD a renforcé les bases légales concernant le consentement pour toute offre directe de services de la société de l'information à destination des mineurs, et la charge de la preuve (non ambigüe) incombe au responsable de traitement ou au sous-traitant.

[27] Voir articles 7 et 8 du [RGPD].
[28] Concernant la licéité du traitement, voir le chapitre 2.1.
[29] Voir sur le site de la CNIL : « Editeurs de sites pour enfants : n'oubliez pas vos obligations ! ».
[30] Voir article 8 du [RGPD].

En pratique, le consentement du responsable parental est requis pour les enfants de moins de 16 ans, avec la possibilité pour les États membres de fixer un âge inférieur, mais qui ne peut être en deçà de 13 ans. Le responsable du traitement s'efforce raisonnablement de vérifier que le consentement est bien donné par le responsable parental, compte tenu des moyens technologiques disponibles.

Attention[31] : Lorsque le consentement d'un mineur peut être légalement obtenu et que l'application est destinée à l'utilisation par un enfant ou un mineur, le responsable du traitement doit être attentif au fait que le mineur peut avoir une compréhension limitée du traitement des données et qu'il n'accorde que peu d'attention aux informations sur le sujet.

Les développeurs d'applications, en collaboration avec les magasins d'applications et les fabricants de systèmes d'exploitation et de dispositifs, devraient présenter les informations utiles de manière simple, dans un langage adapté à un jeune âge.

2.2.3 Exercice des droits d'accès[32] et à la portabilité[33]

Si le traitement bénéficie d'une exemption au droit d'accès, prévue par l'article 15 du [RGPD], vous le justifierez ci-dessous.

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

Dans le cas contraire, vous trouverez ci-dessous une liste de mesures destinées à assurer le droit d'accès des utilisateurs (ou de leurs parents) à l'ensemble des données à caractère personnel les concernant.

Vous y détaillerez leur mise en œuvre sur l'appareil, l'application mobile et l'espace personnel, ainsi qu'une justification sur les modalités ou l'impossibilité de mise en œuvre.

Mesures pour le droit d'accès	Appareil	Application mobile	Espace personnel	Justification
Possibilité d'accéder à l'ensemble des données personnelles de l'utilisateur, via les interfaces courantes				
Possibilité de consulter, de manière sécurisée, les traces d'utilisation liées à l'utilisateur				
Possibilité de télécharger une archive de l'ensemble des données à caractère personnel liées à l'utilisateur				

Enfin, si le droit à la portabilité s'applique au traitement conformément à l'article 20 du [RGPD], vous en détaillerez la mise en œuvre ci-dessous.

[31] Voir l'avis 02/2013 du G29 sur les applications destinées aux dispositifs intelligents.
[32] Voir article 15 du [RGPD].
[33] Voir article 48 de la Loi 2016-1321 du 7 octobre 2016 pour une République numérique et article 20 du [RGPD].

Mesures pour le droit à la portabilité	Appareil	Application mobile	Espace personnel	Justification
Possibilité de récupérer, sous une forme aisément réutilisable, les données personnelles qui ont été fournies par l'utilisateur, afin de pouvoir les transférer à un service tiers				

2.2.4 Exercice des droits de rectification et d'effacement[34]

Si le traitement bénéficie d'une exemption au droit de rectification et d'effacement, prévue par l'article 17 du [RGPD] vous le justifierez ci-dessous.

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

Dans le cas contraire, vous trouverez ci-dessous une liste de mesures destinées à assurer le droit à la rectification ou l'effacement des données des utilisateurs (ou de leurs parents[35]) qui le souhaitent.

Vous y détaillerez leur mise en œuvre sur l'appareil, l'application mobile et l'espace personnel, ainsi qu'une justification sur les modalités ou l'impossibilité de mise en œuvre.

Mesures pour les droits de rectification et d'effacement	Appareil	Application mobile	Espace personnel	Justification
Possibilité de rectifier les données personnelles				
Possibilité de supprimer les données personnelles				
Indication des données personnelles qui seront conservées malgré tout (contraintes techniques, obligations légales, *etc.*)				
Mise en œuvre du droit à l'oubli pour les mineurs				
Indications claires et étapes simples pour effacer les données avant de mettre l'appareil au rebut				
Conseils fournis pour remise à zéro en cas de vente de l'appareil				
Possibilité d'effacer les données en cas de vol de l'appareil				

Attention[36] : Le responsable de traitement dispose d'un délai d'un mois pour effacer les données ou répondre à la personne ; passé ce délai, la personne concernée peut saisir la CNIL. Des exceptions

[34] Voir articles 16, 17 et 19 du [RGPD].
[35] Voir sur le site de la CNIL : « Editeurs de sites pour enfants : n'oubliez pas vos obligations ! ».
[36] Voir la Loi 2016-1321 du 7 octobre 2016 pour une République numérique modifiant l'article 40 de la [Loi-I&L], qui complète le « droit à l'oubli » prévu par l'article 17 du [RGPD].

existent, notamment dans le cas où les informations publiées sont nécessaires à liberté d'information, pour des motifs d'intérêt public ou pour respecter une obligation légale.

Un internaute âgé de moins de 18 ans au moment de la publication ou de la création d'un compte en ligne peut directement et sans autre motif demander au site l'effacement, dans les meilleurs délais, des données le concernant.

2.2.5 Exercice des droits de limitation du traitement et d'opposition[37]

Si le traitement bénéficie d'une exemption au droit de limitation et d'opposition, prévue par l'article 21 du [RGPD], vous le justifierez ci-dessous.

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

Dans le cas contraire, vous trouverez ci-dessous une liste de mesures destinées à assurer le droit d'opposition et de limitation soit sur les différentes finalités soit sur l'ensemble d'un traitement.

Vous y détaillerez leur mise en œuvre sur l'appareil, l'application mobile et l'espace personnel, ainsi qu'une justification sur les modalités ou l'impossibilité de mise en œuvre.

Mesures pour les droits de limitation et d'opposition	Appareil	Application mobile	Espace personnel	Justification
Existence de paramètres « Vie privée »				
Invitation à changer les paramètres par défaut				
Paramètres « Vie privée » accessibles pendant l'initialisation du dispositif				
Paramètres « Vie privée » accessibles après l'initialisation du dispositif				
Existence d'un dispositif de contrôle parental pour les enfants de moins de 13 ans				
Existence d'un dispositif permettant à l'utilisateur de demander la limitation du traitement				
Existence de moyens techniques permettant au RT de verrouiller l'accès et l'utilisation des données objet de la limitation				
Possibilité de désactiver certaines fonctions de l'appareil (micro, navigateur web, *etc.*)				
Existence d'applications alternatives pour accéder à l'appareil				
Possibilité de s'opposer au fonctionnement de l'application mobile en arrière-plan				

[37] Voir articles 18 et 21 du [RGPD].

Mesures pour les droits de limitation et d'opposition	Appareil	Application mobile	Espace personnel	Justification
Conformité en matière de traçage (*cookies*, publicité, *etc.*)				
Exclusion des enfants de moins de 13 ans des traitements de profilage automatisé				
Exclusion effective de traitement des données de l'utilisateur en cas de retrait du consentement				

Note : le droit à la limitation permet à la personne concernée d'exiger le « gel » du traitement de ses données, comme mesure conservatoire le temps d'en vérifier la légitimité, par exemple.

2.2.6 Sous-traitance : identifiée et contractualisée[38]

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 dans les meilleurs délais de toute violation de données, *etc.*

Vous trouverez ci-dessous un tableau permettant de détailler les contrats pour chacun des sous-traitants.

Nom du sous-traitant	Finalité	Périmètre	Référence du contrat	Conformité art.28

2.2.7 Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne[39]

Vous trouverez ci-dessous un tableau permettant de détailler le lieu géographique de stockage des données de l'appareil, de l'application mobile et de l'espace personnel dans le *cloud*.

En fonction du pays concerné, vous devrez justifier le choix d'un hébergement éloigné et indiquer les modalités d'encadrement juridique mises en œuvre afin d'assurer une protection adéquate aux données faisant l'objet d'un transfert transfrontalier.

Lieu de stockage des données	France	Union européenne	Pays reconnu adéquat par l'UE	Autre pays	Justification et encadrement (clauses contractuelles types, règles internes d'entreprise)
Données de l'appareil					

[38] Voir article 28 du [RGPD].
[39] Voir articles 44 à 50 du [RGPD].

Lieu de stockage des données	France	Union européenne	Pays reconnu adéquat par l'UE	Autre pays	Justification et encadrement (clauses contractuelles types, règles internes d'entreprise)
Données de l'application mobile					
Données de l'espace personnel					

2.3 Évaluation du respect des principes fondamentaux

Vous trouverez ci-dessous un tableau permettant, pour chacun des points de respect des exigences légales, de résumer la manière dont il est appliqué dans le traitement.

Les deux dernières colonnes sont destinées à l'évaluateur :

→ Acceptable / améliorable ?

L'évaluateur devra estimer si les mesures permettent de respecter les principes fondamentaux.

→ Mesures correctives :

Le cas échéant, il indiquera les mesures complémentaires qui seraient nécessaires.

Mesures garantissant la proportionnalité et la nécessité du traitement	Justification	Acceptable / améliorable ?	Mesures correctives
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 concernées	**Justification**	**Acceptable / améliorable ?**	**Mesures correctives**
Information des personnes concernées (traitement loyal et transparent)			
Recueil du consentement			
Exercice du droit d'accès et droit 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			

3 Étude des risques liés à la sécurité des données[40]

Un risque est un scénario hypothétique qui décrit un événement redouté et toutes les menaces qui permettraient qu'il survienne. Plus précisément, il décrit :

- comment des sources de risques (ex. : un salarié soudoyé par un concurrent)
- pourraient exploiter les vulnérabilités des supports de données (ex. : le système de gestion des fichiers, qui permet de manipuler les données)
- dans le cadre de menaces (ex. : détournement par envoi de courriers électroniques)
- et permettre à des événements redoutés de survenir (ex. : accès illégitime à des données)
- sur les données à caractère personnel (ex. : fichier des clients)
- et ainsi provoquer des impacts sur la vie privée des personnes concernées (ex. : sollicitations non désirées, sentiment d'atteinte à la vie privée, ennuis personnels ou professionnels).

3.1 Évaluation des mesures existantes ou prévues

Généralement réalisé par la maîtrise d'œuvre[41], puis évaluée par une personne en charge de la sécurité de l'information[42] notamment le responsable de la sécurité des systèmes d'information si désigné.

Objectif : obtenir une bonne connaissance des mesures contribuant à la sécurité.

- Identifier ou déterminer les **mesures existantes ou prévues** (déjà engagées), qui peuvent être de trois natures différentes :
  1. **mesures portant spécifiquement sur les données du traitement** : chiffrement, anonymisation, cloisonnement, contrôle d'accès, traçabilité, *etc.* ;
  2. **mesures générales de sécurité du système dans lequel le traitement est mis en œuvre** : sécurité de l'exploitation, sauvegardes, sécurité des matériels, *etc.* ;
  3. **mesures organisationnelles (gouvernance)** : politique, gestion des projets, gestion des personnels, gestion des incidents et violations, relations avec les tiers, *etc.*
- Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer chaque mesure et sa description, conformément aux bonnes pratiques de sécurité.
- Le cas échéant, préciser leur description ou proposer des mesures complémentaires.

Notes : Les catégories de mesures de sécurité ci-dessous correspondent aux bonnes pratiques recommandées par la CNIL[43].

Vous devrez également tenir compte des référentiels sectoriels applicables à votre traitement[44] (politique générale de sécurité, *PIA Framework*, code de conduite, *etc.*).

Note : Vous trouverez au §3.1.4 un tableau pour récapituler la mise en œuvre de l'ensemble de ces mesures et y consigner leur évaluation et les éventuelles mesures correctives.

[40] Voir article 32 du [RGPD].
[41] Elle peut être déléguée, représentée ou sous-traitée.
[42] Responsable de la sécurité des systèmes d'information ou autre.
[43] Voir le Guide sécurité des données personnelles de la CNIL.
[44] Voir article 35 (8) du [RGPD].

3.1.1 Mesures portant spécifiquement sur les données du traitement

Chiffrement

*Décrivez ici les **moyens mis en œuvre pour assurer la confidentialité des données** conservées (en base de données, dans des fichiers plats, les sauvegardes, etc.), ainsi que les modalités de gestion des clés de chiffrement (création, conservation, modification en cas de suspections de compromission, etc.).*

Détaillez les moyens de chiffrement employés pour les flux de données (VPN, TLS, etc.) mis en œuvre dans le traitement.

Notes : penser à la sécurité du Wifi (chiffrement, stockage du mot de passe Wifi).

Penser à la sécurisation des certificats, stockés sur l'appareil ou le *smartphone*, utilisés pour authentifier et chiffrer les connexions.

Anonymisation

Indiquez ici si des mécanismes d'anonymisation sont mis en œuvre, lesquels et à quelle fin.

Note : penser à bien faire la distinction entre les données anonymes et pseudonymes.

Cloisonnement des données (par rapport au reste du système d'information)

Indiquez ici si un cloisonnement du traitement est prévu, et comment il est réalisé.

Contrôle des accès logiques

*Indiquez ici comment les **profils utilisateurs** sont définis et attribués.*

*Précisez les moyens d'**authentification** mis en œuvre[45].*

*Le cas échéant, précisez les règles applicables aux **mots de passe** (longueur minimale, structure obligatoire, durée de validité, nombre de tentatives infructueuses avant blocage du compte, etc.).*

Notes : penser à la sécurité du mot de passe utilisateur, que ce soit sur l'appareil, sur le *smartphone* ou dans le *cloud*. Les mots de passe doivent être stockés sous forme hachée par un algorithme robuste avec application préalable d'un sel.

Penser à la protection de l'accès à l'application sur *smartphone* par mot de passe spécifique.

Penser à sécuriser l'appairage entre l'appareil, l'application mobile et l'espace personnel.

Penser à protéger les données, y compris les métadonnées (dont Exif) et traces techniques, en cas d'accès direct par connexion physique à l'appareil ou au *smartphone*.

[45] Voir la délibération de la CNIL n°2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe.

Traçabilité (journalisation)

*Indiquez ici si des **événements sont journalisés** et la durée de conservation de ces traces.*

Contrôle d'intégrité

Le cas échéant, indiquez ici si des mécanismes de contrôle d'intégrité des données stockées sont mis en œuvre, lesquels et à quelle fin. *Détaillez les mécanismes de contrôle d'intégrité employés sur les flux de données.*

Archivage

Le cas échéant, décrivez ici le processus de gestion des archives (versement, stockage, consultation, etc.) relevant de votre responsabilité. Précisez les rôles en matière d'archivage (service producteur, service versant, etc.) et la politique d'archivage. *Indiquez si les données sont susceptibles de relever des archives publiques.*

Sécurité des documents papier

Si des documents papiers contenant des données sont utilisés dans le cadre du traitement, indiquez ici comment ils sont imprimés, stockés, détruits et échangés.

3.1.2 Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre

Les mesures suivantes relèvent généralement de la sécurité de l'ensemble de l'organisme. Elles peuvent notamment être formalisées dans une politique de sécurité des systèmes d'information (PSSI) ou équivalent.

Sécurité de l'exploitation

*Décrivez ici comment les **mises à jour des logiciels** (systèmes d'exploitation, applications, etc.) et l'application des correctifs de sécurité sont réalisées.*

Note : penser aux possibilités de mettre à jour l'appareil.

Gestion des postes de travail et lutte contre les logiciels malveillants

Détaillez ici les mesures mises en œuvre sur les postes de travail (verrouillage automatique, pare-feu, etc.) et précisez si un antivirus est installé et régulièrement mis à jour sur tous les postes.

Sécurité des sites web

Indiquez ici si les "Recommandations pour la sécurisation des sites web" de l'ANSSI sont mises en œuvre.

Sauvegardes

Indiquez ici comment les sauvegardes sont gérées. Précisez si elles sont stockées dans un endroit sûr.

Maintenance

Décrivez ici comment est gérée la maintenance physique des équipements, et précisez si elle est sous-traitée.

Indiquez si la maintenance à distance des applications est autorisée, et suivant quelles modalités.

Précisez si les matériels défectueux sont gérés spécifiquement.

Sécurité des canaux informatiques (réseaux)

Indiquez ici sur quel type de réseau le traitement est mis en œuvre (isolé, privé, ou Internet).
Précisez quels système de pare-feu, sondes de détection d'intrusion, ou autres dispositifs actifs ou passifs sont chargés d'assurer la sécurité du réseau.

Surveillance

Indiquez ici si une surveillance en temps réel du réseau local est mise en œuvre et avec quels moyens.
Indiquez si un contrôle des configurations matérielles et logicielles est effectué et par quels moyens.

Contrôle d'accès physique

Indiquez ici la manière dont est réalisé le contrôle d'accès physique aux locaux hébergeant le traitement (zonage, accompagnement des visiteurs, port de badge, portes verrouillées, etc.).
Indiquez s'il existe des moyens d'alerte en cas d'effraction.

Sécurité des matériels

*Indiquez ici les mesures de **sécurité physique des serveurs et des postes clients** (stockage sécurisé, câbles de sécurité, filtres de confidentialité, effacement sécurisé avant mise au rebut, etc.).*

Éloignement des sources de risques

*Indiquez ici si la zone d'implantation est sujette à des **sinistres environnementaux** (zone inondable, proximité d'industries chimiques, zone sismique ou volcanique, etc.).*
*Précisez si la zone contient des **produits dangereux**.*

Protection contre les sources de risques non humaines

*Décrivez ici les moyens de prévention, de détection et de lutte contre l'**incendie**.*
*Le cas échéant, indiquez les moyens de prévention de **dégâts des eaux**.*
*Précisez également les moyens de surveillance et de secours de l'**alimentation électrique**.*

3.1.3 Mesures organisationnelles (gouvernance)

Organisation

*Indiquez si les **rôles et responsabilités** en matière de protection des données sont définis.*
Précisez si une personne est chargée de la mise en application des lois et règlements touchant à la protection de la vie privée.
*Précisez s'il existe un **comité de suivi** (ou équivalent) chargé des orientations et du suivi des actions concernant la protection de la vie privée.*

Politique (gestion des règles)

*Indiquez ici s'il existe une **charte informatique** (ou équivalent) traitant de la protection des données et de la bonne utilisation des moyens informatiques.*

Gestion des risques

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.

Gestion des projets

*Indiquez ici si les **tests** des dispositifs sont réalisés sur des données fictives/anonymes.*

Gestion des incidents et des violations de données

*Indiquez ici si les **incidents** informatiques font l'objet d'une gestion documentée et testée.*

Gestion des personnels

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.

Relations avec les tiers

*Indiquez ici, pour les **sous-traitants** amenés à avoir accès aux données, les modalités et les mesures de sécurité mises en œuvre pour ces accès.*

Supervision

Indiquez ici si l'effectivité et l'adéquation des mesures touchant à la vie privée sont contrôlées.

3.1.4 Évaluation des mesures de sécurité

Vous trouverez ci-dessous un tableau permettant, pour chacune des mesures de sécurité recommandées par la CNIL, de résumer la manière dont elle est mise en œuvre ou de justifier pourquoi elle ne l'est pas.

Les deux dernières colonnes sont destinées à l'évaluateur :

→ Acceptable / améliorable ?

L'évaluateur devra estimer si les mesures respectent les bonnes pratiques recommandées par la CNIL.

→ Mesures correctives :

Le cas échéant, il indiquera les mesures complémentaires qui seraient nécessaires.

Mesures portant spécifiquement sur les données du traitement	Mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
Chiffrement			
Anonymisation			
Cloisonnement des données (par rapport au reste du système d'information)			
Contrôle des accès logiques			
Traçabilité (journalisation)			
Contrôle d'intégrité			
Archivage			
Sécurité des documents papier			
Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	**Mise en œuvre ou justification sinon**	**Acceptable / améliorable ?**	**Mesures correctives**
Sécurité de l'exploitation			
Gestion des postes de travail et lutte contre les logiciels malveillants			
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)	Mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
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			

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

Généralement réalisée par la maîtrise d'ouvrage, puis évaluée par une personne en charge de la sécurité de l'information.

Objectif : obtenir une bonne compréhension des causes et conséquences des risques.

- Pour chaque événement redouté (un accès illégitime à des données[46], une modification non désirée de données[47], et une disparition de données[48]) :
  - déterminer les **impacts** potentiels[49] sur la vie privée des personnes concernées s'ils survenaient[50] ;
  - estimer sa **gravité**, notamment en fonction du caractère préjudiciable des impacts potentiels et, le cas échéant, des mesures susceptibles de les modifier ;
  - Identifier les **menaces**[51] sur les supports des données qui pourraient mener à cet événement redouté[52] et les **sources de risques**[53] qui pourraient en être à l'origine ;
  - estimer sa **vraisemblance**, notamment en fonction des vulnérabilités des supports de données, des capacités des sources de risques à les exploiter et des mesures susceptibles de les modifier ;
- Déterminer si les risques ainsi identifiés[54] peuvent être jugé acceptables compte tenu des mesures existantes ou prévues (déjà engagées).
- Dans la négative, proposer des mesures complémentaires et réévaluer le niveau de chacun des risques en tenant compte de celles-ci, afin de déterminer les risques résiduels[55].

Attention : les mesures existantes ou prévues (déjà engagées) étant prises en compte dans l'appréciation des risques, il est nécessaire, avant d'aborder la présente partie 3.2, que les mesures identifiées au §2 (juridiques) et au §3.1 (sécurité) aient été évaluées afin de s'assurer que leur liste est complète et conforme à la réalité du terrain.

Attention : les éventuelles mesures correctives proposées par l'évaluateur au §2.3 et au §3.1.4 devront, quant à elles, être prises en compte lors du calcul des risques résiduels au §3.2.1, au §3.2.2 et au §3.2.3, en même temps que les mesures correctives spécifiques à chacun des risques.

L'ensemble des mesures correctives sera repris dans le plan d'action au §4.1.

[46] Elles sont connues de personnes non autorisées (atteinte à la confidentialité des données).
[47] Elles ne sont plus intègres ou sont changées (atteinte à l'intégrité des données).
[48] Elles ne sont pas ou plus disponibles (atteinte à la disponibilité des données).
[49] Voir l'annexe 3 – Échelle de gravité et exemples d'impacts.
[50] Répondre à la question « Que craint-on qu'il arrive aux personnes concernées ? ».
[51] Voir l'annexe 4 – Échelle de vraisemblance et exemples de menaces.
[52] Répondre à la question « Comment cela pourrait-il arriver ? ».
[53] Voir l'annexe 2 – Sources de risques.
[54] Un risque est composé d'un événement redouté et de toutes les menaces qui permettraient qu'il survienne.
[55] Risques qui subsistent après application des mesures.

3.2.1 Accès illégitime à des données

Évaluation du risque

Vous trouverez ci-dessous un tableau permettant de consigner le résultat de l'analyse de ce risque.

Pour illustrer son utilisation, il est renseigné avec les éléments de notre exemple de jouet fictif.

Risque	Principales sources de risques[56]	Principales menaces[57]	Principaux impacts potentiels[58]	Principales mesures réduisant la gravité et la vraisemblance[59]	Gravité[60]	Vraisemblance[61]
Accès illégitime à des données	Entourage malintentionné Voisin malintentionné Employé malintentionné Société tierce autorisée Attaquant ciblant un utilisateur ou une des sociétés	Consultation/vol des données sur le serveur Usurpation d'un compte (via un *smartphone*) Récupération d'un appareil mis au rebut	Conséquences d'une communication d'informations potentiellement sensibles (discrimination, menaces, agressions, perte d'emploi, perte d'accès à des services, *etc.*) *Phishing* Publicité ciblée	Minimisation Durées de conservation Contrôle d'accès logique des utilisateurs Chiffrement de flux (SSL) Authentification des équipements *Cloud* privé Contrôle d'accès logique des utilisateurs Habilitation des employés Journalisation des accès Audits des journaux Notification de la violation aux personnes concernées et prescription de mesures préventives adaptées	Importante	Maximale

Décrivez ici quelques scénarios représentatifs du risque d'accès illégitime aux données, en reprenant les sources, les menaces et les impacts.

Vous trouverez ci-dessous une illustration basée sur notre exemple de jouet fictif :

[56] Sources pertinentes pour ce risque, parmi celles identifiés dans le contexte du traitement (cf. annexe 2 – Sources de risques).
[57] Voir l'annexe 4 – Échelle de vraisemblance et exemples de menaces.
[58] Voir l'annexe 3 – Échelle de gravité et exemples d'impacts.
[59] Mesures parmi celles identifiées au §2 (juridiques) et au §3.1 (sécurité).
[60] Voir l'annexe 3 – Échelle de gravité et exemples d'impacts.
[61] Voir l'annexe 4 – Échelle de vraisemblance et exemples de menaces.

Des données pourraient être volées par un employé agissant par appât du gain ou malveillance, consultées par l'entourage usurpant le compte via le smartphone, ou récupérées sur un matériel mis au rebut par le voisinage ou un attaquant dans le but de caractériser une situation relevant de la vie privée des personnes.

Évaluation des risques résiduels

→ *Acceptable / améliorable ?*

L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable.

→ *Mesures correctives :*

Le cas échéant, il indiquera ici les mesures complémentaires qui seraient nécessaires.

→ *Risques résiduels :*

L'évaluateur indiquera ici le risque demeurant pour le traitement après la mise en œuvre des mesures complémentaires ci-dessus, en estimant la gravité et la vraisemblance compte tenu de ces mesures.

Gravité : ***Vraisemblance :***

Attention : une mesure complémentaire prise pour traiter un des risques peut également avoir un effet, positif ou négatif, sur les autres risques.

Vous trouverez ci-dessous une illustration basée sur notre exemple de jouet fictif :

→ *Améliorable :*

Les mesures prévues ne réduisent pas suffisamment ce risque pour qu'il puisse être jugé acceptable.

→ *Mesures correctives :*

- mettre en œuvre des mesures de chiffrement des données stockées en base ;
- préciser à l'utilisateur les bonnes pratiques à suivre lors de la mise au rebut des matériels ;
- mettre en place une charte d'utilisation des moyens informatiques et un engagement de confidentialité pour les employés.

→ *Risques résiduels :*

Des données pourraient être consultées par l'entourage usurpant le compte via le smartphone.

***Gravité** : Importante* ***Vraisemblance** : Négligeable*

3.2.2 Modification non désirée de données

Évaluation du risque

Vous trouverez ci-dessous un tableau permettant de consigner le résultat de l'analyse de ce risque. Pour illustrer son utilisation, il est renseigné avec les éléments de notre exemple de jouet fictif.

Risques	Principales sources de risques	Principales menaces	Principaux impacts potentiels	Principales mesures réduisant la gravité et la vraisemblance	Gravité	Vraisemblance
Modification non désirée de données	Utilisateur ou entourage, négligent ou malintentionné Voisin malintentionné Employé négligent ou malintentionné Attaquant ciblant une des sociétés	Altération des données sur le serveur	Usurpation d'identité Détérioration de la qualité du service	Sauvegarde du serveur *cloud* Chiffrement de flux (SSL) Authentification des équipements *Cloud* privé Contrôle d'accès logique des utilisateurs Habilitation des employés Journalisation des accès Audits des journaux Notification de la violation aux personnes concernées et prescription de mesures préventives adaptées	Limitée	Limitée

Décrivez ici quelques scénarios représentatifs du risque de modification non désirée de données, en reprenant les sources, les menaces et les impacts.

Évaluation des risques résiduels

→ Acceptable / améliorable ?

L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable.

→ Mesures correctives :

Le cas échéant, il indiquera ici les mesures complémentaires qui seraient nécessaires.

→ Risques résiduels :

L'évaluateur indiquera ici le risque demeurant pour le traitement après la mise en œuvre des mesures complémentaires ci-dessus, en estimant la gravité et la vraisemblance compte tenu de ces mesures.

Gravité : ***Vraisemblance :***

3.2.3 Disparition de données

Évaluation du risque

Vous trouverez ci-dessous un tableau permettant de consigner le résultat de l'analyse de ce risque. Pour illustrer son utilisation, il est renseigné avec les éléments de notre exemple de jouet fictif.

Risques	Principales sources de risques	Principales menaces	Principaux impacts potentiels	Principales mesures réduisant la gravité et la vraisemblance	Gravité	Vraisemblance
Disparition de données	Utilisateur ou entourage, négligent ou malintentionné Employé négligent ou malintentionné Attaquant ciblant un utilisateur ou une des sociétés Sinistre chez une des sociétés	Suppression de données (via l'application ou le serveur) Détérioration de serveurs Dégradation physique de l'appareil	Nécessité de recréer un compte d'utilisation Perte de l'historique et de la personnalisation du service Détérioration de la qualité du service	Sauvegarde du serveur *cloud* *Cloud* privé Protection physique des serveurs *cloud* Maintenance Conservation locale et temporaire des données Contrôle d'accès logique des utilisateurs Habilitation des employés Authentification forte des employés Journalisation des accès Garantie pour l'appareil	Limitée	Limitée

Décrivez ici quelques scénarios représentatifs du risque de disparition de données, en reprenant les sources, les menaces et les impacts.

Évaluation des risques résiduels

→ Acceptable / améliorable ?

L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable.

→ Mesures correctives :

Le cas échéant, il indiquera ici les mesures complémentaires qui seraient nécessaires.

→ Risques résiduels :

L'évaluateur indiquera ici le risque demeurant pour le traitement après la mise en œuvre des mesures complémentaires ci-dessus, en estimant la gravité et la vraisemblance compte tenu de ces mesures.

Gravité : ***Vraisemblance :***

4 Validation du PIA

Généralement réalisée par le responsable de traitement, avec l'aide d'une personne en charge des aspects « Informatique et libertés », notamment le Délégué à la protection des données si désigné.

Objectif : Décider d'accepter ou non le PIA au regard des résultats de l'étude.

4.1 Préparation des éléments utiles à la validation

- Consolider et mettre en forme les résultats de l'étude :
  1. élaborer une représentation visuelle des **mesures choisies pour respecter les principes fondamentaux,** en fonction de leur conformité au [RGPD] (ex : à améliorer, ou jugé comme conforme) ;
  2. élaborer une représentation visuelle des **mesures choisies pour contribuer à la sécurité des données,** en fonction de leur conformité aux bonnes pratiques de sécurité (ex : à améliorer, ou jugé comme conforme) ;
  3. élaborer une cartographie visuelle des **risques** (le cas échéant, initiaux et résiduels[62]) en fonction de leur gravité et vraisemblance ;
  4. élaborer un **plan d'action** à partir des mesures complémentaires identifiées lors des étapes précédentes : pour chaque mesure, déterminer au moins le responsable de sa mise en œuvre, son coût (financier ou en termes de charge) et son échéance prévisionnelle.

- Formaliser la prise en compte des parties prenantes :
  1. le **conseil de la personne en charge des aspects « Informatique et libertés »**[63];
  2. l'**avis des personnes concernées ou de leurs représentants**[64].

Note : Les zones permettant de consigner l'évaluation des mesures et des risques sont insérées directement au sein des parties précédentes, au plus près des éléments à évaluer.

Toutes les parties doivent avoir été évaluées avant de statuer sur la validation du PIA.

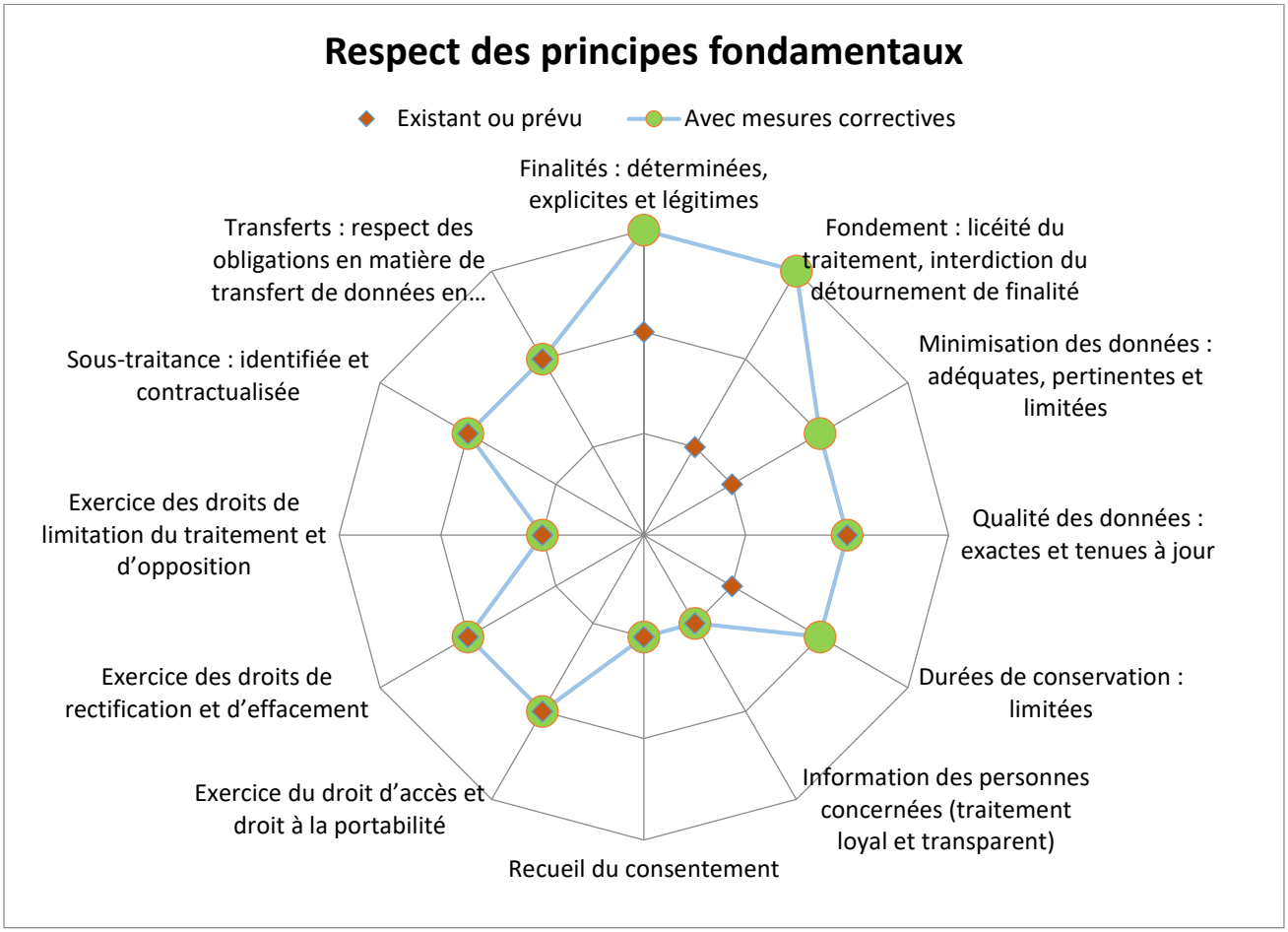
[62] Risques qui subsistent après application des mesures.
[63] Voir article 35 (2) du [RGPD]
[64] Voir article 35 (9) du [RGPD]

4.1.1 Cartographie du respect des principes fondamentaux

Vous trouverez ci-dessous un graphique pour représenter les mesures de respect des principes fondamentaux, en attribuant à chacune une valeur de conformité selon son évaluation au §2.3.

Pour illustrer son utilisation, il est renseigné avec les éléments de notre exemple de jouet fictif.

Si les mesures complémentaires sont correctement mises en œuvre, le respect des principes fondamentaux pourrait être représenté comme suit :



Échelle du graphe :

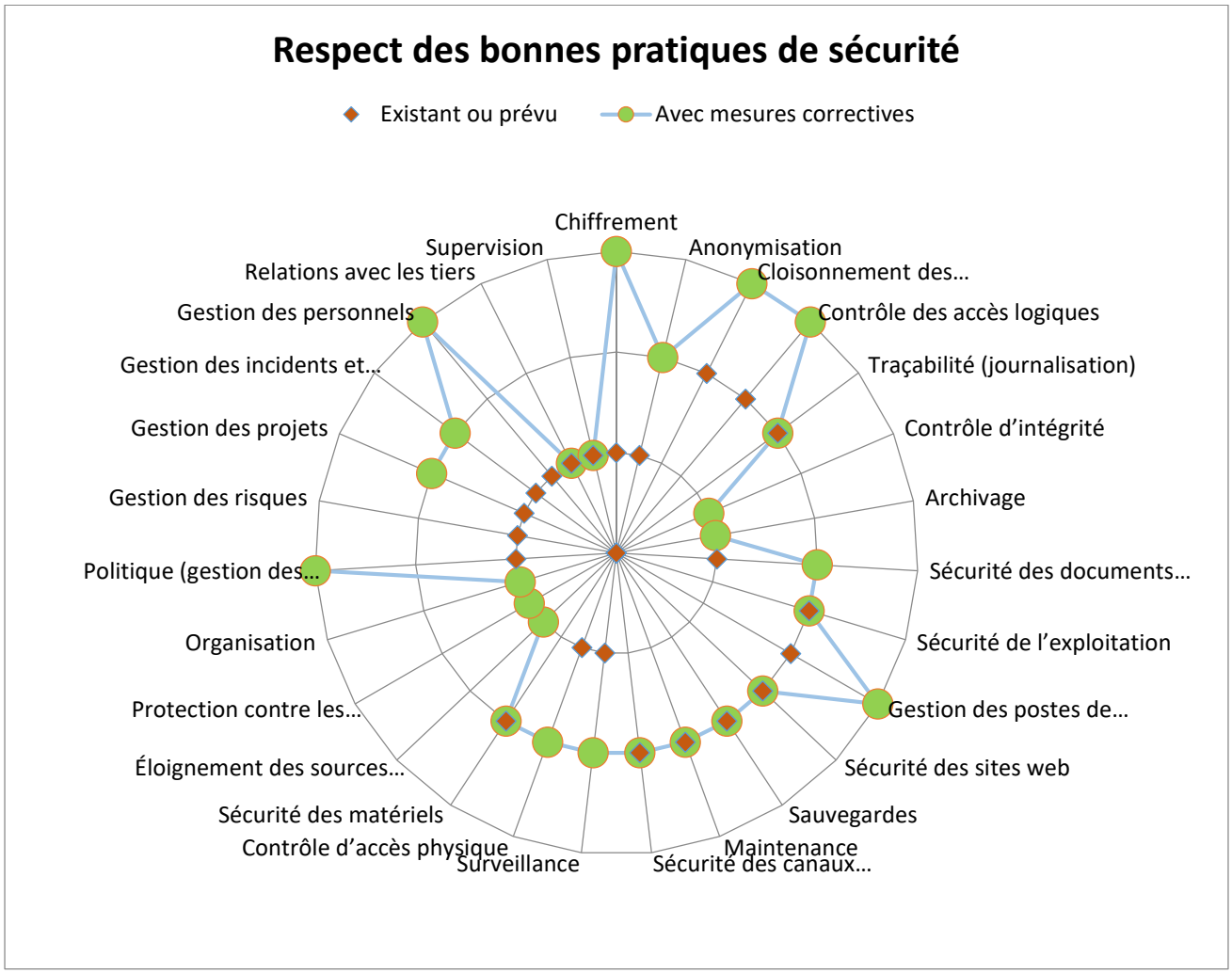
0. Non applicable
1. Améliorable
2. Acceptable
3. Bonnes pratiques

4.1.2 Cartographie du respect des bonnes pratiques de sécurité

Vous trouverez ci-dessous un graphique pour représenter les bonnes pratiques de sécurité, en attribuant à chacune une valeur de conformité selon son évaluation au §3.1.4.

Pour illustrer son utilisation, il est renseigné avec les éléments de notre exemple de jouet fictif.

Si les mesures complémentaires sont correctement mises en œuvre, le respect des bonnes pratiques de sécurité pourrait être représenté comme suit :



Échelle du graphe :

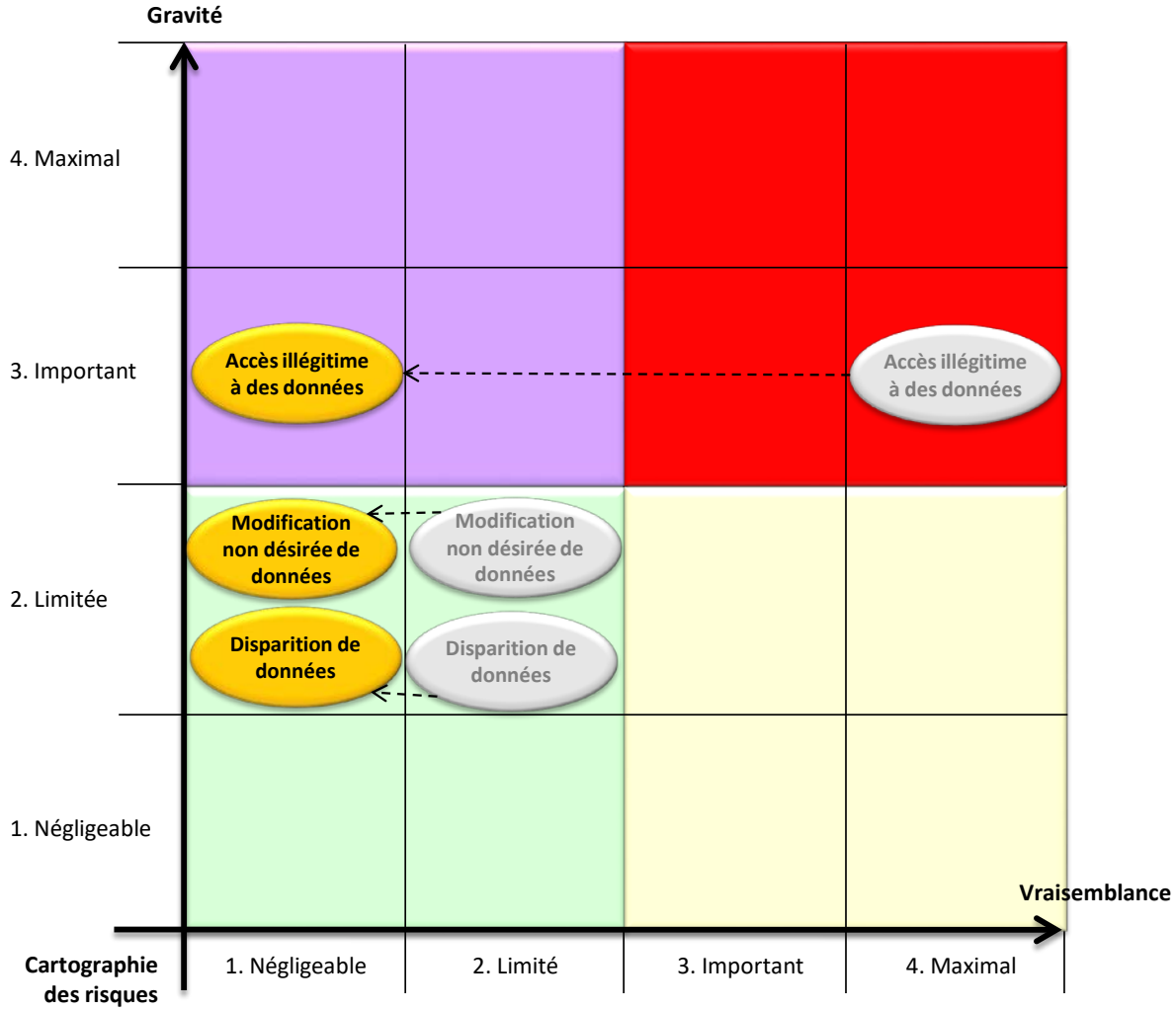
0. Non applicable
1. Améliorable
2. Acceptable
3. Bonnes pratiques

4.1.3 Cartographie des risques

Vous trouverez ci-dessous un graphique pour représenter les risques engendrés par le traitement et les risques résiduels compte tenu de l'ensemble des mesures correctives du plan d'action au §4.1.

Pour illustrer son utilisation, il est renseigné avec les éléments de notre exemple de jouet fictif.

Si les mesures complémentaires sont correctement mises en œuvre, les risques résiduels devraient être les suivants :



4.1.4 Plan d'action : détail des mesures complémentaires prévues

Vous trouverez ci-dessous un tableau pour regrouper l'ensemble des mesures correctives proposées par l'évaluateur au §2.3, §3.1.4, §3.2.1, §3.2.2 et §3.2.3, et ainsi constituer un plan d'action en indiquant pour chaque action son responsable, son terme, sa difficulté, son coût et son état d'avancement (cf. annexe 5 – Échelles pour le plan d'action).

Pour illustrer son utilisation, il est renseigné avec les éléments de notre exemple de jouet fictif.

Mesures complémentaires demandées	Responsable	Terme	Difficulté	Coût	Avancement
Préciser à l'utilisateur les bonnes pratiques à suivre lors de la mise au rebut des matériels	Service clients et RSSI	Mois	Faible	Nul	Non démarré
Mettre en place une charte d'utilisation des moyens informatiques à destination des employés	Service juridique et RSSI	Mois	Faible	Nul	En cours
Mettre en place un engagement de confidentialité des employés	Service juridique et RSSI	Mois	Faible	Nul	Non démarré
Mettre en œuvre des mesures de chiffrement des données stockées en base	MOE et RSSI	Trimestre	Moyenne	Moyen	Non démarré

Attention : toutes les mesures spécifiées dans le plan d'action devront être formalisées, mises en place, contrôlées de manière régulière et améliorées de manière continue.

4.1.5 Conseil de la personne en charge des aspects « Informatique et libertés »[65]

Vous trouverez ci-dessous une zone pour consigner l'avis général de la personne en charge des aspects « Informatique et libertés », avant validation.

Note : cet avis peut être défavorable à la mise en œuvre du traitement, sans pour autant contraindre la décision du responsable de traitement.

Le jj/mm/aaaa, le Délégué à la Protection des Données de la société X a rendu l'avis suivant concernant la conformité du traitement et de l'étude PIA réalisée :

[Signature]

[65] Voir l'article 35 (2) du [RGPD].

4.1.6 Avis des personnes concernées ou de leurs représentants[66]

Vous trouverez ci-dessous une zone pour consigner l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu.

Attention[67] : le responsable de traitement doit demander l'avis des personnes concernées ou de leurs représentants, le cas échéant.

Cet avis peut être recueilli par divers moyens, selon le contexte (étude interne ou externe concernant la finalité et les moyens du traitement, question aux représentants du personnel ou aux syndicats, enquête auprès des futurs clients du responsable de traitement.

Si le responsable de traitement décide de passer outre l'avis des personnes concernées, il doit consigner la justification de sa décision.

Si le responsable de traitement considère que recueillir l'avis des personnes concernées n'est pas pertinent, il doit également en consigner la justification.

Les personnes concernées [ont/n'ont pas été] consultées [et ont émis l'avis suivant sur la conformité du traitement au vu de l'étude réalisée] :

Justification de la décision du responsable de traitement :

[66] Voir l'article 35 (9) du [RGPD].
[67] Voir les lignes directrices du G29 sur les PIA (en anglais).

4.2 Validation formelle du PIA

- Décider de l'acceptabilité des mesures choisies, des risques résiduels et du plan d'action, de manière argumentée, au regard des enjeux préalablement identifiés et de l'avis des parties prenantes. Le PIA peut ainsi être :
  - validé ;
  - à améliorer (expliquer en quoi) ;
  - refusé (ainsi que le traitement considéré).

- Le cas échéant, revoir les étapes précédentes pour que le PIA puisse être validé[68].

Note : cette décision ne préjuge en rien de l'évaluation de conformité qui peut être faite, le cas échéant, par l'autorité de protection des données (en France, la CNIL), par exemple dans le cadre de formalités préalables ou de contrôles.

Vous trouverez ci-dessous un modèle de validation formelle du PIA, illustré avec les éléments de notre exemple de jouet fictif.

Le jj/mm/aaaa, le directeur général de la société X valide le PIA du traitement de jouet connecté, au vu de l'étude réalisée, en sa qualité de responsable du traitement.

Le traitement a pour finalité de fournir une interactivité à l'enfant, à travers la possibilité de dialogue avec le jouet (questions/réponses en langage naturel par reconnaissance vocale), de permettre à l'enfant de communiquer en ligne (envoi de messages vocaux, de textes et de photos) avec ses amis et/ou ses parents et de remonter des informations aux parents (dispositif de surveillance).

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]

[68] Voir notamment l'annexe 6 – Typologie d'objectifs pour traiter les risques.

Annexes

1. Mesures de minimisation des données

Mesures de minimisation	Description
Filtrage et retrait	Lors de l'importation de données, différents types de métadonnées (par exemple, des données EXIF attachées avec un fichier d'image) peuvent être involontairement collectés. Ces métadonnées doivent être identifiées et éliminées si elles ne sont pas nécessaires aux finalités spécifiées.
Réduction de la sensibilité par transformation	Après réception de données sensibles, faisant partie d'un lot d'informations générales ou transmises à des fins statistiques uniquement, celles-ci peuvent être converties en une forme moins sensible ou pseudonymisée. Par exemple, si le système collecte l'adresse IP pour déterminer l'emplacement de l'utilisateur dans un but statistique, l'adresse IP peut être supprimées après déduction de la ville ou du quartier. Si le système reçoit des données vidéo à partir de caméras de surveillance, il peut reconnaître les personnes debout ou en mouvement dans la scène et les flouter. Si le système est un compteur intelligent, il peut agréger l'utilisation de l'énergie sur une certaine période, sans l'enregistrer en temps réel.
Réduction du caractère identifiant des données	Le système peut faire en sorte que : 1) l'utilisateur peut utiliser une ressource ou un service sans risque de divulguer son identité (données anonymes) 2) l'utilisateur peut utiliser une ressource ou un service sans divulguer son identité, mais reste identifiable et responsable de cette utilisation (données pseudonymes) 3) l'utilisateur peut faire de multiples utilisations des ressources ou des services sans risque que ces utilisations puissent être reliées ensemble (données non corrélables) 4) l'utilisateur peut utiliser une ressource ou un service sans risque que d'autres, en particulier des tiers, puissent être en mesure d'observer que la ressource ou le service est utilisé (non-observabilité) Le choix d'une méthode de la liste ci-dessus doit dépendre des menaces identifiées. Pour certains types de menaces sur la vie privée, la pseudonymisation sera plus appropriée que l'anonymisation (par exemple, s'il y a un besoin de traçabilité). En outre, certaines menaces sur la vie privée seront traitées par une combinaison de plusieurs méthodes.
Réduction de l'accumulation de données	Le système peut être structuré en parties indépendantes avec des fonctions de contrôle d'accès distinctes. Les données peuvent également être réparties entre ces sous-systèmes indépendants et contrôlées par chaque sous-système en utilisant différents mécanismes de contrôle d'accès. Si un sous-système est compromis, les impacts sur l'ensemble des données peuvent ainsi être réduits.
Restriction de l'accès aux données	Le système peut limiter l'accès aux données selon le principe du « besoin d'en connaître ». Le système peut séparer les données sensibles et appliquer des politiques de contrôle d'accès spécifiques. Le système peut aussi chiffrer les données sensibles pour protéger leur confidentialité lors de la transmission et du stockage. L'accès aux fichiers cachés temporaires qui sont produits au cours du traitement des données devrait également être protégé.

2. Sources de risques

À titre d'illustration, le tableau suivant décrit les sources de risques et leurs capacités, pertinentes dans le contexte de notre exemple de jouet fictif.

Types de sources de risques	Sources de risques pertinentes	Description des capacités	Description des motivations	Décision
Sources humaines internes agissant accidentellement ou de manière délibérée	**Employé négligent ou malintentionné**	Proximité du système, compétences, privilèges et temps disponible potentiellement élevés, possible manque de formation et de sensibilisation	Maladresse, erreur, négligence Vengeance, volonté d'alerter, malveillance Appât du gain, espionnage,	Retenu
	Utilisateur ou entourage, négligent ou malintentionné	Accès direct à l'appareil et à l'application	Maladresse, erreur, négligence Jeu, malveillance Vengeance, espionnage	Retenu
Sources humaines externes agissant de manière délibérée	**Voisin malintentionné**	Proximité physique permettant de s'insérer dans les communications de l'appareil	Jeu, nuisance, malveillance Vengeance, espionnage	Retenu
	Attaquant ciblant un utilisateur	Connaissance de l'utilisateur et de certaines des informations le concernant	Jeu, nuisance, malveillance Vengeance, espionnage	Retenu
	Attaquant ciblant une des sociétés	Connaissance des sociétés pouvant permettre d'attenter à leur image	Vengeance, volonté d'alerter, malveillance Appât du gain, espionnage	Retenu
	Société tierce autorisée	Accès privilégiés pouvant être utilisés pour accéder illégitimement à des informations	Appât du gain, volonté de disposer de beaucoup de données et de les exploiter	Retenu
Sources humaines externes agissant accidentellement	**Voisin ignorant**	Proximité physique permettant d'émettre sur le canal de communication de l'appareil	Ignorance	Non retenu
Sources non humaines	**Incident ou sinistre chez l'utilisateur** (coupure de courant, incendie, inondation, *etc.*)	Divers		Non retenu
	Sinistre chez une des sociétés (coupure de courant, incendie, inondation, *etc.*)	Divers		Retenu

3. Échelle de gravité et exemples d'impacts

L'échelle suivante peut être utilisée pour estimer la gravité des événements redoutés (**attention : ce ne sont que des exemples, qui peuvent être très différents selon le contexte**) :

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels[69]	Exemples d'impacts matériels[70]	Exemples d'impacts moraux[71]
1. Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté	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 Internet à des fins de publicité ciblée (information des réseaux sociaux réutilisation pour un mailing papier) Publicité ciblée pour des produits de consommation courants	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 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)	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

[69] Préjudice d'agrément, d'esthétique ou économique lié à l'intégrité physique.
[70] Perte subie ou gain manqué concernant le patrimoine des personnes.
[71] Souffrance physique ou morale, préjudice esthétique ou d'agrément.

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels[69]	Exemples d'impacts matériels[70]	Exemples d'impacts moraux[71]
			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	
3. Importante	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives	Affection physique grave causant un préjudice à long 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.	Détournements d'argent non indemnisé Difficultés financières non 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	Affection psychologique grave (ex. : dépression, développement d'une phobie) 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)

4. Échelle de vraisemblance et exemples de menaces

L'échelle suivante peut être utilisée pour estimer la vraisemblance des menaces :

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).

L'action des sources de risques sur les supports constitue une menace. 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 ;
- 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.

Les menaces génériques qui suivent sont conçues pour être exhaustives, indépendantes et appliquées aux spécificités de la protection de la vie privée.

Menaces pouvant mener à un accès illégitime aux DCP

Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
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)
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
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)

Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
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)
Logiciels	Utilisés 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
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
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
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
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)
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)
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
Documents papier	Observés	Lecture, photocopie, photographie	Permet d'observer des données interprétables
Documents papier	Perdus	Vol de dossiers dans les bureaux, vol de courriers dans la boîte aux lettres, récupération de documents mis au rebut	Portable
Canaux papier	Observés	Lecture de parapheurs en circulation, reproduction de documents en transit	Observable

Menaces pouvant mener à une modification non désirées des DCP

Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
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)
Logiciels	Utilisés 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
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
Canaux informatiques	Utilisés 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)
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
Personnes	Détournées	Influence (rumeur, désinformation)	Influençable (naïf, crédule, obtus)
Documents papier	Modifiés	Modification de chiffres dans un dossier, remplacement d'un document par un faux	Falsifiable (support papier au contenu modifiable)
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

Menaces pouvant mener à une disparition des DCP

Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
Matériels	Utilisés de manière inadaptée	Stockage de fichiers personnels, utilisation à des fins personnelles	Utilisable en dehors de l'usage prévu
Matériels	Surchargés	Unité de stockage pleine, panne de courant, surexploitation des capacités de traitement, échauffement, température excessive, attaque par dénis de service	Dimensionnement inapproprié des capacités de stockage, dimensionnement inapproprié des capacités de traitement, n'est pas approprié aux conditions d'utilisation, requiert en permanence de l'électricité pour fonctionner, sensible aux variations de tension
Matériels	Modifiés	Ajout d'un matériel incompatible menant à une panne, retrait d'un matériel indispensable au fonctionnement du système	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions) via des connecteurs (ports, slots), permet de désactiver des éléments (port USB)
Matériels	Détériorés	Inondation, incendie, vandalisme, dégradation du fait de l'usure naturelle, dysfonctionnement d'un dispositif de stockage	Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement) ; n'est pas approprié aux conditions d'utilisation ; effaçable (vulnérable aux effets magnétiques ou vibratoires)
Matériels	Perdus	Vol d'un ordinateur portable, perte d'un téléphone portable, mise au rebut d'un support ou d'un matériel, disques sous dimensionnés amenant à une multiplication des supports et à la perte de certains	Portable, attractif (valeur marchande)
Logiciels	Utilisés de manière inadaptée	Effacement de données, utilisation de logiciels contrefaits ou copiés, erreur de manipulation menant à la suppression 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
Logiciels	Surchargés	Dépassement du dimensionnement d'une base de données, injection de données en dehors des valeurs prévues, attaque par dénis de service	Permet de saisir n'importe quelle donnée, permet de saisir n'importe quel volume de données, permet d'exécuter des actions avec les données entrantes, peu interopérable
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
Logiciels	Détériorés	Effacement d'un exécutable en production ou de code sources, virus, bombe logique	Possibilité d'effacer ou de supprimer des programmes, exemplaire unique, utilisation complexe (mauvaise ergonomie, peu d'explications)
Logiciels	Perdus	Non renouvellement de la licence d'un logiciel utilisé pour accéder aux données, arrêt des mises à jour de maintenance de sécurité par l'éditeur, faillite de l'éditeur, corruption du module de stockage contenant les numéros de licence	Exemplaire unique (des contrats de licence ou du logiciel, développé en interne), attractif (rare, novateur, grande valeur commerciale), cessible (clause de cessibilité totale dans la licence)

Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
Canaux informatiques	Surchargés	Détournement de la bande passante, téléchargement non autorisé, coupure d'accès Internet	Dimensionnement fixe des capacités de transmission (dimensionnement insuffisant de la bande passante, plage de numéros téléphoniques limitée)
Canaux informatiques	Détériorés	Sectionnement de câblage, mauvaise réception du réseau wifi, oxydation des câbles	Altérable (fragile, cassable, câble de faible structure, à nu, gainage disproportionné), unique
Canaux informatiques	Perdus	Vol de câbles de transmission en cuivre	Attractif (valeur marchande des câbles), transportable (léger, dissimulable), peu visible (oubliable, insignifiant, peu remarquable)
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 aux conditions d'exercice de ses fonctions, incapacité à s'adapter au changement
Personnes	Détériorées	Accident du travail, maladie professionnelle, autre blessure ou maladie, décès, affection neurologique, psychologique ou psychiatrique	Limites physiques, psychologiques ou mentales
Personnes	Perdues	Décès, retraite, changement d'affectation, fin de contrat ou licenciement, 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
Documents papier	Utilisés de manière inadaptée	Effacement progressif avec le temps, effacement volontaire de parties d'un texte, réutilisation des papiers pour prendre des notes sans relation avec le traitement, pour faire la liste de course, utilisation des cahiers pour faire autre chose	Modifiable (support papier au contenu effaçable, papiers thermiques non résistants aux modifications de températures)
Documents papier	Détériorés	Vieillissement de documents archivés, embrasement des dossiers lors d'un incendie	Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement), n'est pas approprié aux conditions d'utilisation
Documents papier	Perdus	Vol de documents, perte de dossiers lors d'un déménagement, mise au rebut	Portable
Canaux papier	Surchargés	Surcharge de courriers, surcharge d'un processus de validation	Existence de limites quantitatives ou qualitatives
Canaux papier	Détériorés	Coupure du flux suite à une réorganisation, blocage du courrier du fait d'une grève	Instable, unique
Canaux papier	Modifiés	Modification dans l'expédition des courriers, réaffectation des bureaux ou des locaux, réorganisation de circuits papier, changement de langue professionnelle	Modifiable (remplaçable)
Canaux papier	Perdus	Réorganisation supprimant un processus, disparition d'un transporteur de documents, vacance de postes	Utilité non reconnue

5. Échelles pour le plan d'action

Les échelles suivantes peuvent être utilisées pour élaborer le plan d'action et suivre sa mise en œuvre :

Critère	Niveau 1	Niveau 2	Niveau 3
Difficulté	Faible	Moyenne	Élevée
Coût financier	Nul	Moyen	Important
Terme	Année	Trimestre	Mois
Avancement	Non démarré	En cours	Terminé

6. Typologie d'objectifs pour traiter les risques

Des objectifs peuvent être fixés en fonction du niveau des risques, par exemple :

1. pour les risques dont la gravité et la vraisemblance sont élevées[72] : ces risques devraient absolument être évités ou réduits par l'application de mesures de sécurité diminuant leur gravité et leur vraisemblance. Dans l'idéal, il conviendrait même de s'assurer qu'ils sont traités à la fois par des mesures indépendantes de prévention (actions avant le sinistre), de protection (actions pendant le sinistre) et de récupération (actions après le sinistre) ;
2. pour les risques dont la gravité est élevée, mais la vraisemblance faible[73] : ces risques devraient être évités ou réduits par l'application de mesures de sécurité diminuant leur gravité ou leur vraisemblance. Les mesures de prévention devraient être privilégiées. Ils peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur gravité et si leur vraisemblance est négligeable ;
3. pour les risques dont la gravité est faible mais la vraisemblance élevée : ces risques devraient être réduits par l'application de mesures de sécurité diminuant leur vraisemblance. Les mesures de récupération devraient être privilégiées. Ils peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur vraisemblance et si leur gravité est négligeable ;
4. pour les risques dont la gravité et la vraisemblance sont faibles : ces risques devraient pouvoir être pris, d'autant plus que le traitement des autres risques devrait également contribuer à leur traitement.

Notes : Les risques peuvent généralement être réduits, transférés ou pris. Toutefois, certains risques ne peuvent l'être, notamment lorsque des données sensibles sont traitées ou quand les préjudices dont peuvent être victimes les personnes concernées sont très importants. Dans de tels cas, il pourra s'avérer nécessaire de les éviter, par exemple en ne mettant pas en œuvre tout ou partie d'un traitement.

[72] Niveaux 3. Important et 4. Maximal.
[73] Niveaux 1. Négligeable et 2. Limité.