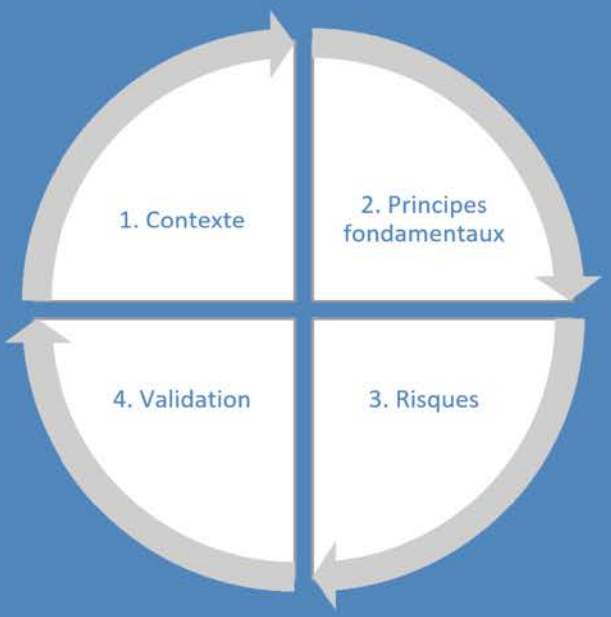
Analyse d'impact relative à la protection des données

Privacy Impact Assessment (PIA)

LA MÉTHODE



CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Édition février 2018

Table des matières

Avant-propos **1**
Introduction **2**
Comment mener un PIA ? **3**
1 Étude du contexte **4**
1.1 Vue d'ensemble 4
1.2 Données, processus et supports 4
2 Étude des principes fondamentaux **5**
2.1 Évaluation des mesures garantissant la proportionnalité et la nécessité du traitement 5
2.2 Évaluation des mesures protectrices des droits des personnes des personnes concernées 5
3 Étude des risques liés à la sécurité des données **6**
Qu'est-ce qu'un risque sur la vie privée ? 6
3.1 Évaluation des mesures existantes ou prévues 7
3.2 Appréciation des risques : les atteintes potentielles à la vie privée 7
4 Validation du PIA **8**
4.1 Préparation des éléments utiles à la validation 8
4.2 Validation formelle 8
Annexes **9**
Définitions 9
Références bibliographiques 10
Couverture des critères des [LignesDirectrices-G29] 11

Avant-propos

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

Ils sont téléchargeables sur le site de la CNIL :







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

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

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

Introduction

Ce guide explique comment mener une "analyse d'impact relative à la protection des données" (cf. art. 35 du [RGPD]), plus communément appelée *Privacy Impact Assessment* (PIA).

Il décrit la manière d'employer la méthode [EBIOS][1] dans le contexte spécifique « Informatique et libertés ». La démarche est conforme aux critères des [LignesDirectrices-G29] (voir la démonstration de couverture fournie en annexe) et compatible avec les normes internationales relatives à la gestion des risques (ex : [ISO 31000]).

Le fonctionnement itératif de cette méthode doit permettre de garantir une utilisation raisonnée et fiable de données à caractère personnel dans le cadre de leur traitement.

La méthode ne traite ni des conditions en amont déterminant s'il faut mener un PIA (cf. art. 35.1 du [RGPD]) ni de celles en aval déterminant qu'il faut consulter l'autorité de protection des données (cf. art. 36.1 du [RGPD]).

Théoriquement mené par un responsable de traitement, 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.

Ce guide s'adresse aux responsables de traitements qui souhaitent justifier de leur démarche de conformité et des mesures qu'ils ont choisies (notion de responsabilité ou d'*accountability* en anglais, cf. art. 25 du [RGPD]), ainsi qu'aux fournisseurs de produits qui souhaitent démontrer que leurs solutions sont conçues dans une logique de conception respectueuse de la vie privée (notion de *Privacy by Design* en anglais, cf. art. 25 du [RGPD])[2]. Il est utile à toutes les parties prenantes dans la création ou l'amélioration de traitements de données à caractère personnel ou de produits :

- les autorités décisionnaires, qui commanditent et valident la création de nouveaux traitements de données à caractère personnel ou produits ;
- les maîtrises d'ouvrage, qui doivent apprécier les risques pesant sur leur système et donner des objectifs de sécurité ;
- les maîtrises d'œuvre, qui doivent proposer des solutions pour traiter les risques conformément aux objectifs identifiés par les maîtrises d'ouvrage ;
- les correspondants « informatique et libertés » ou délégués à la protection des données, qui doivent accompagner les maîtrises d'ouvrage et les autorités décisionnaires dans la protection des données à caractère personnel ;
- les responsables de la sécurité des systèmes d'information, qui doivent accompagner les maîtrises d'ouvrage dans le domaine de la sécurité des systèmes d'information.

[1] EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité – est la méthode de gestion des risques publiée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).
[2] Dans la suite du document, le terme « traitement de données à caractère personnel » est interchangeable avec le terme « produit ».

Comment mener un PIA ?

La démarche de conformité mise en œuvre en menant un PIA repose sur deux piliers :

1. **les principes et droits fondamentaux**[3], « non négociables », qui sont fixés par la loi et doivent être respectés, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
2. **la gestion des risques sur la vie privée**[4], qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données[5].



Figure 1 – La démarche de conformité à l'aide d'un PIA

En résumé, pour mener un PIA, il convient de :

1. délimiter et décrire le **contexte** du(des) traitement(s) considéré(s) ;
2. analyser les mesures garantissant le respect des **principes fondamentaux** : la proportionnalité et la nécessité du traitement, et la protection des droits des personnes concernées ;
3. apprécier les **risques** sur la vie privée liés à la sécurité des données et vérifier qu'ils sont convenablement traités ;
4. formaliser la **validation** du PIA au regard des éléments précédents ou bien décider de réviser les étapes précédentes.

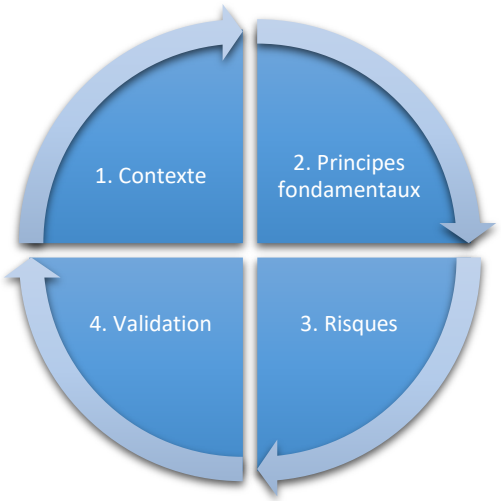


Figure 2 – Démarche générale pour mener un PIA

Il s'agit d'un processus d'amélioration continue. Il requiert donc parfois plusieurs itérations pour parvenir à un dispositif de protection de la vie privée acceptable. Il requiert en outre une surveillance des évolutions dans le temps (du contexte, des mesures, des risques, etc.), par exemple tous les ans, et des mises à jour dès qu'une évolution significative a lieu.

La démarche devrait être employée dès la conception d'un nouveau traitement de données à caractère personnel. En effet, une application en amont permet de déterminer les mesures nécessaires et suffisantes, et donc d'optimiser les coûts. A contrario, une application tardive, alors que le système est déjà créé et les mesures en place, peut remettre en question les choix effectués.

---

[3] Finalité déterminée, explicite et légitime ; données adéquates, pertinentes et non excessives ; information claire et complète des personnes ; durée de conservation limitée ; droit d'opposition, d'accès, de rectification et suppression, *etc.*

[4] Liés à la sécurité des données à caractère personnel et ayant un impact sur la vie privée des personnes concernées.

[5] Afin de « *prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* » (article 34 de la [Loi-I&L]).

1 Étude du contexte

Généralement réalisée par la maîtrise d'ouvrage[6], avec l'aide d'une personne en charge des aspects « Informatique et libertés »[7].

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

1.1 Vue d'ensemble

- Présenter le **traitement** considéré, sa **nature**, sa **portée**, son **contexte**, ses **finalités** et ses **enjeux**[8] de manière synthétique.
- Identifier le **responsable du traitement** et les éventuels **sous-traitants**.
- Recenser les **référentiels applicables** au traitement, utiles ou à respecter[9], notamment les codes de conduite approuvés (cf. art. 40 du [RGPD]) et certifications en matière de protection des données (cf. art. 42 du [RGPD])[10].

1.2 Données, processus et supports

- Délimiter et décrire le périmètre de manière détaillée :
  - les **données** personnelles concernées, leurs **destinataires** 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).

[6] Il s'agit des métiers. Elle peut être déléguée, représentée ou sous-traitée.
[7] Correspondant Informatique et libertés, délégué à la protection des données, ou autre.
[8] Répondre à la question « Quels sont les bénéfices attendus (pour l'organisme, pour les personnes concernées, pour la société en général...) ? ».
[9] 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.
[10] Autres exemples : politique de sécurité, normes juridiques sectorielles, etc.

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.

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

- Expliciter et justifier les **choix effectués pour respecter les exigences** suivantes :
  1. **finalité(s)** : déterminée, explicite et légitime (cf. art. 5.1 (b) du [RGPD]) ;
  2. **fondement** : licéité du traitement, interdiction du détournement de finalité (cf. art. 6 du [RGPD])[11] ;
  3. **minimisation des données** : adéquates, pertinentes et limitées (cf. art. 5.1 (c) du [RGPD])[12] ;
  4. **qualité des données** : exactes et tenues à jour (cf. art. 5.1 (d) du [RGPD]) ;
  5. **durées de conservation** : limitées (cf. art. 5.1 (e) du [RGPD]).
- 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.

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

- Identifier ou déterminer, et décrire, les **mesures retenues** (existantes ou prévues) **pour respecter les exigences** suivantes (nécessitant d'expliquer comment il est prévu de les mettre en œuvre) :
  1. **information** des personnes concernées (traitement loyal et transparent, cf. art. 12, 13 et 14 du [RGPD]) ;
  2. **recueil du consentement**, le cas échéant[13] : exprès, démontrable, retirable (cf. art. 7 et 8 du [RGPD]) ;
  3. exercice des **droits d'accès et à la portabilité** (cf. art. 15 et 20 du [RGPD]);
  4. exercice des **droits de rectification et d'effacement** (cf. art. 16 et 17 du [RGPD])
  5. exercice des **droits de limitation du traitement et d'opposition** (cf. art. 18 et 21 du [RGPD]) ;
  6. **sous-traitance** : identifiée et contractualisée (cf. art. 28 du [RGPD]) ;
  7. **transferts** : respect des obligations en matière de transfert de données en dehors de l'Union européenne (cf. art. 44 à 49 du [RGPD]).
- Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer chaque mesure et sa description, conformément au [RGPD].
- Le cas échéant, revoir leur description ou proposer des mesures complémentaires.

[11] Démontrer également que les destinataires sont légitimes.
[12] Démontrer également que les destinataires ont réellement besoin d'accéder aux données.
[13] Justifier les cas où le consentement n'est pas obtenu.

3 Étude des risques liés à la sécurité des données[14]

Qu'est-ce qu'un risque sur la vie privée ?

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).

Le schéma suivant synthétise l'ensemble des notions présentées :

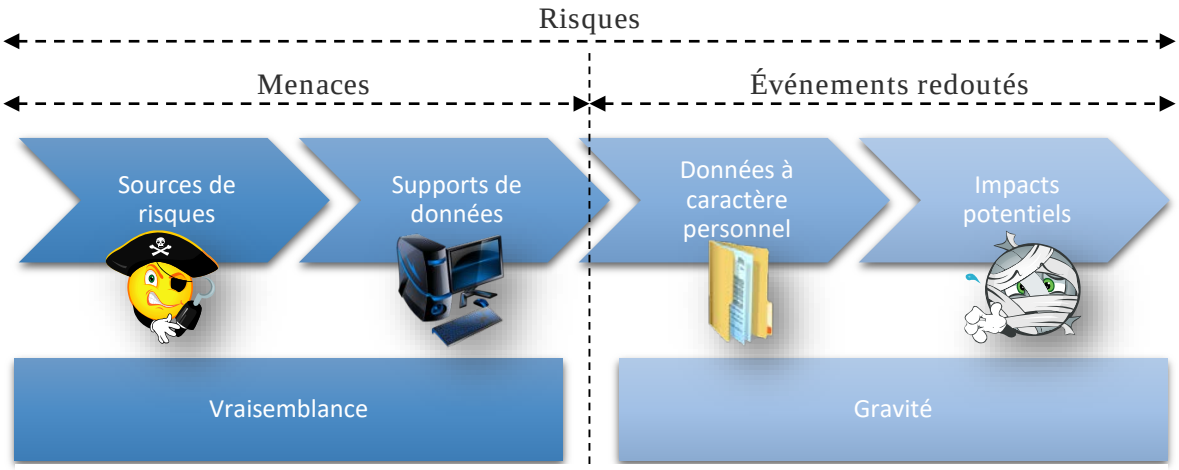


Figure 3 – Éléments composant les risques

Le niveau d'un risque est estimé en termes de gravité et de vraisemblance :

- la **gravité** représente l'ampleur d'un risque. Elle dépend essentiellement du caractère préjudiciable des impacts potentiels[15] ;
- la **vraisemblance** traduit la possibilité qu'un risque se réalise. Elle dépend essentiellement des vulnérabilités des supports face aux menaces et des capacités des sources de risques à les exploiter.

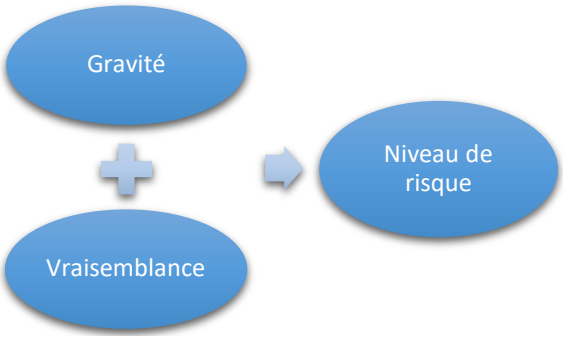


Figure 4 – Éléments permettant d'estimer les risques

[14] Cf. art. 32 du [RGPD].
[15] Compte tenu du contexte (nature des données, personnes concernées, finalité du traitement, etc.).

3.1 Évaluation des mesures existantes ou prévues

Généralement réalisé par la maîtrise d'œuvre[16], puis évaluée par une personne en charge de la sécurité de l'information[17].

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.

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[18], une modification non désirée de données[19], et une disparition de données[20]) :
  1. déterminer les **impacts** potentiels sur la vie privée des personnes concernées s'ils survenaient[21] ;
  2. estimer sa **gravité**, notamment en fonction du caractère préjudiciable des impacts potentiels et, le cas échéant, des mesures susceptibles de les modifier ;
  3. identifier les **menaces** sur les supports des données qui pourraient mener à cet événement redouté[22] et les **sources de risques** qui pourraient en être à l'origine ;
  4. 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[23] peuvent être jugés acceptables compte tenu des mesures existantes ou prévues.
- Dans la négative, proposer des mesures complémentaires et ré-estimer le niveau de chacun des risques en tenant compte de celles-ci, afin de déterminer les risques résiduels.

[16] Elle peut être déléguée, représentée ou sous-traitée.
[17] Responsable de la sécurité des systèmes d'information ou autre.
[18] Elles sont connues de personnes non autorisées (atteinte à la confidentialité des données).
[19] Elles ne sont plus intègres ou sont changées (atteinte à l'intégrité des données).
[20] Elles ne sont pas ou plus disponibles (atteinte à la disponibilité des données).
[21] Répondre à la question « Que craint-on qu'il arrive aux personnes concernées ? ».
[22] Répondre à la question « Comment cela pourrait-il arriver ? ».
[23] Un risque est composé d'un événement redouté et de toutes les menaces qui permettraient qu'il survienne.

4 Validation du PIA

Généralement réalisée par le responsable de traitement, avec l'aide d'une personne en charge des aspects « Informatique et libertés ».

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 résiduels**[24] 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 et/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 »**, si elle a été désignée (cf. art. 35 (2) du [RGPD]) ;
  2. l'**avis des personnes concernées ou de leurs représentants**, le cas échéant (cf. art. 35 (9) du [RGPD]).

4.2 Validation formelle

- 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 :
  1. validé ;
  2. à améliorer (expliquer en quoi) ;
  3. refusé (ainsi que le traitement considéré).
- Le cas échéant, revoir les étapes précédentes pour que le PIA puisse être validé.

[24] Risques qui subsistent après application des mesures.

Annexes

Définitions

Note : les libellés entre parenthèses correspondent aux libellés courts employés dans ce document.

Donnée à caractère personnel (donnée)

Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. [RGPD]

Note : pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. [Loi-I&L]

Événement redouté

Violation potentielle de données pouvant mener à des impacts sur la vie privée des personnes concernées.

Gravité

Estimation de l'ampleur des impacts potentiels sur la vie privée des personnes concernées.

Note : elle dépend essentiellement du caractère préjudiciable des impacts potentiels.

Menace

Mode opératoire composé d'une ou plusieurs actions unitaires sur des supports de données.

Note : elle est utilisée, volontairement ou non, par des sources de risques, et peut provoquer un événement redouté.

Mesure

Action à entreprendre.

Note : elle peut être technique ou organisationnelle, et peut consister mettre en œuvre des principes fondamentaux ou à éviter, réduire, transférer ou prendre tout ou partie des risques.

Personnes concernées

Personnes auxquelles se rapportent les données qui font l'objet du traitement. [Loi-I&L]

Responsable de traitement

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre. [RGPD]

Note : sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement. [Loi-I&L]

Risque

Scénario décrivant un événement redouté et toutes les menaces qui le rendent possibles.

	Note : il est estimé en termes de gravité et de vraisemblance.
Source de risque	Personne ou source non humaine qui peut être à l'origine d'un risque. *Note : elle peut agir de manière accidentelle ou délibérée.*
Support de données	Bien sur lequel reposent des données. *Note : il peut s'agir de matériels, de logiciels, de canaux informatiques, de personnes, de supports papier ou de canaux de transmission papier.*
Traitement de données à caractère personnel (traitement)	Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. [RGPD]
Vraisemblance	Estimation de la possibilité qu'un risque se réalise. *Note : elle dépend essentiellement des vulnérabilités exploitables et des capacités des sources de risques à les exploiter.*

Références bibliographiques

[Charte-UE]	Charte des droits fondamentaux de l'Union européenne, 2010/C 83/02.
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
[Loi-I&L]	Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée[25].
[LignesDirectrices-G29]	Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP 248 rév. 01, Groupe de travail « Article 29 » sur la protection des données.
[EBIOS]	Expression des Besoins et Identification des Objectifs de Sécurité – EBIOS – Méthode de gestion des risques, ANSSI.
[ISO 31000]	ISO 31000:2009, Management du risque – Principes et lignes directrices, ISO.

[25] Modifiée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et par la loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures.

Couverture des critères des [LignesDirectrices-G29]

Critères des [LignesDirectrices-G29] (et références au [RGPD])	Couverture	Chapitre de ce guide
Une description systématique du traitement est fournie (Article 35(7)(a)) : - la nature, la portée, le contexte et les finalités du traitement sont pris en compte (considérant 90) ; - les données à caractère personnel, destinataires et durée de conservation sont recensés ; - une description fonctionnelle du traitement est fournie ; - les biens sur lesquels reposent les données à caractère personnel (matériels, logiciels, réseaux, personnes, papier ou canaux de transmission papier) sont identifiés ; - la conformité à des codes de conduite approuvés est prise en compte (Article 35(8)).	☑	1. Étude du contexte

La nécessité et la proportionnalité sont évaluées (Article 35(7)(b)) :
- les mesures envisages pour se conformer au Règlement sont déterminées (Article 35(7)(d) et considérant 90) en tenant compte :
  - des mesures contribuant à la proportionnalité et à la nécessité du traitement, sur la base de :
  - une(des) finalité(s) déterminée(s), explicite(s) et légitime(s) (Article 5(1)(b));
  - la licéité du traitement (Article 6);
  - des données adéquates, pertinentes et limitées à ce qui est nécessaire (Article 5(1)(c));
  - une durée de conservation limitée (Article 5(1)(e));
  - des mesures contribuant aux droits des personnes concernées :
  - l'information des personnes concernées (Articles 12, 13 et 14);
  - le droit d'accès et à la portabilité (Articles 15 et 20) ;
  - les droits de rectification et à l'effacement (Articles 16 et 17);
  - les droits d'opposition et à la limitation du traitement (Articles 16 et 21);
  - les sous-traitants (Article 28);
  - les mesures encadrant le(s) transfert(s) internationaux (Chapitre V).
	☑	2. Étude des principes fondamentaux

Les risques sur les droits et libertés des personnes concernées sont gérés (Article 35(7)(c)):
- l'origine, la nature, la particularité et la gravité des risques sont appréciées (cf. considérant 84) ou, plus spécifiquement, pour chaque risque (accès illégitime, modification non désirée et disparition de données), du point de vue des personnes concernées :
  - les sources de risques sont prises en compte (considérant 90) ;
  - les impacts potentiels sur les droits et libertés des personnes concernées sont identifiés en cas d'accès illégitime, de modification on désirée et de disparition de données ;
  - les menaces qui pourraient mener à un accès illégitime, une modification non désirée et une disparition de données sont identifiées ;
  - la vraisemblance et la gravité sont estimées (considérant 90) ;
- les mesures envisagées pour traiter ces risques sont déterminées (Article 35(7)(d) et considérant 90).
	☑	3. Étude des risques liés à la sécurité des données

Les parties intéressées sont impliquées : - le conseil du délégué à la protection des données est demandé (Article 35(2)) ; - l'avis des personnes concernées ou de leurs représentants sont demandés (Article 35(9)).	☑	4. Validation du PIA

Analyse d'impact relative à la protection des données

Privacy Impact Assessment (PIA)

LES MODÈLES



CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Édition février 2018

Table des matières

Avant-propos 2

1 Modèles utiles à l'étude du contexte 4

1.1 Vue d'ensemble 4
Présentation du(des) traitement(s) considéré(s) 4
Recensement des référentiels applicables au traitement 4

1.2 Données, processus et supports 4
Description des données, destinataires et durées de conservation 4
Description des processus et supports 4

2 Modèles utiles à l'étude des principes fondamentaux 5

2.1 Évaluation des mesures garantissant la proportionnalité et la nécessité du traitement 5
Explication et justification des finalités 5
Explication et justification du fondement 5
Explication et justification de la minimisation des données 6
Explication et justification de la qualité des données 6
Explication et justification des durées de conservation 6
Évaluation des mesures 6

2.2 Évaluation des mesures protectrices des droits des personnes des personnes concernées 7
Détermination et description des mesures pour l'information des personnes 7
Détermination et description des mesures pour le recueil du consentement 8
Détermination et description des mesures pour les droits d'accès et à la portabilité 8
Détermination et description des mesures pour les droits de rectification et d'effacement 10
Détermination et description des mesures pour les droits de limitation du traitement et d'opposition 11
Détermination et description des mesures pour la sous-traitance 11
Détermination et description des mesures pour le transfert de données en dehors de l'Union européenne 12
Évaluation des mesures 12

3 Modèles utiles à l'étude des risques liés à la sécurité des données 13

3.1 Évaluation des mesures 13
Description et évaluation des mesures contribuant à traiter des risques liés à la sécurité des données 13
Description et évaluation des mesures générales de sécurité 15
Description et évaluation des mesures organisationnelles (gouvernance) 18

3.2 Appréciation des risques : les atteintes potentielles à la vie privée 20
Analyse et estimation des risques 20
Évaluation des risques 20

4 Modèles utiles à la validation du PIA 21

4.1 Préparation des éléments utiles à la validation 21
Élaboration de la synthèse relative à la conformité au [RGPD] des mesures permettant de respecter les principes fondamentaux 21
Élaboration de la synthèse relative à la conformité aux bonnes pratiques des mesures des mesures contribuant à traiter les risques liés à la sécurité des données 22
Élaboration de la cartographie des risques liés à la sécurité des données 23
Élaboration du plan d'action 24
Formalisation du conseil de la personne en charge des aspects « Informatique et libertés » 24
Formalisation de l'avis des personnes concernées ou de leurs représentants 24

4.2 Validation formelle 25
Formalisation de la validation 25

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Avant-propos

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







Ils sont téléchargeables sur le site de la CNIL :

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

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

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

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

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

1 Modèles utiles à l'étude du contexte

1.1 Vue d'ensemble

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

Description du traitement[1]	
Finalités du traitement	
Enjeux du traitement	
Responsable du traitement	
Sous-traitant(s)	

Recensement des référentiels applicables au traitement[2]

Référentiels applicables au traitement	Prise en compte

1.2 Données, processus et supports

Description des données, destinataires et durées de conservation

Données	Destinataires	Durées de conservation

Description des processus et supports

[insérer un schéma des flux de données et la description détaillée des processus mis en œuvre]

Processus	Description détaillée du processus	Supports des données concernés

[1] Sa nature, sa portée, son contexte, *etc.*
[2] Voir article 35 (8) du [RGPD].

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

2 Modèles utiles à l'étude des principes fondamentaux

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

Explication et justification des finalités

Finalités	Légitimité

Explication et justification du fondement

Critères de licéité	Applicable	Justification
La personne concernée a consenti[3] 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[4]		

[3] Concernant le recueil du consentement de la personne et son information, voir le 2.2.
[4] Ce point ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Explication et justification de la minimisation des données

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation

Explication et justification de la qualité des données

Mesures pour la qualité des données	Justification

Explication et justification des durées de conservation

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)			

Évaluation des mesures

Mesures garantissant la proportionnalité et la nécessité du traitement	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		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

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

Détermination et description des mesures pour l'information des personnes

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

Dispense d'information des personnes concernées	Justification

Dans le cas contraire :

Mesures pour le droit à l'information	Modalités de mise en œuvre	Justification des modalités ou de l'impossibilité de leur mise en œuvre
Présentation des conditions d'utilisation/confidentialité		
Possibilité d'accéder aux conditions d'utilisation/confidentialité		
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.)		
Présentation détaillée des données personnelles collectées		
Présentation des éventuels accès à des identifiants de l'appareil, en précisant si ces identifiants sont communiqués à des tiers		
Présentation des droits de la personne concernée (retrait du consentement, suppression de données, etc.)		
Information sur le mode de stockage sécurisé des données, notamment en cas d'externalisation		
Modalités de contact de l'entreprise (identité et coordonnées) pour les questions de confidentialité		
Le cas échéant, information de la personne concernée de tout changement concernant les données collectées, les finalités, les clauses de confidentialité		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Mesures pour le droit à l'information	Modalités de mise en œuvre	Justification des modalités ou de l'impossibilité de leur mise en œuvre
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 entreprises tierces		

Détermination et description des mesures pour le recueil du consentement[5]

Mesures pour le recueil du consentement	Modalités de mise en œuvre	Justification des modalités ou de l'impossibilité de leur mise en œuvre
Consentement exprès à l'inscription		
Consentement segmenté par catégorie de données ou types de traitement		
Consentement exprès avant le partage de données avec des tiers		
Consentement présenté de manière compréhensible et adapté à la personne cible (notamment pour les enfants)		
Recueil du consentement des parents pour les mineurs de moins de 13 ans		
Pour une nouvelle personne, mise en œuvre d'un nouveau recueil de consentement		
Après une longue période sans utilisation, demande à la personne concernée 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 de contrat, les paramètres liés à son consentement sont maintenus		

Détermination et description des mesures pour les droits d'accès et à la portabilité

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

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

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

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

Dans le cas contraire :

Mesures pour le droit d'accès	Données internes	Données externes	Justification
Possibilité d'accéder à l'ensemble des données personnelles de l'utilisateur, via les interfaces courantes			
Possibilité de consulter, de manière sécurisée, les traces d'utilisation liées à la personne concernée			
Possibilité de télécharger une archive de l'ensemble des données à caractère personnel liées à la personne concernée			

Enfin, quand le droit à la portabilité est applicable au traitement prévu par l'article 20 du [RGPD] :

Mesures pour le droit à la portabilité	Données internes	Données externes	Justification
Possibilité de récupérer, sous une forme aisément réutilisable, les données personnelles qui ont été fournies par la personne concernée, afin de pouvoir les transférer à un service tiers			

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Détermination et description des mesures pour les droits de rectification et d'effacement

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

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

Dans le cas contraire :

Mesures pour les droits de rectification et d'effacement	Données internes	Données externes	Justification
Possibilité de rectifier les données personnelles			
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 : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Détermination et description des mesures pour les droits de limitation du traitement et d'opposition

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

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

Dans le cas contraire :

Mesures pour les droits de limitation et d'opposition	Données internes	Données externes	Justification
Existence de paramètres « Vie privée »			
Invitation à changer les paramètres par défaut			
Paramètres « Vie privée » accessibles pendant l'inscription			
Paramètres « Vie privée » accessibles après l'inscription			
Existence d'un dispositif de contrôle parental pour les enfants de moins de 13 ans			
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			

Détermination et description des mesures pour la sous-traitance

Nom du sous-traitant	Finalité	Périmètre	Référence du contrat	Conformité art.28[6]

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

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Détermination et description des mesures pour le transfert de données en dehors de l'Union européenne

Données	France	UE	Pays reconnu adéquat par l'UE	Autre pays	Justification et encadrement (clauses contractuelles types, règles internes d'entreprise)

Évaluation des mesures

Mesures protectrices des droits des personnes concernées	Acceptable / améliorable ?	Mesures correctives
Information des personnes concernées (traitement loyal et transparent)		
Recueil du consentement		
Exercice des droits d'accès et à la portabilité		
Exercice des droits de rectification et d'effacement		
Exercice des droits de limitation du traitement et d'opposition		
Sous-traitance : identifiée et contractualisée		
Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

3 Modèles utiles à l'étude des risques liés à la sécurité des données

3.1 Évaluation des mesures

Description et évaluation des mesures contribuant à traiter des risques liés à la sécurité des données

Mesures portant spécifiquement sur les données du traitement	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
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.*]		
Anonymisation	[*Indiquez ici si des mécanismes d'anonymisation sont mis en œuvre, lesquels et à quelle fin.*]		
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*[7]. *Le cas échéant, précisez les*		

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

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Mesures portant spécifiquement sur les données du traitement	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
	règles applicables aux mots de passe (longueur minimale, structure obligatoire, durée de validité, nombre de tentatives infructueuses avant blocage du compte, etc.).]		
Traçabilité (journalisation)	[*Indiquez ici si des événements sont journalisés et la durée de conservation de ces traces.*]		
Contrôle d'intégrité	[*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	[*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.*]		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Description et évaluation des mesures générales de sécurité

Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
Sécurité de l'exploitation	[*Décrivez ici comment les mises à jour des logiciels (systèmes d'exploitation, applications, etc.) et l'application des correctifs de sécurité sont réalisées.*]		
Lutte contre les logiciels malveillants	[*Précisez si un antivirus est installé et régulièrement mis à jour sur tous les postes.*]		
Gestion des postes de travail	[*Détaillez ici les mesures mises en œuvre sur les postes de travail (verrouillage automatique, pare-feu, etc.).*]		
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*		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
	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*		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
	moyens de prévention de dégâts des eaux. *Précisez également les moyens de surveillance et de secours de l'alimentation électrique.*]		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Description et évaluation des mesures organisationnelles (gouvernance)

Mesures organisationnelles (gouvernance)	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
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 font l'objet d'une gestion documentée et testée, notamment en ce qui concerne les violations de données à caractère personnel.*]		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Mesures organisationnelles (gouvernance)	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
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, notamment 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.*]		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

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

Analyse et estimation des risques

Risque	Principales sources de risques	Principales menaces	Principaux impacts potentiels	Principales mesures réduisant la gravité et la vraisemblance	Gravité	Vraisemblance
Accès illégitime à des données						
Modification non désirée de données						
Disparition de données						

Évaluation des risques

Risques	Acceptable / améliorable ?	Mesures correctives	Gravité résiduelle	Vraisemblance résiduelle
Accès illégitime à des données	[*L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable.*]	[*Le cas échéant, il indiquera ici les mesures complémentaires qui seraient nécessaires.*]		
Modification non désirée de données	[*L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable.*]	[*Le cas échéant, il indiquera ici les mesures complémentaires qui seraient nécessaires.*]		
Disparition de données	[*L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable.*]	[*Le cas échéant, il indiquera ici les mesures complémentaires qui seraient nécessaires.*]		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

4 Modèles utiles à la validation du PIA

4.1 Préparation des éléments utiles à la validation

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

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

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

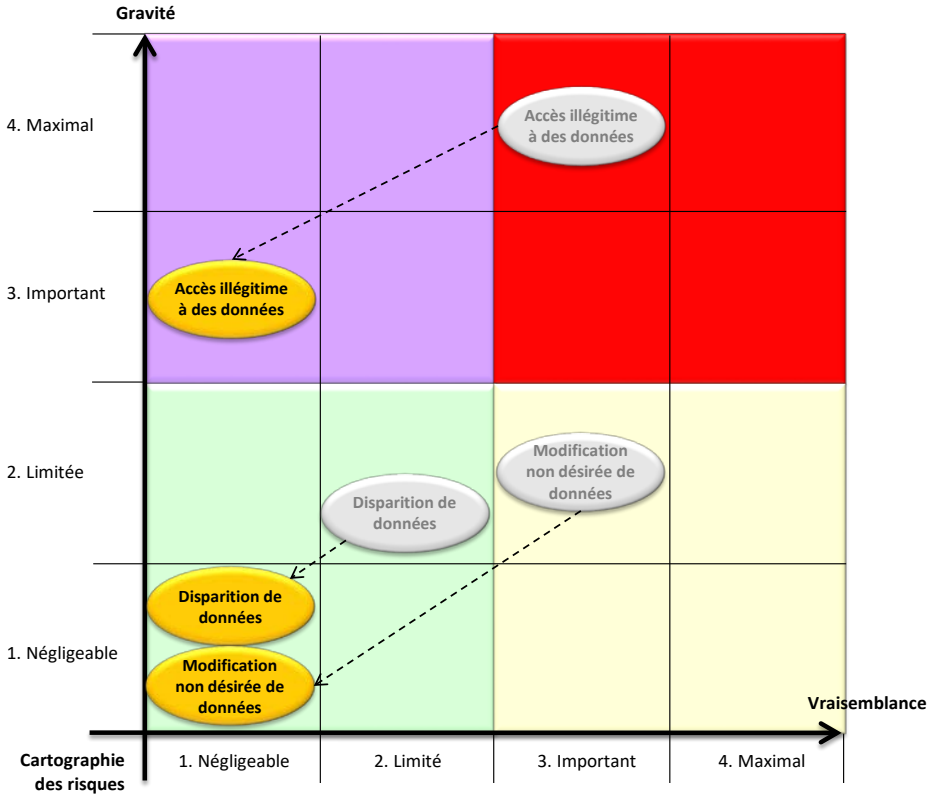
Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

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

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

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

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



Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Élaboration du plan d'action

Mesures complémentaires demandées	Responsable	Terme	Difficulté	Coût	Avancement

Formalisation du conseil de la personne en charge des aspects « Informatique et libertés »[8]

Le [jj/mm/aaaa], le délégué à la protection des données de [nom de l'organisme] a rendu l'avis suivant concernant la conformité du traitement et le PIA mené :

[Signature]

Formalisation de l'avis des personnes concernées ou de leurs représentants[9]

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

Justification de la décision du responsable de traitement :

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

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

4.2 Validation formelle

Formalisation de la validation

Le [jj/mm/aaaa], le [poste du responsable de traitement] de [nom de l'organisme] valide le PIA du traitement [nom du PIA], au vu du PIA mené, en sa qualité de responsable du traitement.

Le traitement a pour finalité de [rappel de la finalité du traitement].

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]

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Analyse d'impact relative à la protection des données

Privacy Impact Assessment (PIA)

LES BASES DE CONNAISSANCES



CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Édition février 2018

Table des matières

Avant-propos **1**
1 Bases de connaissances utiles à l'étude **2**
1.1 Typologie de données à caractère personnel 2
1.2 Typologie de supports de données 2
1.3 Typologie de sources de risques 3
1.4 Échelle et règles pour estimer la gravité 3
1.5 Échelle et règles pour estimer la vraisemblance 5
1.6 Menaces qui peuvent mener à un accès illégitime à des données 6
1.7 Menaces qui peuvent mener à une modification non désirées de données 7
1.8 Menaces qui peuvent mener à une disparition de données 8
1.9 Échelles pour le plan d'action 9
2 Anonymisation **10**
3 Archivage **11**
4 Chiffrement **13**
4.1 Mesures génériques 13
4.2 Spécificités pour un chiffrement symétrique 13
4.3 Spécificités pour un chiffrement asymétrique (ou à clé publique) 14
4.4 Spécificités pour le chiffrement de matériels 15
4.5 Spécificités pour le chiffrement de bases de données 15
4.6 Spécificités pour le chiffrement de partitions ou de conteneurs 15
4.7 Spécificités pour le chiffrement de fichiers isolés 16
4.8 Spécificités pour le chiffrement de courriers électroniques 16
4.9 Spécificités pour le chiffrement d'un canal de communication 16
5 Cloisonnement des données (par rapport au reste du système d'information) **17**
6 Contrôle d'accès physique **18**
7 Contrôle d'intégrité **20**
7.1 Mesures génériques 20
7.2 Spécificités pour une fonction de hachage 20
7.3 Spécificités pour un code d'authentification de message 21
7.4 Spécificités pour une fonction de signature électronique 21
8 Contrôle des accès logiques **23**
8.1 Gérer les privilèges des utilisateurs sur les données 23
8.2 Authentifier les personnes désirant accéder aux données 24
8.3 Spécificités pour une authentification par certificat électronique 25

8.4 Gérer les authentifiants....26
9 Durées de conservation : limitées....28
10 Eloignement des sources de risques....30
11 Exercice des droits de limitation du traitement et d'opposition 31
11.1 Mesures génériques....31
11.2 Spécificités pour un traitement par téléphone....32
11.3 Spécificités pour un traitement par formulaire électronique....32
11.4 Spécificités pour un traitement par courrier électronique....32
11.5 Spécificités pour un traitement par un objet connecté ou une application mobile....33
11.6 Spécificités pour des recherches sur des prélèvements biologiques identifiants (i.e. l'ADN) 33
12 Exercice des droits de rectification et d'effacement....34
12.1 Mesures génériques....34
12.2 Spécificités pour la publicité ciblée en ligne....35
13 Exercice des droits d'accès et à la portabilité....36
13.1 Mesures génériques....36
13.2 Spécificités pour l'accès aux dossiers médicaux....37
14 Finalités : déterminées, explicites et légitimes....38
15 Fondement : licéité du traitement, interdiction du détournement de finalité....39
16 Formalités préalables.... 41
17 Gestion des incidents et des violations de données....42
18 Gestion des personnels....44
19 Gestion des postes de travail....45
19.1 Mesures génériques....45
19.2 Spécificités pour les postes nomades....48
19.3 Spécificités pour les téléphones mobiles / *smartphones*....48
20 Gestion des projets....50
20.1 Mesures génériques....50
20.2 Spécificités pour les acquisitions de logiciels (achats, développements, etc.)....50
21 Gestion des risques....52
22 Information des personnes concernées (traitement loyal et transparent).... 55
22.1 Mesures génériques....55
22.2 Spécificités pour les salariés d'un organisme....56
22.3 Spécificités pour une collecte de données via un site Internet....57
22.4 Spécificités pour une collecte de données via un objet connecté ou une application mobile 57
22.5 Spécificités pour une collecte de données par téléphone....57
22.6 Spécificités pour une collecte de données via un formulaire....58
22.7 Spécificités pour l'utilisation de techniques de publicité ciblée....58

22.8 Spécificités pour la mise à jour d'un traitement existant....58
23 Lutte contre les logiciels malveillants....59
24 Maintenance....60
24.1 Mesures génériques.... 60
24.2 Spécificités pour les postes de travail (ordinateurs fixes et mobiles, *smartphones*, tablettes) 60
24.3 Spécificités pour les supports de stockage.... 61
24.4 Spécificités pour les imprimantes et copieurs multifonctions.... 61
25 Minimisation des données : adéquates, pertinentes et limitées....62
25.1 Minimisation de la collecte....62
25.2 Minimisation des données elles-mêmes....63
26 Organisation....66
27 Politique (gestion des règles)....68
28 Protection contre les sources de risques non humaines....69
29 Qualité des données : exactes et tenues à jour....71
30 Recueil du consentement.... 72
30.1 Mesures génériques....72
30.2 Spécificités pour les données relevant de l'article 8 de la loi informatique et libertés....73
30.3 Spécificités pour la collecte de données via un site Internet....73
30.4 Spécificités pour la collecte de données via des cookies....74
30.5 Spécificités pour une collecte de données via un objet connecté ou une application mobile 74
30.6 Spécificités pour la géolocalisation via un smartphone....75
30.7 Spécificités pour l'utilisation de techniques de publicité ciblée....75
30.8 Spécificités pour des recherches sur des prélèvements biologiques identifiants (i.e. l'ADN) 76
31 Relations avec les tiers.... 77
31.1 Mesures génériques....77
31.2 Spécificités pour les tiers prestataires de service travaillant dans les locaux de l'organisme 77
31.3 Spécificités pour les tiers destinataires....78
31.4 Spécificités pour les tiers autorisés....78
32 Sauvegardes.... 79
33 Sous-traitance : identifiée et contractualisée.... 81
33.1 Mesures génériques....81
33.2 Spécificités pour les sous-traitants (hébergeur, mainteneur, administrateur, prestataires spécialisés...) hors fournisseurs de services de *cloud computing*.... 81
33.3 Spécificités pour les fournisseurs de services de *cloud computing*....82
34 Supervision....83
35 Surveillance....84

35.1 Mesures génériques....84
35.2 Spécificités pour un poste client....85
35.3 Spécificités pour un pare-feu....86
35.4 Spécificités pour un équipement réseau....86
35.5 Spécificités pour un serveur....86
36 Sécurité de l'exploitation....87
37 Sécurité des canaux informatiques (réseaux)....89
37.1 Mesures génériques....89
37.2 Spécificités pour les connexions aux équipements actifs du réseau....91
37.3 Spécificités pour les outils de prise de main à distance....91
37.4 Spécificités pour les postes nomades ou se connectant à distance....91
37.5 Spécificités pour les interfaces sans fil (Wifi, Bluetooth, infrarouge, 4G, etc.)....92
37.6 Spécificités pour le Wifi....92
37.7 Spécificités pour le Bluetooth....93
37.8 Spécificités pour l'infrarouge....93
37.9 Spécificités pour les réseaux de téléphonie mobile (2G, 3G ou 4G, etc.)....93
37.10 Spécificités pour la navigation sur Internet....93
37.11 Spécificités pour le transfert de fichiers....94
37.12 Spécificités pour le fax....94
37.13 Spécificités pour l'ADSL/Fibre....94
37.14 Spécificités pour la messagerie électronique....94
37.15 Spécificités pour les messageries instantanées....95
38 Sécurité des documents papier....96
38.1 Marquer les documents contenant des données....96
38.2 Réduire les vulnérabilités des documents papier....97
38.3 Réduire les vulnérabilités des canaux papier....97
39 Sécurité des matériels....99
39.1 Mesures génériques....99
39.2 Spécificités pour les postes de travail....100
39.3 Spécificités pour les postes nomades....100
39.4 Spécificités pour les supports amovibles....101
39.5 Spécificités pour les imprimantes et copieurs multifonctions....102
40 Sécurité des sites web....103
41 Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne....103
42 Traçabilité (journalisation)....105

Avant-propos

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

Ils sont téléchargeables sur le site de la CNIL :







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

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

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

1 Bases de connaissances utiles à l'étude

1.1 Typologie de données à caractère personnel

Les catégories de données sont généralement les suivantes :

Types de données	Catégories de données
DCP courantes	État-civil, identité, données d'identification
	Vie personnelle (habitudes de vie, situation familiale, hors données sensibles ou dangereuses...)
	Vie professionnelle (CV, scolarité formation professionnelle, distinctions...)
	Informations d'ordre économique et financier (revenus, situation financière, situation fiscale...)
	Données de connexion (adresses IP, journaux d'événements...)
	Données de localisation (déplacements, données GPS, GSM...)
DCP perçues comme sensibles	Numéro de sécurité sociale (NIR)
	Données biométriques
	Données bancaires
DCP sensibles au sens de la [Loi-I&L][1]	Opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, données de santé, origine raciales ou ethniques, relatives à la santé ou à la vie sexuelle
	Infractions, condamnations, mesures de sécurité

Notes

- Les supports des données peuvent être regroupés en ensembles cohérents.

1.2 Typologie de supports de données

Les supports de données sont les composants du système d'information sur lesquels reposent les données à caractère personnel :

Types de supports de données		Exemples
Systèmes informatiques	Matériels et supports de données électroniques	Ordinateurs, relais de communication, clés USB, disques durs
	Logiciels	Systèmes d'exploitation, messagerie, bases de données, applications métier
	Canaux informatiques	Câbles, WiFi, fibre optique
Organisations	Personnes	Utilisateurs, administrateurs informatiques, décideurs
	Supports papier	Impressions, photocopies, documents manuscrits
	Canaux de transmission papier	Envoi postal, circuit de validation

Notes

- Il convient de choisir le niveau de détail le plus approprié au sujet de l'étude.
- Les solutions de sécurité (produits, procédures, mesures...) ne sont pas des supports de données : il s'agit de mesures destinées à traiter les risques.

[1] Voir notamment les articles 8 et 9 de la [Loi-I&L] et l'article 8 de la [Directive-95-46].

1.3 Typologie de sources de risques

Le tableau suivant présente des exemples de sources de risques :

Types de sources de risques	Exemples
Sources humaines internes	Salariés, administrateurs informatiques, stagiaires, dirigeants
Sources humaines externes	Destinataires des DCP, tiers autorisés[2], prestataires, pirates informatiques, visiteurs, anciens employés, militants, concurrents, clients, personnels d'entretien, maintenance, délinquant, syndicats, journalistes, organisations non gouvernementales, organisations criminelles, organisations sous le contrôle d'un État étranger, organisations terroristes, activités industrielles environnantes
Sources non humaines	Codes malveillants d'origine inconnue (virus, vers...), eau (canalisations, cours d'eau...), matières inflammables, corrosives ou explosives, catastrophes naturelles, épidémies, animaux

1.4 Échelle et règles pour estimer la gravité

La gravité représente l'ampleur d'un risque. Elle est essentiellement estimée au regard de la hauteur des impacts potentiels sur les personnes concernées, compte tenu des mesures existantes, prévues ou complémentaires (qu'il convient de mentionner en tant que justification).

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[3]	Exemples d'impacts matériels[4]	Exemples d'impacts moraux[5]
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] Par exemple, des autorités publiques et auxiliaires de justice peuvent demander communication de certaines données quand la loi les y autorise expressément.
[3] Préjudice d'agrément, d'esthétique ou économique lié à l'intégrité physique.
[4] Perte subie ou gain manqué concernant le patrimoine des personnes.
[5] Souffrance physique ou morale, préjudice esthétique ou d'agrément.

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels[3]	Exemples d'impacts matériels[4]	Exemples d'impacts moraux[5]
2. Limitée	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	- Affection physique mineure (ex. : maladie bénigne suite au non respect de contre-indications) - Absence de prise en charge causant un préjudice minime mais réel (ex : handicap) - Diffamation donnant lieu à des représailles physiques ou psychiques	- Paiements non prévus (ex. : amendes attribuées de manière erronée), frais supplémentaires (ex. : agios, frais d'avocat), défauts de paiement - Refus d'accès à des services administratifs ou prestations commerciales - Opportunités de confort perdues (ex. : annulation de loisirs, d'achats, de vacances, fermeture d'un compte en ligne) - Promotion professionnelle manquée - Compte à des services en ligne bloqué (ex. : jeux, administration) - Réception de courriers ciblés non sollicités susceptible de nuire à la réputation des personnes concernées - Élévation de coûts (ex. : augmentation du prix d'assurance) - Données non mises à jour (ex. : poste antérieurement occupé) - Traitement de données erronées créant par exemple des dysfonctionnements de comptes (bancaires, clients, auprès d'organismes sociaux, etc.) - Publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel (ex : publicité grossesse, traitement pharmaceutique) - Profilage imprécis ou abusif	- Refus de continuer à utiliser les systèmes d'information (whistleblowing, réseaux sociaux) - Affection psychologique mineure mais objective (diffamation, réputation) - Difficultés relationnelles avec l'entourage personnel ou professionnel (ex. : image, réputation ternie, perte de reconnaissance) - Sentiment d'atteinte à la vie privée sans préjudice irrémédiable - Intimidation sur les réseaux sociaux
3. Importante	Les personnes concernées pourraient connaître 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	- 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

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels[3]	Exemples d'impacts matériels[4]	Exemples d'impacts moraux[5]
			- Perte de données clientèle	
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)

On retient la valeur dont la description correspond le mieux aux impacts potentiels identifiés, en comparant les impacts identifiés dans le contexte considéré avec les impacts génériques de l'échelle.

Elle peut être augmentée ou diminuée en fonction d'autres facteurs, tels que les suivants :

- le caractère identifiant des données ;
- la nature des sources de risques ;
- le nombre d'interconnexions (notamment avec l'étranger) ;
- le nombre de destinataires (ce qui facilite la corrélation de données initialement séparées).

1.5 Échelle et règles pour estimer la vraisemblance

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

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).

On retient la valeur dont la description correspond le mieux aux vulnérabilités des supports et aux sources de risques identifiés.

Elle peut être augmentée ou diminuée en fonction d'autres facteurs, tels que les suivants :

- une ouverture sur Internet ou un système fermé ;
- des échanges de données avec l'étranger ou non ;
- des interconnexions avec d'autres systèmes ou aucune interconnexion ;
- l'hétérogénéité ou l'homogénéité du système ;
- la variabilité ou la stabilité du système ;
- l'image de l'organisme.

1.6 Menaces qui peuvent mener à un accès illégitime à des données

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

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

1.7 Menaces qui peuvent mener à une modification non désirées de données

Critères touché	Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
I	Matériels	Modifiés	Ajout d'un matériel incompatible menant à un dysfonctionnement, retrait d'un matériel indispensable au fonctionnement correct d'une application	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions) via des connecteurs (ports, slots), permet de désactiver des éléments (port USB)
I	Logiciels	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
I	Logiciels	Modifiés	Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre	Modifiable (améliorable, paramétrable), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes), ne fonctionne pas correctement ou conformément aux attentes
I	Canaux informatiques	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)
I	Personnes	Surchargées	Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences	Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail, compétences inappropriées à la fonction Incapacité à s'adapter au changement
I	Personnes	Détournées	Influence (rumeur, désinformation)	Influençable (naïf, crédule, obtus)
I	Documents papier	Modifiés	Modification de chiffres dans un dossier, remplacement d'un document par un faux	Falsifiable (support papier au contenu modifiable)
I	Canaux papier	Modifiés	Modification d'une note à l'insu du rédacteur, changement d'un parapheur par un autre, envoi multiple de courriers contradictoires	Permet d'altérer les documents communiqués, seule ressource de transmission pour le canal, permet la modification du circuit papier

1.8 Menaces qui peuvent mener à une disparition de données

Critères touché	Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
D	Matériels	Utilisés de manière inadaptée	Stockage de fichiers personnels, utilisation à des fins personnelles	Utilisable en dehors de l'usage prévu
D	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
D	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)
D	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)
D	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)
D	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
D	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
D	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
D	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)
D	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)
D	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)
D	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

Critères touché	Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
D	Canaux informatiques	Perdus	Vol de câbles de transmission en cuivre	Attractif (valeur marchande des câbles), transportable (léger, dissimulable), peu visible (oubliable, insignifiant, peu remarquable)
D	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
D	Personnes	Détériorées	Accident du travail, maladie professionnelle, autre blessure ou maladie, décès, affection neurologique, psychologique ou psychiatrique	Limites physiques, psychologiques ou mentales
D	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
D	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)
D	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
D	Documents papier	Perdus	Vol de documents, perte de dossiers lors d'un déménagement, mise au rebut	Portable
D	Canaux papier	Surchargés	Surcharge de courriers, surcharge d'un processus de validation	Existence de limites quantitatives ou qualitatives
D	Canaux papier	Détériorés	Coupure du flux suite à une réorganisation, blocage du courrier du fait d'une grève	Instable, unique
D	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)
D	Canaux papier	Perdus	Réorganisation supprimant un processus, disparition d'un transporteur de documents, vacance de postes	Utilité non reconnue

1.9 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	Trimestre	Année	3 ans
Avancement	Non démarré	En cours	Terminé

2 Anonymisation

Objectifs : faire perdre le caractère identifiant des données à caractère personnel.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Déterminer ce qui doit être anonymisé selon le contexte, la forme de stockage des données (champs d'une base de données, extraits de textes, etc.) et les risques identifiés.
- Anonymiser de manière irréversible ce qui doit l'être, selon la forme des données à anonymiser (base de données, documents textuels, etc.) et les risques identifiés.
- Si ce qui doit être anonymisé ne peut l'être de manière irréversible, choisir les outils (suppression partielle, chiffrement, hachage, hachage à clé, index, etc.) qui satisfont le mieux possible les besoins fonctionnels.

3 Archivage

Objectifs : définir l'ensemble des modalités de conservation et gestion d'archives électroniques contenant des données à caractère personnel destinées à garantir leur valeur, notamment juridique, pendant toute la durée nécessaire (versement, stockage, migration, accessibilité, élimination, politique d'archivage, protection de la confidentialité, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Vérifier que les processus de gestion des archives sont définis.
  - ♦ *Recommandations : distinguer les processus de versement, stockage, gestion des données descriptives, consultation/communication et administration (relation avec les services producteurs, veille technologique et juridique, projets d'évolution et migration des supports et des formats).*
- Vérifier que les rôles en matière d'archivage sont identifiés.
  - ♦ *Recommandations : distinguer les services producteurs, services versants, autorités d'archivage (responsables de la conservation), services contrôleurs (exerçant le contrôle scientifique et technique sur les archives publiques).*
- Vérifier que les mesures prises permettent de garantir, si besoin, l'identification et l'authentification de l'origine des archives, l'intégrité des archives, l'intelligibilité et la lisibilité des archives, la durée de conservation des archives, la traçabilité des opérations effectuées sur les archives (versement, consultation, migration, élimination, etc.), la disponibilité et l'accessibilité des archives, les compléter si ce n'est pas le cas.
  - ♦ *Recommandations : mettre en œuvre des modalités d'accès spécifiques aux données archivées, chiffrer les archives et prévoir de les re-chiffrer de manière sécurisée avec de nouvelles clés avant la fin de vie des clés de chiffrement, prévoir le changement des supports obsolètes des données, choisir un mode opératoire de destruction des archives garantissant que l'intégralité a été détruite?*
- Déterminer les moyens de protection de la confidentialité des données archivées selon les risques identifiés.
  - ♦ *Recommandations : chiffrer systématiquement les données sensibles (données sensibles au sens de l'article 8 et les données relevant de l'article 9 de la loi informatique et libertés) archivées.*
- Vérifier que les autorités d'archivage disposent d'une politique d'archivage (PA).
  - ♦ *Recommandations : le document de PA devrait formaliser les contraintes juridiques, fonctionnelles, opérationnelles et techniques à respecter par les différents acteurs afin que l'archivage électronique mis en place puisse être considéré comme fiable et pérenne.*
- Vérifier qu'il existe une déclaration des pratiques d'archivage (DPA).
  - ♦ *Recommandations : le document de DPA devrait décrire tous les moyens mis en œuvre pour atteindre les objectifs fixés dans la PA.*

Outillage / Pour aller plus loin

- Voir le guide ANSSI Archivage à venir et la norme NF-42-013.
- Voir le site des archives de France.

4 Chiffrement

4.1 Mesures génériques

Objectifs : rendre les données à caractère personnel incompréhensibles à toute personne non autorisée à y avoir accès (chiffrement symétrique ou asymétrique, utilisation d'algorithmes publics réputés forts, certificat d'authentification, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Déterminer ce qui doit être chiffré (un disque dur entier, une partition, un conteneur , certains fichiers, des données d'une base de données, un canal de communication, etc.) selon la forme de stockage des données, les risques identifiés et les performances exigées .
- Choisir le type de chiffrement (symétrique ou asymétrique) selon le contexte et les risques identifiés.
- Recourir à des solutions de chiffrement basées sur des algorithmes publics réputés forts.
    - ♦ *Recommandations : employer des outils (dispositifs de protection des clés privées, module de chiffrement et module de déchiffrement) certifiés, qualifiés ou faisant l'objet d'une certification de sécurité de premier niveau par l'agence nationale de la sécurité des systèmes d'information au niveau correspondant à la robustesse attendue.*
- Mettre en place des mesures pour garantir la disponibilité, l'intégrité et la confidentialité des éléments permettant de récupérer des secrets perdus (mots de passe administrateurs, CD de recouvrement, etc.).

Outillage / Pour aller plus loin

- Voir les exigences relatives à la fonction « Confidentialité » du référentiel général de sécurité (RGS).

4.2 Spécificités pour un chiffrement symétrique

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- N'employer une clé que pour un seul usage.
- Choisir un mécanisme reconnu par les organisations compétentes.
    - ♦ *Recommandations : employer des mécanismes conformes au RGS tels que l'algorithme AES , employer une taille de blocs traités au moins égale à 128 bits, un mode opératoire de chiffrement non déterministe (tel qu'un mécanisme CBC avec un vecteur d'initialisation aléatoire), des clés cryptographiques de longueur conforme à la durée d'utilisation prévue (par*

exemple, au moins 128 bits pour une confidentialité assurée jusqu'en 2020) et qui ne soient pas des clés faibles, etc.

- Formaliser la manière dont les clés vont être gérées.
  - ♦ *Recommandations : rédiger une procédure.*

4.3 Spécificités pour un chiffrement asymétrique (ou à clé publique)

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- N'employer une bi-clé que pour un seul usage.
- Choisir un mécanisme reconnu par les organisations compétentes et qui dispose d'une preuve de sécurité.
  - ♦ *Recommandations : employer des mécanismes conformes au RGS tels que RSAES-OAEP, employer des clés cryptographiques de longueur conforme à la durée d'utilisation prévue (par exemple, au moins 128 bits pour une confidentialité assurée jusqu'en 2020).*
- Générer les clés conformément au RGS.
  - ♦ *Recommandations : avoir recours à un prestataire de service de certification électronique (PSCE) référencé conforme au RGS dans sa version 1.0 pour un usage de chiffrement.*
- Mettre en place des mécanismes de vérification des certificats électroniques.
  - ♦ *Recommandations : lors de la réception d'un certificat électronique, vérifier au minimum que le certificat contient une indication d'usage conforme à ce qui est attendu, qu'il est valide et non révoqué, et qu'il a une chaîne de certification correcte à tous les niveaux.*
- Protéger la sécurité de la génération et de l'utilisation des clés en cohérence avec leur niveau dans la hiérarchie des clés.
  - ♦ *Recommandations : le stockage des clés des utilisateurs est protégé (règles restrictives de droits d'accès, mot de passe, carte à puce à code, etc.), la génération et l'utilisation des clés racines d'une infrastructure de gestion des clés (celles qui vont être utilisées pour signer les autres clés) font l'objet de mesures de sécurité renforcée (ex. : obligation de réunir plusieurs détenteurs d'une partie des secrets pour utiliser les clés, stockage dans un coffre-fort), etc.*
- Formaliser la manière dont les clés vont être gérées.
  - ♦ *Recommandations : élaborer une « politique de certification » qui précise les responsabilités, l'identification et l'authentification, les exigences opérationnelles dans le cycle de vie des certificats, les mesures de sécurité non techniques et techniques, les profils des certificats et listes de révocation, les audits de conformité et autres évaluations.*

4.4 Spécificités pour le chiffrement de matériels

Objectifs : rendre les données inintelligibles à toute personne non autorisée à y avoir accès pour réduire les risques liés à la récupération d'un matériel (poste de travail, serveur, support amovible, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer les données au niveau matériel (surface du disque dur) ou au niveau du système d'exploitation (chiffrement d'une partition ou d'un conteneur).
  - ♦ *Recommandations : utiliser des équipements chiffrables tels que des disques durs avec une technologie SED , ou des logiciels tels que dm-crypt sous Linux, FileVault sous MacOS, VeraCrypt sous Windows.*
- Privilégier les dispositifs ne stockant pas les clés sur le matériel à chiffrer sauf à ce que celui ci mette en œuvre un dispositif de stockage sécurisé (par exemple une puce TPM pour les ordinateurs portables).

4.5 Spécificités pour le chiffrement de bases de données

Objectifs : rendre les données inintelligibles à toute personne non autorisée à y avoir accès pour réduire les risques liés au vol du serveur, à un accès physique illégitime au poste de travail ou au serveur et à un accès direct aux données du serveur par un administrateur .

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Selon les risques identifiés, chiffrer l'espace de stockage (au niveau matériel, du système d'exploitation ou de la base de données) afin de se protéger d'un vol physique, de la donnée elle-même (chiffrement par l'application) afin de garantir la confidentialité de certaines données vis à vis des administrateurs eux-mêmes. Le chiffrement par la base de données peut dans le cas d'équipes informatiques cloisonnées permettre de rendre les données uniquement accessibles des administrateurs de base de données sans que les administrateurs système y aient accès.

4.6 Spécificités pour le chiffrement de partitions ou de conteneurs

Objectifs : rendre les données inintelligibles à toute personne non autorisée à y avoir accès pour réduire les risques liés à la récupération d'un matériel (poste de travail, serveur, support amovible, etc.), un accès physique illégitime à un poste de travail ou au serveur et un accès direct aux données du serveur par un administrateur.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer les données au niveau du système d'exploitation (chiffrement d'une partition, d'un répertoire ou d'un fichier) ou à l'aide d'un logiciel spécialisé (chiffrement d'un conteneur).
  - ♦ *Recommandations : utiliser des logiciels tels que VeraCrypt ou Zed!.*

4.7 Spécificités pour le chiffrement de fichiers isolés

Objectifs : rendre les données inintelligibles à toute personne non autorisée à y avoir accès pour réduire les risques liés au vol d'un poste de travail ou du serveur, un accès physique illégitime à un poste de travail ou au serveur et un accès direct aux données du serveur par un administrateur.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer les fichiers stockés ou les pièces à joindre à des courriers électroniques.
  - ♦ *Recommandations : utiliser des logiciels tels que ZoneCentral, ceux utilisant la librairie Security BOX Crypto 6.0, ou encore AxCrypt ou Gnu Privacy Guard (GPG). A défaut, utiliser au moins un outil de compression qui permet de chiffrer avec mot de passe, tel que 7-Zip qui permet le chiffrement AES, ou bien recourir à une solution matérielle telle qu'une carte Bull Trustway PCI cryptographic card, etc.*

4.8 Spécificités pour le chiffrement de courriers électroniques

Objectifs : rendre les données contenues dans des courriers électroniques inintelligibles à toute personne non autorisée pour réduire les risques liés à l'interception de messages électroniques.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer les messages électroniques.
  - ♦ *Recommandations : utiliser des logiciels tels que Gnu Privacy Guard (GPG).*

4.9 Spécificités pour le chiffrement d'un canal de communication

Objectifs : rendre les données inintelligibles à toute personne non autorisée à y avoir accès pour réduire les risques liés à l'interception de flux de données.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer le canal de communication entre un serveur authentifié et un client distant.
  - ♦ *Recommandations : utiliser un certificat d'authentification de serveur conforme au RGS et le protocole TLS (anciennement SSL) dans ces dernières versions (penser à exiger d'entrer un mot de passe pour utiliser la clé privée et à protéger l'accès à celle-ci par des droits d'accès très restrictifs), ou bien SSH pour mettre en place un tunnel sécurisé (VPN), ou encore des solutions de chiffrement IP (VPN-IPSec), etc.*

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

Objectifs : réduire la possibilité de corréler des données à caractère personnel et de provoquer une violation de l'ensemble des données (identifier les données propres à chaque métier, les séparer logiquement, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Identifier les seules données utiles à chaque processus métier.
  - ♦ *Recommandations : prévoir un accès des personnes aux seules données dont elles ont besoin. Par exemple, le service statistiques n'a pas accès aux noms et prénoms.*
- Séparer logiquement les données utiles à chaque processus.
  - ♦ *Recommandations : gérer des droits d'accès différenciés selon les processus métiers (gestion de la paie, gestion des congés, gestion de l'avancement de carrière, etc.), disposer d'un environnement informatique dédié pour les systèmes traitant des données les plus sensibles, etc.*
- Vérifier de manière régulière que les données sont bien cloisonnées, et que des destinataires ou des interconnexions n'ont pas été ajoutés.

6 Contrôle d'accès physique

Objectifs : limiter les risques que des personnes non autorisées n'accèdent physiquement aux données à caractère personnel (liste des personnes autorisées, authentification des collaborateurs et des visisteurs, trace des accès, alerte en cas d'effraction, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Distinguer les zones des bâtiments selon les risques.
  - ♦ *Recommandations : délimiter une zone ouverte au public lorsqu'il y a une obligation fonctionnelle d'accueil (comptoir d'accueil, salle d'attente ou de réunion, etc.), une zone réservée au service (zone à accès contrôlé correspondant aux bureaux où sont traitées les données), et une zone de sécurité (elle héberge les serveurs, les stations d'administration du réseau, les éléments actifs du réseau ou certaines ressources sensibles telles que des équipements d'alimentation et de distribution d'énergie, ou des équipements réseau et de téléphonie).*
- Tenir à jour une liste des personnes (visiteurs, employés, employés habilités, stagiaires, prestataires, etc.) autorisées à pénétrer dans chaque zone.
  - ♦ *Recommandations : réexaminer régulièrement les droits d'accès aux zones de sécurité, les supprimer si nécessaire.*
- Choisir des moyens d'authentification des collaborateurs proportionnels aux risques selon chaque zone.
  - ♦ *Recommandations : si les risques ne sont pas élevés, une personne à l'accueil peut suffire pour reconnaître les collaborateurs, alors que s'ils sont plus élevés (zone réservée ou de sécurité), l'usage d'un portillon ou d'un autre moyen de contrôle d'accès avec un badge de proximité comportant la photographie d'identité du porteur et/ou un numéro d'identification personnel est conseillé, le badge devant être porté de manière visible.*
- Choisir des moyens d'authentification des visiteurs (personnes venant en réunion, prestataires externes, auditeurs, etc.) proportionnels aux risques selon chaque zone.
  - ♦ *Recommandations : si les risques ne sont pas élevés, l'authentification peut ne pas être nécessaire ; en revanche, si les risques sont élevés, il convient de mettre en place un accueil des visiteurs externes dans une grille horaire prédéfinie, de vérifier leur pièce d'identité, puis de leur fournir un badge spécifique qui ne fonctionnera que pendant la durée de leur visite.*
- Déterminer les actions à entreprendre en cas d'échec de l'authentification (impossible de vérifier une identité, défaut d'habilitation à pénétrer dans une zone sécurisée, etc.).
  - ♦ *Recommandations : refuser l'accès au visiteur, prévenir la personne en charge de la sécurité, etc.*
- Conserver une trace des accès après en avoir informé les personnes concernées.

- ♦ *Recommandations : enregistrer l'identité, la date et l'heure de l'entrée, ainsi que la date et l'heure de la sortie des visiteurs, tenir à jour un journal des accès des trois derniers mois au plus.*

- Faire accompagner les visiteurs, en dehors des zones d'accueil du public (depuis leur entrée, pendant leur visite et jusqu'à leur sortie des locaux) par une personne appartenant à l'organisme.
- Protéger les zones les plus sensibles de manière proportionnelle aux risques.
  - ♦ *Recommandations : mettre en place une porte verrouillée, un digicode ou un vidéophone, renouveler régulièrement les moyens d'accès (code des digicodes), identifier la zone avec une signalétique claire, visible et compréhensible par tout public, sécuriser les ouvrants (barreaux aux fenêtres pour les locaux situés au rez-de-chaussée ou bas étages, porte renforcée avec digicode).*
- Installer un dispositif permettant d'être alerté en cas d'effraction.
  - ♦ *Recommandations : équiper les ouvrants de systèmes de détection des ouvertures et de détection d'effraction faisant remonter les alertes de manière centralisée (gardiennage local, prestations externalisées, etc.) notamment dans les zones de sécurité, surveiller les zones les plus sensibles à l'aide d'un dispositif de vidéosurveillance.*

Outillage / Pour aller plus loin

- Prévoir les moyens de ralentir les personnes qui auraient pénétré dans une zone dont l'accès leur est interdit, ainsi que les moyens d'intervention dans de telles situations, de telle sorte que le délai d'intervention soit inférieur au temps qu'il faut aux personnes non autorisées pour sortir de la zone.

7 Contrôle d'intégrité

7.1 Mesures génériques

Objectifs : être alerté en cas de modification non désirée ou de disparition de données à caractère personnel (fonction de hachage, code d'authentification de message, signature électronique, prévenir les injections SQL, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Identifier les données dont l'intégrité doit être contrôlée selon les risques identifiés.
- Choisir un moyen de contrôler l'intégrité selon le contexte, les risques appréciés et la robustesse attendue.
    - ♦ *Recommandations : utiliser une fonction de hachage pour générer une empreinte (hash) des données afin de traiter les risques liés aux erreurs, appliquer un code d'authentification de messages (MAC) afin de traiter les risques liés aux erreurs et à la modification par toute personne ignorant la clé, appliquer une fonction de signature électronique afin de traiter les risques liés aux erreurs et à la modification par toute personne autre que le signataire, etc.*
- Définir le moment auquel la fonction est appliquée et celui où le contrôle doit être effectué selon le déroulement du processus métier.
    - ♦ *Recommandations : si l'on veut contrôler l'intégrité de données à chaque utilisation, une empreinte de chaque donnée peut être réalisée à la saisie, une autre empreinte peut être réalisée à chaque affichage, et une alerte visuelle peut apparaître si elles ne correspondent pas (auquel cas on pourra restaurer les données si elles ont été préalablement sauvegardées), etc.*
- Lorsque les données sont envoyées dans une base de données, il est nécessaire de mettre en place des mesures d'analyse permettant de prévenir les attaques par injection SQL ou de scripts.
    - ♦ *Recommandations : empêcher la saisie de n'importe quelle donnée (caractère spéciaux, commandes SQL, etc.), filtrer ou encoder les données avant leur enregistrement, limiter le volume des données pouvant être saisi.*

7.2 Spécificités pour une fonction de hachage

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Utiliser un mécanisme reconnu par les organisations compétentes.
    - ♦ *Recommandations : utiliser une fonction de hachage conforme au référentiel général de sécurité (RGS) telle que SHA-256 pour calculer une empreinte sur les données et la transmettre (par un canal différent ou après l'avoir signée électroniquement) afin que l'intégrité des données soit vérifiée au moment de*

leur réception dans le cas d'un envoi par courrier électronique, ou bien la stocker de manière sécurisée afin que le contrôle d'intégrité puisse être réalisé lors de leur utilisation dans le cas de sauvegardes, d'archivage ou simplement de stockage, etc.

7.3 Spécificités pour un code d'authentification de message

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

• Choisir un mécanisme reconnu par les organisations compétentes et qui dispose d'une preuve de sécurité.

♦ *Recommandations : utiliser un algorithme de calcul de code d'authentification de message conforme au RGS tel que le CBC-MAC « retail » utilisant l'AES comme mécanisme de chiffrement par bloc et deux clés distinctes (une pour la chaîne CBC et l'autre pour le surchiffrement dit « retail »).*

7.4 Spécificités pour une fonction de signature électronique

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- N'employer une bi-clé que pour un seul usage.
- Recourir à des solutions de signature basées sur des algorithmes publics réputés forts.
  - ♦ *Recommandations : employer des outils (dispositifs de création de signature, application de création de signature et module de vérification de signature) certifiés, qualifiés ou faisant l'objet d'une certification de sécurité de premier niveau par l'agence nationale de la sécurité des systèmes d'information (ANSSI), au niveau correspondant à la robustesse attendue.*
- Choisir un mécanisme reconnu par les organisations compétentes et qui dispose d'une preuve de sécurité.
  - ♦ *Recommandations : employer des mécanismes conforme au RGS tels que RSA-SSA-PSS, ou bien ECDSA en utilisant l'une des courbes P-256, P-384, P-521, B-283, B-409 ou B-571, etc.*
- Générer les clés conformément au RGS.
  - ♦ *Recommandations : avoir recours à un prestataire de service de certification électronique référencé comme conforme au RGS dans sa version 2 pour un usage de signature.*
- Mettre en place des mécanismes de vérification des certificats électroniques.
  - ♦ *Recommandations : lors de la réception d'un certificat électronique, vérifier au minimum que le certificat contient une indication d'usage conforme à ce qui est attendu, qu'il est valide et non révoqué, et qu'il a une chaîne de certification qui est correcte à tous les niveaux.*

- Protéger la sécurité de la génération et de l'utilisation des clés en cohérence avec leur niveau dans la hiérarchie des clés.
- Formaliser la manière dont les clés vont être gérées.
    - ♦ *Recommandations : élaborer une « politique de certification » qui précise les responsabilités, l'identification et l'authentification, les exigences opérationnelles dans le cycle de vie des certificats, les mesures de sécurité non techniques et techniques, les profils des certificats et listes de révocation, les audits de conformité et autres évaluations, etc.*

Outillage / Pour aller plus loin

- Voir les exigences relatives à la fonction « Signature électronique » du RGS.

Notes

- Dans le cas de l'utilisation d'une carte à puce comme dispositif de création de signature, il est recommandé d'utiliser un lecteur de carte à puce avec PIN-pad intégré permettant de saisir son code d'activation et de le vérifier sans que celui-ci ne transite via l'ordinateur ou la borne d'accès publique utilisés.

8 Contrôle des accès logiques

Objectifs : limiter les risques que des personnes non autorisées accèdent aux données à caractère personnel par voie électronique (gestion de profils utilisateurs, mécanisme d'authentification, politique de mots de passe, etc.).

8.1 Gérer les privilèges des utilisateurs sur les données

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Gérer les profils d'utilisateurs en séparant les tâches et les domaines de responsabilité, de préférence de manière centralisée, afin de limiter l'accès aux données aux seuls utilisateurs habilités, en appliquant les principes du besoin d'en connaître et du moindre privilège.
    - ♦ *Recommandations : définir un ou plusieurs profils d'utilisateurs de façon centralisée (avec des privilèges spécifiques d'utilisation des fonctionnalités, de création, d'accès, de modification, de transfert et de suppression des données), faire rattacher chaque personne à un des profils définis en début de contrat ou de changement d'emploi.*
- Identifier toute personne ayant un accès légitime aux données (employés, contractants et autres tiers) par un identifiant unique.
- Dans le cas où l'utilisation d'identifiants génériques ou partagés est incontournable, obtenir une validation de la hiérarchie et mettre en œuvre des moyens de traçabilité de l'utilisation de ce type d'identifiant.
    - ♦ *Recommandations : renseigner une fiche de présence, remplir une main courante des actions, etc.*
- Limiter l'accès aux outils et interfaces d'administration aux personnes habilitées.
- Limiter l'utilisation des comptes permettant de disposer de privilèges élevés aux opérations qui le nécessitent.
- Limiter l'utilisation des comptes « administrateurs » au service en charge de l'informatique et ce, uniquement pour les actions d'administration qui le nécessitent.
    - ♦ *Recommandations : les comptes « administrateurs » ne doivent être réservés qu'aux tâches d'administrations ; les administrateurs doivent utiliser un compte ayant des droits plus limités lorsqu'ils effectuent des actions plus exposées (ex : lecture de mail, internet, etc.).*
- Chaque compte, et d'autant plus s'il a des privilèges élevés (ex : compte administrateur), doit avoir un mot de passe propre.
    - ♦ *Recommandations : les comptes « administrateurs » doivent être, autant que possible, individuels et requérir un mot de passe personnel.*
- Journaliser les informations liées à l'utilisation des privilèges (voir la page Traçabilité (journalisation)).
- Réaliser une revue annuelle des privilèges afin d'identifier et de supprimer les comptes non utilisés, et de réaligner les privilèges sur les fonctions de chaque utilisateur.

- Retirer les droits des employés, contractants et autres tiers dès lors qu'ils ne sont plus habilités à accéder à un local ou à une ressource ou à la fin de leur contrat, et les ajuster en cas de changement de poste. Pour les personnes ayant un compte temporaire
(stagiaire, prestataire...), configurer une date d'expiration à la création du compte.

8.2 Authentifier les personnes désirant accéder aux données

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Choisir un moyen d'authentification pour les ouvertures de session, adapté au contexte, au niveau des risques et à la robustesse attendue.
    - ♦ *Recommandations : si les risques ne sont pas élevés, l'usage d'un mot de passe est envisageable ; en revanche, si les risques sont plus élevés, il convient d'utiliser un boitier électronique générateur de mots de passe à usage unique OTP (token), sans oublier de changer les mots de passe d'activation par défaut, ou sur l'envoi d'une partie du mot de passe par SMS, une carte avec code PIN, un certificat électronique ou tout autre moyen d'authentification forte.*
- Interdire que les mots de passe utilisés apparaissent en clair dans les programmes, fichiers, scripts, traces ou fichiers journaux, ou à l'écran lors de leur saisie.
- Déterminer les actions à entreprendre en cas d'échec de l'authentification.
    - ♦ *Recommandations : bloquer le compte après cinq échecs de connexion, accroître le temps d'attente entre deux tentatives de connexion?*
    - ♦ *Journaliser les informations liées aux accès logiques (voir la page Traçabilité (journalisation)).*
- Limiter l'authentification par identifiants et mots de passe au contrôle de l'accès au poste de travail (déverrouillage uniquement).
- Authentifier le poste de travail auprès du système d'information distant (serveurs) à l'aide de mécanismes cryptographiques.

Notes

- Un mécanisme d'authentification forte requiert au minimum deux facteurs d'authentification distincts parmi ce que l'on sait (ex. : mot de passe), ce que l'on a (ex. : certificat électronique, carte à puce, etc.) et une caractéristique qui nous est propre (ex. : empreinte digitale ou autre caractéristique biométrique).
- Dans un environnement informatique peu sécurisé (ex. : postes partagés), prévoir une deuxième authentification pour l'accès à l'application contenant des données.
- La loi informatique et libertés subordonne le recours à des dispositifs biométriques à l'autorisation préalable de la CNIL. D'une manière générale, la CNIL recommande l'utilisation de biométrie sans traces (contour de la main, réseaux veineux, etc.) ou l'enregistrement des empreintes digitales dans un support individuel.

Outillage / Pour aller plus loin

- Voir les exigences relatives à la fonction « Authentification » du référentiel général de sécurité (RGS).
- Voir le document CNIL Empreinte sur les dispositifs basés sur l'empreinte digitale.
- Des solutions de contrôle d'accès au réseau (NAC ? *Network Access Control*) sont préconisées dès lors qu'un nombre important d'utilisateurs doit être géré.

8.3 Spécificités pour une authentification par certificat électronique

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- N'employer une clé que pour un seul usage .
- Recourir à des solutions d'authentification basées sur des algorithmes publics réputés forts.
    - ♦ *Recommandations : employer des outils (dispositif d'authentification, application d'authentification et module de vérification d'authentification) certifiés, qualifiés ou faisant l'objet d'une certification de sécurité de premier niveau par l'agence nationale de la sécurité des systèmes d'information, au niveau correspondant à la robustesse attendue.*
- Choisir un mécanisme reconnu par les organisations compétentes et qui dispose d'une preuve de sécurité.
    - ♦ *Recommandations : employer des mécanismes conforme au RGS tels que RSA-SSA-PSS, ou bien ECDSA en utilisant l'une des courbes P-256, P-384, P521, B-283, B-409 ou B-571*
- Générer les clés conformément au RGS.
    - ♦ *Recommandations : avoir recours à un prestataire de service de certification électronique référencé comme conforme au RGS dans sa version 1.0 pour un usage d'authentification.*
- Mettre en place des mécanismes de vérification des certificats électroniques.
    - ♦ *Recommandations : lors de la réception d'un certificat électronique, vérifier au minimum que le certificat contient une indication d'usage conforme à ce qui est attendu, qu'il est valide et non révoqué, et qu'il a une chaîne de certification qui est correcte à tous les niveaux.*
- Protéger la sécurité de la génération et de l'utilisation des clés en cohérence avec leur niveau dans la hiérarchie des clés.
- Formaliser la manière dont les clés vont être gérées.
    - ♦ *Recommandations : élaborer une « politique de certification » qui précise les responsabilités, l'identification et l'authentification, les exigences opérationnelles dans le cycle de vie des certificats, les mesures de sécurité non techniques et techniques, les profils des certificats et listes de révocation, les audits de conformité et autres évaluations?.*

8.4 Gérer les authentifiants

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Adopter une politique de mots de passe, la mettre en œuvre et la contrôler automatiquement dans la mesure où les applications et les ressources le permettent, et y sensibiliser les utilisateurs.
    - ♦ *Recommandations : les mots de passe sont constitués de huit caractères minimum, ils doivent être renouvelés au moindre doute de compromission et éventuellement de manière périodique (tous les six mois ou une fois par an), ils comprennent au minimum trois types de caractères parmi les quatre types de caractères (majuscules, minuscules, chiffres et caractères spéciaux) ; lors d'un changement de mot de passe, il est interdit de réutiliser un des cinq derniers mots de passe ; éviter d'utiliser le même mot de passe pour des accès différents ; éviter de choisir des mots de passe ayant un lien avec soi (nom, date de naissance?)?*
- Adopter une politique spécifique de mots de passe pour les administrateurs, la mettre en œuvre et la contrôler automatiquement dans la mesure où les applications et les ressources le permettent, et y sensibiliser les administrateurs.
    - ♦ *Recommandations : les mots de passe doivent respecter la Délibération n° 2017-012 du 19 janvier 2017. En outre, il convient de ne jamais utiliser le même mot de passe pour des accès différents, d'éviter de choisir des mots de passe ayant un lien avec soi (nom, date de naissance?), de configurer les logiciels pour qu'ils ne retiennent jamais les mots de passe, de définir un nombre de tentatives maximum au-delà duquel une alerte est émise et l'authentification est bloquée (temporairement ou jusqu'à ce qu'elle soit manuellement débloquée).*
- Modifier immédiatement après installation d'une application ou d'un système les mots de passe par défaut.
- Créer chaque compte utilisateur avec un mot de passe initial aléatoire unique, le transmettre de manière sécurisée à l'utilisateur, par exemple en utilisant deux canaux séparés (papier et autres) ou une « case à gratter », et le contraindre à le modifier lors de sa première connexion et lorsque qu'un nouveau mot de passe lui est fourni (par exemple en cas d'oubli).
- Stocker les informations d'authentification (mots de passe d'accès aux systèmes d'information, clés privés liées aux certificats électroniques?) de façon à être accessibles uniquement par des utilisateurs autorisés.
    - ♦ *Recommandations : limiter les droits d'accès (lecture, écriture, etc.) au strict minimum, chiffrer les fichiers dans lesquels on note ses mots de passe.* Placer les authentifiants permettant l'administration des ressources des systèmes informatiques sous séquestre et les tenir à jour, dans un coffre ou une armoire fermé à clé.
- Dans le cas où de nombreux mots de passe ou secrets (clés privées, certificats, etc.) doivent être utilisés, mettre en place une solution d'authentification centralisée, de mots de passe à usage unique ou de coffres-forts sécurisés.

- *Recommandations : contrôle d'accès constitué au minimum par un mot de passe maître robuste, stockage sécurisé des mots de passe garantissant que les mots de passe protégés ne peuvent être récupérés sans connaissance du secret (chiffrement, masquage, etc.), affichage sécurisé des mots de passe (masquage des mots de passe dans les boîtes de connexion, etc.), résistance aux attaques (déchiffrement, force brute, rejeu, etc.), fermeture ou blocage automatique (après une certaine durée, lors de la mise en veille sécurisée, etc.).*
- En cas de départ d'un administrateur disposant de privilèges sur des composants des systèmes informatiques, désactiver les comptes individuels dont il disposait et changer les éventuels mots de passe d'administration dont il avait connaissance (mots de passe des comptes fonctionnels, comptes génériques ou comptes de service utilisés dans le cadre des fonctions de l'administrateur, etc.).

Notes

- Des moyens mnémotechniques permettent de créer des mots de passe complexes, par exemple :
  - en ne conservant que les premières lettres des mots d'une phrase ;
  - en mettant une majuscule si le mot est un nom (ex : Chef) ;
  - en gardant des signes de ponctuation (ex : ') ;
  - en exprimant les nombres à l'aide des chiffres de 0 à 9 (ex : Un ->1).
- *Ainsi, la phrase « un Chef d'Entreprise averti en vaut deux » correspond au mot de passe 1Cd'Eaev2.*
- Il convient d'être vigilant à supprimer toute donnée d'authentification à caractère biométrique intervenant dans des dispositifs de contrôle d'accès.

Outillage / Pour aller plus loin

- Voir la note CERTA MotsDePasse.

9 Durées de conservation : limitées

Objectifs : être conforme aux articles 6 et 36 de la loi informatique et libertés et l'article 5.1(e) du règlement général sur la protection des données (RGPD) ; réduire la gravité des risques en s'assurant que les données à caractère personnel ne seront pas conservées plus que nécessaire.

Bonnes pratiques

- Définir, pour chaque catégorie de données, des durées de conservation limitées dans le temps et en adéquation avec la finalité du traitement et/ou des contraintes légales.
  - ♦ *Recommandations : définir des durées de conservation adaptées à chaque type de données traitées ; distinguer les données courantes, les données archivées (dont l'accès sera restreint aux seuls acteurs concernés), les traces fonctionnelles, les journaux techniques (logs).*
- Vérifier que le traitement permet de détecter la fin de la durée de conservation (mettre en place un mécanisme automatique basé sur la date de création des données ou de leur dernier usage).
  - ♦ *Recommandations : le traitement affiche la date a laquelle la donnée va ou doit être supprimée.*
- Vérifier que le traitement permet de supprimer les données en fin de durée de conservation et que le moyen choisi pour les supprimer est approprié aux risques qui pèsent sur les libertés et la vie privée des personnes concernées.
  - ♦ *Recommandations :* La suppression d'une donnée arrivée au terme de sa durée de conservation ne peut être logique (indicateur d'état indiquant que la donnée est effacée mais permettant toujours de la lire directement dans la base de données).
  - ♦ Une bonne pratique peut consister à définir une durée de conservation intermédiaire permettant de ne rendre les données accessible de tous que pendant une certaine période puis passé un certain délai uniquement par une liste restreinte de personne (Ex. la donnée reste accessible de tous pendant 6 mois puis uniquement par le service contentieux ensuite).
- Une fois la durée de conservation atteinte, sous réserve de l'archivage intermédiaire pour les données qui le nécessitent, supprimer les données sans délai (voir également la page Minimisation des données : adéquates, pertinentes et limitées).
  - ♦ *Recommandations : développer une fonctionnalité automatisée qui archive/efface les données dont la durée de conservation est atteinte, y compris pour les traces et journaux techniques. Dans le cas ou l'effacement est effectué manuellement, l'outil doit mettre à disposition de l'utilisateur une fonctionnalité d'effacement par lot.*
  - ♦ *Le cas échéant, lorsque le contexte le permet, la durée de conservation d'une donnée peut être prolongée par l'utilisateur. Par défaut, la donnée est effacée au terme initialement prévu.*

Notes

- D'une manière générale, la finalité des traitements ne justifie pas de conserver des données en prévisions d'actions de Police ou en Justice au-delà de ce qui est prévu conformément à la loi informatique et libertés et au RGPD. Toutefois, dans certains secteurs, il est obligatoire de conserver certaines données pendant une durée déterminée (opérateurs de télécommunication, passagers de vols aériens, etc.).
- 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.

10 Eloignement des sources de risques

Objectifs : éviter que des sources de risques, humaines ou non humaines, portent atteinte aux données à caractère personnel (produits dangereux, zones géographiques dangereuses, transfert des données en dehors de l'UE, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Placer les produits dangereux (inflammables, combustibles, corrosifs, explosifs, aérosols, humides, etc.) dans des lieux de stockage appropriés et éloignés de ceux où sont traitées des données.
- Éviter les zones géographiques dangereuses (zones inondables, proximité d'aéroports, zones d'industries chimiques, zones sismiques, zones volcaniques, etc.).
- Ne pas stocker les données dans un état étranger sauf s'il existe des garanties permettant d'assurer un niveau de protection des données suffisant : si le transfert a lieu vers un pays reconnu comme "adéquat" par la Commission européenne - Canada, Suisse, Argentine, territoires de Guernesey, Jersey et Isle de Man ? ou si des clauses contractuelles types, approuvées par la Commission européenne, sont signées entre deux entreprises ou si des règles internes d'entreprises (*Binding Corporate Rules* - BCR) sont adoptées au sein d'un groupe ou si dans le cas d'un transfert vers les États-Unis, l'entreprise destinataire a adhéré au *Privacy Shield* ou si l'une des exceptions prévues par l'article 69 de la loi Informatique et libertés est invoquée. Dans tous les cas, le responsable du traitement reste responsable de la sécurité des données stockées et doit s'assurer du niveau de sécurité du stockage.

11 Exercice des droits de limitation du traitement et d'opposition

11.1 Mesures génériques

Objectifs : être conforme à l'article 38 de la loi informatique et libertés et les articles 18 et 21 du règlement général sur la protection des données (RGPD) : garantir aux personnes la possibilité de s'opposer à l'utilisation de données à caractère personnel qui les concernent ; permettre à l'utilisateur d'exiger le « gel » du traitement de ses données, comme mesure conservatoire le temps d'en vérifier la légitimité, par exemple ; vérifier que le traitement ne fait pas l'objet d'une exception mentionnée à l'article 38 de la loi informatique et libertés (obligation légale, exclusion dans l'acte portant création du traitement) et à l'article 21 du RGPD (motifs légitimes et impérieux, droits en justice, intérêt public) interdisant à la personne de s'opposer au traitement.

Bonnes pratiques

- Déterminer les moyens pratiques qui vont être mis en œuvre pour permettre l'exercice du droit d'opposition. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais.
- S'assurer que le droit d'opposition pourra toujours s'exercer et que les données collectées et traitées permettent effectivement l'exercice du droit d'opposition.
    - ♦ *Recommandations : étudier les cas où les moyens pratiques choisis ne sont plus opérationnels et déterminer des solutions de secours le cas échéant.*
- S'assurer que « l'intéressé est mis en mesure d'exprimer son choix avant la validation définitive de ses réponses », conformément à l'article 96 du décret informatique et libertés.
    - ♦ *Recommandations : vérifier que le droit d'opposition peut s'exercer avant la validation définitive des réponses des personnes concernées ou avant la fin de la collecte.*
- Vérifier que les demandes d'exercice du droit d'opposition faites sur place permettent de s'assurer de l'identité des demandeurs et des personnes qu'ils peuvent mandater.
- Vérifier que les demandes d'exercice du droit d'opposition faites par voie postale sont signées et accompagnées de la photocopie d'un titre d'identité (qui ne devrait pas être conservée sauf en cas de besoin de conserver une preuve) et qu'elles précisent l'adresse à laquelle doit parvenir la réponse.
- Vérifier que les demandes d'exercice du droit d'opposition faites par voie électronique (en utilisant un canal chiffré si la transmission se fait via Internet) sont accompagnées d'un titre d'identité numérisé (qui ne devrait pas être conservé sauf en cas de besoin de conservation d'une preuve, et ce, en noir et blanc, en faible définition et sous la forme d'un fichier chiffré).

- S'assurer que le motif légitime des personnes exerçant leur droit d'opposition est fourni et apprécié (sauf dans le cas de la prospection et des traitements ayant pour fin la recherche dans le domaine de la santé relevant du chapitre IX de la loi informatique et libertés, pour lesquels la personne dispose d'un droit d'opposition discrétionnaire).
- S'assurer que tous les destinataires du traitement seront informés des oppositions exercées par des personnes concernées, conformément à l'article 97 du décret informatique et libertés.

Notes

- 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.

11.2 Spécificités pour un traitement par téléphone

Bonnes pratiques

• Prévoir un mécanisme permettant aux personnes concernées de signifier leur opposition à l'aide du téléphone.

♦ *Recommandations : prévoir la possibilité de s'opposer en appuyant sur une touche.*

11.3 Spécificités pour un traitement par formulaire électronique

Bonnes pratiques

• Créer un formulaire, facilement accessible, avec des cases à décocher (dit « *opt-out* ») ou prévoir la possibilité de se désinscrire d'un service (suppression de compte).

11.4 Spécificités pour un traitement par courrier électronique

Bonnes pratiques

- S'assurer que l'expéditeur des messages apparaît très clairement.
- S'assurer que le corps des messages est en rapport avec le sujet des messages.
- Prévoir une opposition en répondant au message ou en cliquant sur un lien permettant de s'opposer. La personne ne doit pas avoir besoin de s'authentifier pour être désinscrite.

11.5 Spécificités pour un traitement par un objet connecté ou une application mobile

Bonnes pratiques

- Proposer des paramètres « Vie privée ».
  - ♦ *Recommandations : inviter l'utilisateur à changer les paramètres par défaut ; rendre ces paramètres accessibles au premier démarrage de l'appareil ou de l'application, et ensuite à tout moment par un menu spécifique.*
- Permettre à l'utilisateur de s'opposer à la collecte de données particulières.
  - ♦ *Recommandations : prévenir l'utilisateur (icône, voyant lumineux) quand l'application fonctionne en arrière plan, quand l'appareil "écoute" avec le micro, quand la localisation est collectée, etc. et lui permettre de s'y opposer.*
- Prendre en compte les utilisateurs mineurs.
  - ♦ *Recommandations : proposer un dispositif de contrôle parental, exclure les enfants de moins de 13 ans de tout traitement de profilage automatisé.*
- Arrêter effectivement toute collecte de données si l'utilisateur retire son consentement.

11.6 Spécificités pour des recherches sur des prélèvements biologiques identifiants (i.e. l'ADN)

Bonnes pratiques

- Si les prélèvements sont conservés pour un traitement ultérieur différent du traitement initial, permettre également aux personnes concernées par cet autre traitement de s'y opposer et ce, sans requérir un motif légitime.

12 Exercice des droits de rectification et d'effacement

12.1 Mesures génériques

Objectifs : être conforme à l'article 40 de la loi informatique et libertés et les articles 16, 17 et 19 du règlement général sur la protection des données (RGPD) ; garantir aux personnes la possibilité de rectifier, compléter, mettre à jour, verrouiller ou supprimer des données à caractère personnel qui les concernent ; vérifier que le traitement ne fait pas l'objet d'une exception mentionnée à l'article 41 de la loi informatique et libertés (sûreté de l'État, défense ou sécurité publique) ou à l'article 17 du RGPD (liberté d'expression et d'information, obligation légale, intérêt public ou d'autorité publique, santé publique, recherche scientifique ou historique ou à des fins statistiques, droits en justice).

Bonnes pratiques

- Déterminer les moyens pratiques qui vont être mis en œuvre pour permettre l'exercice du droit de rectification. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais.
- S'assurer que le droit de rectification pourra toujours s'exercer.
  - ♦ *Recommandations : étudier les cas où les moyens pratiques choisis ne sont plus opérationnels et déterminer des solutions de secours le cas échéant.*
- S'assurer que le droit d'effacement pourra toujours s'exercer.
  - ♦ *Recommandations : fournir des indications claires et des étapes simples pour effacer les données en cas de vente de l'appareil ou avant de le mettre au rebut ; permettre d'effacer les données à distance en cas de vol de l'appareil.*
- S'assurer que l'identité des demandeurs va être vérifiée.
  - ♦ *Recommandations : vérifier que les demandes d'exercice du droit de rectification faites par voie postale sont signées et accompagnées de la photocopie d'un titre d'identité (qui ne devrait pas être conservée sauf en cas de besoin de conserver une preuve), que celles faites par voie électronique (en utilisant un canal chiffré si la transmission est faite via Internet) sont accompagnées d'un titre d'identité numérisé (qui ne devrait pas être conservé sauf en cas de besoin de conserver une preuve, et ce, en noir et blanc, en faible définition et chiffré), et qu'elles précisent l'adresse à laquelle doit parvenir la réponse, vérifier l'identité des demandeurs venant sur place et des personnes qu'ils peuvent mandater ou des héritiers d'une personne décédée, etc.*
- S'assurer que la véracité des rectifications demandées sera vérifiée.
- S'assurer de l'effacement effectif des données à supprimer.
- S'assurer qu'une confirmation sera fournie aux demandeurs.
- S'assurer que les destinataires à qui des données auraient été transmises seront informés des rectifications faites.

- Suite à une demande d'effacement, préciser à l'utilisateur si des données personnelles seront conservées malgré tout (contraintes techniques, obligations légales, etc.)
- Mettre en œuvre le droit à l'oubli pour les mineurs.
    - ♦ *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. Des exceptions 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.*

Outillage / Pour aller plus loin

- Voir les articles 92 à 95 et 99 à 100 du décret informatique et libertés.

Notes

- 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 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.

12.2 Spécificités pour la publicité ciblée en ligne

Bonnes pratiques

• Prévoir un accès par la personne aux centres d'intérêt établis pour son profil et la possibilité de les modifier. L'authentification de la personne peut se faire sur la base des informations utilisées pour accéder à son compte ou sur la base du cookie (ou équivalent) présent sur son poste.

13 Exercice des droits d'accès et à la portabilité

13.1 Mesures génériques

Objectifs : être conforme à l'article 39 de la loi informatique et libertés et les articles 15 et 20 du règlement général sur la protection des données (RGPD) ; garantir aux personnes la possibilité de prendre connaissance des données à caractère personnel qui les concernent ; permettre à l'utilisateur de récupérer, sous une forme aisément réutilisable, les données personnelles qu'il a fournies au traitement afin de les transférer vers un autre service ; vérifier que le traitement ne fait pas l'objet d'une exception mentionnée dans les articles 39 et 41 de la loi informatique et libertés (comme des données traitées pour une finalité de statistiques ou de recherche lorsqu'il n'y a aucun risque d'atteinte à la vie privée des personnes et que les données ne sont conservées seulement le temps nécessaire à ces finalités, pour la sûreté de l'État, la défense ou la sécurité publique) et à l'article 20 du RGPD (pas de portabilité pour les traitements d'intérêt public ou d'autorités publiques, respects des droits et libertés de tiers).

Bonnes pratiques

- Déterminer les moyens pratiques qui vont être mis en œuvre pour permettre l'exercice du droit d'accès. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois (un mois dans le cadre du RGPD) pour des données, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais excédant le coût de la reproduction.
    - ♦ *Recommandations : mettre en place un processus permettant de tenir informés les demandeurs de la prise en compte de leur demande et du traitement nécessaire (par exemple par un courrier postal ou électronique indiquant la prise en compte de la demande et le délai à prévoir pour la réponse). Dans le cas de données archivées, il existe une tolérance au niveau des délais si le responsable de traitement a informé le demandeur de ses difficultés et indiqué un délai de réponse raisonnable.*
- S'assurer que le droit d'accès pourra toujours s'exercer.
    - ♦ *Recommandations : étudier les cas où les moyens pratiques choisis ne sont plus opérationnels et déterminer des solutions de secours le cas échéant.*
- Vérifier que les demandes d'exercice du droit d'accès faites sur place permettent de s'assurer de l'identité des demandeurs et des personnes qu'ils peuvent mandater.
- Vérifier que les demandes d'exercice du droit d'accès faites par voie postale sont signées
  et accompagnées de la photocopie d'un titre d'identité (qui ne devrait pas être conservée sauf en cas de besoin de conserver une preuve) et qu'elles précisent l'adresse à laquelle doit parvenir la réponse.
- Vérifier que les demandes d'exercice du droit d'accès faites par voie électronique (en utilisant un canal chiffré si la transmission se fait via Internet) sont accompagnées d'un titre d'identité numérisé (qui ne devrait pas être conservé sauf en cas de besoin de conservation d'une preuve, et ce, en noir et blanc, en faible définition et sous la forme d'un fichier chiffré).

- S'assurer de la possibilité de fournir toutes les informations qui peuvent être demandées par les personnes concernées, tout en protégeant les données des tiers.

Outillage / Pour aller plus loin

- Voir les articles 92 à 95 et 98 du décret informatique et libertés.
- Voir le guide CNIL-Employeurs.

13.2 Spécificités pour l'accès aux dossiers médicaux

Bonnes pratiques

- Communiquer les informations au plus tard dans les huit jours suivant la demande et dans les deux mois si les informations remontent à plus de cinq ans (à compter de la date à laquelle l'information médicale a été constituée).
- Permettre l'exercice du droit d'accès par les titulaires de l'autorité parentale, pour les mineurs, ou le représentant légal, pour les personnes faisant l'objet d'une mesure de tutelle, conformément à l'article 58 de la loi informatique et libertés.

Outillage / Pour aller plus loin

- Voir le décret-2002-637.

14 Finalités : déterminées, explicites et légitimes

Objectifs : être conforme à l'article 6 de la loi informatique et libertés et à l'article 5.1(b) du règlement général sur la protection des données (RGPD) ; éviter les usages incompatibles et le détournement de finalité.

Bonnes pratiques

- Détailler les finalités de traitement des données et justifier leur légitimité.
- Expliciter les finalités de partage avec des tiers ainsi que les finalités de traitement de données pour l'amélioration du service.
- Expliciter les modalités particulières du traitement, en précisant notamment les croisements de données s'il y a lieu.

15 Fondement : licéité du traitement, interdiction du détournement de finalité

Objectifs : être conforme à l'article 6 du règlement général sur la protection des données (RGPD).

Bonnes pratiques

• Déterminer et justifier le critère de licéité qui s'applique au traitement de données considéré :

- ♦ la personne concernée a consenti 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.

Notes

- 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.
- 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?) qui sera recueilli lors de l'activation du produit.
- 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 ;
- 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.

16 Formalités préalables

Objectifs : respecter les obligations en matière de formalités préalables au traitement des données.

Bonnes pratiques

- Déclarer le traitement auprès de la CNIL préalablement à la mise en œuvre du traitement.
- Vérifier que le traitement de données est effectivement conforme à la finalité déclarée.
- Réaliser une étude d'impact sur la vie privée (EIVP ou PIA) et le faire valider.
- Consulter la CNIL si les risques résiduels sont importants, selon l'article 36 du règlement général sur la protection des données (RGPD).
- Réaliser les autres formalités sectorielles et contractuelles applicables au traitement (par exemple, formalités liées à d'autres codes et règlements, contrat avec une source externe de données, etc.)

Outillage / Pour aller plus loin

- Voir la méthode PIA et les guides PIA de la CNIL.
- Voir les Guidelines sur les DPIA du G29.

17 Gestion des incidents et des violations de données

Objectifs : disposer d'une organisation opérationnelle permettant de détecter et de traiter les événements susceptibles d'affecter les libertés et la vie privée des personnes concernées (définition des responsabilités, plan de réaction, qualifier les violations, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques :

- Définir les rôles et responsabilités des parties prenantes, ainsi que les procédures de remontées d'informations et de réaction, en cas de violation de données.
  - ♦ *Recommandations : formaliser les responsabilités du référent « Informatique et libertés » (CIL, DPO ou équivalent), les interactions avec la CNIL, les personnes concernées, la constitution d'une cellule de crise en cas de sinistre.*
- Établir un annuaire des personnes en charges de gérer les violations de données.
- Élaborer un plan de réaction en cas de violation de données pour chaque risque élevé, le tenir à jour et le tester périodiquement.
  - ♦ *Recommandations : tester le plan au moins une fois tous les deux ans.*
- Permettre de qualifier les violations de données selon leur impact sur les droits et libertés des personnes concernées.
  - ♦ *Recommandations : un simple événement est une violation de données sans conséquence, un incident correspond à une violation de données avec des conséquences isolées, un sinistre à une violation de données avec des conséquences immédiates importantes pour une ou plusieurs personnes, une crise à une violation de données avec des conséquences importantes et à plus long terme sur une ou plusieurs personnes.*
- Traiter les événements selon leur qualification (événement, incident, sinistre, crise, etc.). ♦ *Recommandations*
  - ◊ *s'il s'agit d'un événement, le consigner et avertir le référent « Informatique et libertés » (CIL, DPO ou équivalent) ;*
  - ◊ *s'il s'agit d'un incident, le résoudre en plus et, le cas échéant, notifier les personnes concernées par la violation (la notification d'une violation des données n'est pas nécessaire si la violation ne présente pas un risque élevé pour les droits et libertés des personnes, si le responsable de traitement a prouvé, à la satisfaction de l'autorité compétente, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.) ;*
  - ◊ *s'il s'agit d'un sinistre, déclencher en plus le lancement d'une analyse approfondie ;*
  - ◊ *s'il s'agit d'une crise, déclencher en plus un plan de gestion préalablement établi.*

- Tenir à jour une documentation des violations de données tel que prévu par l'article 33-5 du règlement général sur la protection des données (RGPD).
    - ♦ *Recommandations : consigner le contexte des violations de données, les catégorie de personnes et d'enregistrements concernés, le volume de personnes et d'enregistrement concernés, les effets de la violation, les mesures prises pour y remédier.*
- Étudier la possibilité d'améliorer les mesures de sécurité en fonction des violations de données qui ont eu lieu.

Notes

- Le « Paquet télécom » adopté par le Parlement européen en 2009 et transposé en droit français en 2011 crée une obligation de notifier certaines violations de données à la CNIL. Cette obligation est généralisée à tous les responsables de traitements et pas uniquement les « fournisseurs de services de communications électroniques accessibles au public » par le RGPD.devant entrer en vigueur en mai 2018. Ces textes définissent la forme des notifications :
    - ♦ la notification des personnes concernées, dans le cas où la dite violation engendre un risque élevé pour les droits et libertés des personnes, décrit au minimum la nature de la violation de données et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données;
    - ♦ la notification faite à l'autorité nationale compétente (la CNIL en France) décrit en outre les conséquences de la violation de données à caractère personnel, et les mesures proposées ou prises par le fournisseur pour y remédier. Dans le cadre du RGPD, cette notification est nécessaire dès lors que la violation engendre un risque pour les droits et libertés des personnes.
    - ♦ Cette obligation n'est pas exclusive et n'annule pas les obligations de notification présentes au sein des autres textes nationaux ou européens.
- Il est important d'être en capacité de recueillir, conserver et présenter des preuves lorsqu'une action en justice est engagée suite à un incident.

Outillage / Pour aller plus loin

- Voir la procédure CLUSIF Victime.
- Voir la note CERTA Intrusion.
- Voir la Directive-2009-136.
- Voir les articles 33 et 24 du RGDP.

18 Gestion des personnels

Objectifs : diminuer la possibilité que les caractéristiques des personnes (employés, personnes ne faisant pas partie de l'organisme mais placées sous sa responsabilité) soient exploitées pour porter atteinte aux données (ressources et compétences adéquates, sensibilisation, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Vérifier que les personnes ayant accès aux données et au traitement sont aptes à exercer leur fonction.
  - ♦ *Recommandations : vérifier que les personnes ont des compétences appropriées aux conditions d'exercice de leurs fonctions ou sinon prévoir des formations.*
- S'assurer que les conditions de travail des personnes ayant accès aux données et au traitement sont satisfaisantes.
  - ♦ *Recommandations : veiller à ce que les ressources (capacités de travail et disponibilités) soient suffisantes pour les tâches assignées.*
- Sensibiliser les personnes ayant accès aux données et au traitement aux risques liés à l'exploitation de leurs vulnérabilités.
  - ♦ *Recommandations : expliquer aux personnes que le fait qu'elles soient peu discrètes (loquaces, sans réserve, etc.), routinières (habitudes facilitant l'espionnage récurrent), influençables (naïves, crédules, obtuses, faible estime de soi, faible loyauté, etc.) ou manipulables (vulnérables face à la pression sur elles-mêmes ou leur entourage) peut être utilisé par des personnes mal intentionnées pour porter atteintes aux données.*

Outillage / Pour aller plus loin

- Dans certains cas, il convient également de mettre en œuvre des mesures d'accompagnement du changement (nouveaux services, nouveaux outils, nouvelles méthodes de travail, etc.) pour les personnes ayant accès aux données et au traitement.

19 Gestion des postes de travail

19.1 Mesures génériques

Objectifs : diminuer la possibilité que les caractéristiques des logiciels (systèmes d'exploitation, applications métiers, logiciels bureautiques, paramétrages, etc.) ne soient exploitées pour porter atteinte aux données à caractère personnel (mises à jour, protection physique et des accès, travail sur un espace réseau sauvegardé, contrôleurs d'intégrité, journalisation, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Assurer la mise à disposition et le maintien en conditions opérationnelles et de sécurité des postes de travail des utilisateurs par le service en charge de l'informatique.
- Protéger les postes peu volumineux, donc susceptibles d'être facilement emportés, et notamment les ordinateurs portables, à l'aide d'un câble physique de sécurité, dès que l'utilisateur ne se trouve pas à proximité et que le local n'est pas sécurisé physiquement.
- Récupérer les données, à l'exception des données signalées comme privées ou personnelles, présentes sur un poste préalablement à sa réaffectation à une autre personne.
- Effacer les données présentes sur un poste préalablement à sa réaffectation à une autre personne ou pour les postes partagés.
- Supprimer les données temporaires à chaque reconnexion des postes partagés.
- En cas de compromission d'un poste, rechercher toute trace d'intrusion dans le système afin de détecter si l'attaquant a compromis d'autres éléments.
- Tenir les systèmes et applications à jour (versions, correctifs de sécurité, etc.) ou, lorsque cela est impossible (ex : application uniquement disponible sur un système qui n'est plus maintenu par l'éditeur), isoler la machine et porter une attention particulière aux journaux.
    - ♦ *Recommandations : utiliser des versions maintenues par le constructeur ou un service tiers, mettre les logiciels à jour sans délai en programmant une vérification automatique hebdomadaire, tester les mises à jour avant de les déployer sur l'ensemble du système, s'assurer que les mises à jour soient réversibles en cas d'échec de leur application, vérifier régulièrement que les licences des logiciels sont valables, etc.*
- Documenter les configurations et les mettre à jour à chaque changement notable.

♦ *Recommandations : les modes opératoires liés au renforcement des ressources informatiques sont décrits, les liens nécessaires pour assurer les mises à jour de sécurité lors de l'installation sont identifiés, etc.*

- Limiter les possibilités de détournements d'usages.
    - ♦ *Recommandations : gérer les droits d'accès unitaires selon la règle du « moindre privilège » (éviter notamment d'autoriser l'usage de fonctionnalités*

avancées si ce n'est pas nécessaire), gérer les attributions d'adresses IP publiques ou privées en fonction des besoins effectifs, désactiver ou supprimer les services qui ne sont pas strictement nécessaires, désactiver ou supprimer les comptes inutiles (compte invité, comptes de support éditeur par défaut, etc.), interdire l'accès logique aux ports de diagnostic et de configuration à distance, désactiver l'exécution automatique lors de l'insertion d'un périphérique amovible, démarrer uniquement sur le disque local ou la mémoire locale, etc.

- Protéger les accès.
  - ♦ *Recommandations : protéger la configuration système bas niveau (exemple : BIOS) par mot de passe, changer les mots de passe par défaut, verrouiller l'accès au système par un écran de veille protégé par mot de passe et se déclenchant au bout d'un délai d'inactivité (5 minutes pour les opérations de maintenance, 15 minutes au plus pour une utilisation courante), afficher les dates et heures de la dernière connexion lors de la connexion à un compte, etc.*
- Activer les mesures de protection offertes par le système et les applications.
  - ♦ *Recommandations : activer les mots de passe d'ouverture de session, le parefeu, la mise à jour automatique, la protection contre les programmes malveillants? quand le système d'exploitation le permet ; activer les contrôles d'accès aux applications quand elles en disposent, etc.*
- Interdire le partage de répertoires ou de données localement sur les postes de travail.
- Stocker les données des utilisateurs sur un espace réseau sauvegardé et non sur les postes de travail.
- Dans le cas où des données doivent être stockées en local sur un poste, fournir des moyens de synchronisation ou de sauvegarde aux utilisateurs et les informer sur leur utilisation.
  - ♦ *Recommandations : des espaces individuels sur les serveurs de fichiers avec un plan de classement explicite, des scripts automatiques de copie de dossiers locaux, des outils de synchronisation automatique gérés par le service en charge de l'informatique.*
- Sécuriser la configuration du navigateur Internet.
  - ♦ *Recommandations : la configuration doit inclure la protection des informations nominatives stockées par le navigateur (formulaires, mots de passe, certificats, etc.), l'utilisation d'un mot de passe principal sous Mozilla Firefox, l'impossibilité de stocker des mots de passe en cas de risques élevés, etc.*
- Déployer le navigateur dont la configuration a été sécurisée sur tous postes de travail nécessitant un accès à Internet ou Intranet.
- Limiter le recours à des modules d'extension (plugins), supprimer ceux qui ne sont pas utilisés et tenir à jour ceux qui sont installés.
- Interdire l'exécution des applications téléchargées ne provenant pas de sources sûres.
- Rechercher les vulnérabilités exploitables.

- ♦ *Recommandations : exercer une veille active concernant les vulnérabilités découvertes sur les logiciels utilisés dans le cadre du traitement, utiliser des outils de détection des vulnérabilités (logiciels scanners de vulnérabilités tels que nmap, nikto, etc.), voire des systèmes de détection et prévention des attaques (Host Intrusion Prevention), s'assurer que les principales vulnérabilités sont couvertes, etc.*

- Contrôler l'intégrité du système à l'aide de contrôleurs d'intégrité (qui vérifient l'intégrité de fichiers choisis).
  - ♦ *Recommandations : surveiller de façon permanente les modifications apportées à certains fichiers ou répertoires (utiliser des logiciels tels que Tripwire), contrôler la base de registre et les processus lancés par le système (utiliser des logiciels tels que Spybot), détecter la présence de rootkits (utiliser des logiciels tels que Rootkit Revealer), etc.*
- S'assurer que la taille maximale des journaux d'événements est suffisante, et notamment que les événements les plus anciens ne sont pas supprimés automatiquement si la taille maximale est atteinte.
- Journaliser les événements relatifs aux applications, à la sécurité et au système (voir la page Traçabilité (journalisation)).
  - ♦ *Recommandations : connexions au système (enregistrer l'identifiant, la date et l'heure de leur tentative de connexion, le fait que la connexion ait réussi ou non, ainsi que la date et l'heure de la déconnexion), modification de paramètres de sécurité, de privilèges, de comptes utilisateurs et de groupes, événements système (arrêt / redémarrage de processus système sensibles), accès / modification de données système, échec lors d'un accès à une ressource (fichier système, objet, réseau, etc.), exécution de transactions sensibles, l'application des correctifs de sécurité, actions d'administration et de prise de main à distance, journaux du logiciel antivirus (activation/désactivation, mises à jour, détection de codes malveillants, etc.), etc.*
- Exporter les journaux à l'aide des fonctionnalités de gestion du domaine ou via un client syslog.
- Analyser principalement les heures de connexions et déconnexions, le type de protocole utilisé pour se connecter et le type d'utilisateur qui y a recours, l'adresse IP d'origine de la connexion, les échecs successifs de connexions, les arrêts inopinés d'applications ou de tâches.

Outillage / Pour aller plus loin

- Selon la nature de l'application, il peut être nécessaire d'assurer l'intégrité, la disponibilité et si besoin la confidentialité des logiciels et des codes sources des applications développées en interne, notamment si elles sont rares, novatrices ou ont une grande valeur marchande, par le recours à des signatures du code exécutable garantissant qu'il n'a subi aucune altération. À cet égard, une vérification de signature tout au long de l'exécution (et pas seulement avant l'exécution) rend plus difficile la compromission d'un programme.

19.2 Spécificités pour les postes nomades

Objectifs : réduire les risques liés au format, au caractère attractif et à l'utilisation des postes nomades (PC portables, assistants personnels, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer les données stockées sur les postes nomades.
  - ♦ *Recommandations : chiffrement du disque dur dans sa totalité au niveau matériel, chiffrement du disque dur dans sa totalité à un niveau logique via le système d'exploitation, chiffrement fichier par fichier, création de conteneurs chiffrés, etc.*
- Limiter le stockage de données sur les postes nomades au strict nécessaire, et éventuellement l'interdire lors de déplacement à l'étranger.
- Assurer la disponibilité des données stockées sur les postes nomades.
  - ♦ *Recommandations : les copier dès que possible sur un autre poste, sur un serveur.*
- Purger les données collectées sur le poste nomade sitôt qu'elles ont été introduites dans le système d'information de l'organisme.
- Positionner un filtre de confidentialité sur les écrans des postes nomades dès qu'ils sont utilisés en dehors de l'organisme.

Notes

- De plus en plus d'ordinateurs portables sont équipés d'un dispositif de lecture d'empreinte digitale. La mise en œuvre de tels dispositifs est soumise à l'autorisation de la CNIL.
- Il convient de ne pas désactiver le chiffrement de disque et de veiller à conserver une copie des clés quand le chiffrement est disponible.

Outillage / Pour aller plus loin

- Voir le guide ANSSI Voyageurs pour les voyages à l'étranger.

19.3 Spécificités pour les téléphones mobiles / *smartphones*

Objectifs : réduire les risques liés au format, au caractère attractif et à l'utilisation des téléphones mobiles / *smartphones*.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Configurer les téléphones avant d'être livrés aux utilisateurs.
  - ♦ *Recommandations : il faut que les téléphones soient verrouillés automatiquement après une période d'inactivité (1 à 5 minutes), la carte*

mémoire (microSD) sur laquelle les courriers électroniques sont stockés doit être chiffrée, le verrou distant doit être activé afin de pouvoir effacer le contenu en cas de perte ou de vol, l'installation de nouvelles applications est limitée (si possible).

- Informer les utilisateurs, par exemple sous la forme d'une note accompagnant la livraison, sur l'usage du téléphone, des applications (ex : business mail, Exchange, etc.) et des services fournis, ainsi que sur les règles de sécurité à respecter.
    - ♦ *Recommandations : les utilisateurs ne doivent pas diminuer le niveau de sécurité en modifiant la configuration du téléphone, ils ne doivent pas ouvrir les courriers d'origine inconnue, ils ne doivent pas stocker de fichiers sensibles (en dehors de la lecture des courriers), ils doivent effacer régulièrement le cache et les cookies, ils doivent immédiatement avertir le service en charge de l'informatique en cas d'incident, ils ne doivent pas installer de logiciels sur l'appareil, sauf s'ils proviennent d'une source de confiance (vérifier la réputation avant d'installer ou d'utiliser des applications ou des services) envoyant un contenu qu'ils s'attendent à recevoir.*
- Sécuriser le serveur.
    - ♦ *Recommandations : isoler le serveur du reste du réseau dans une DMZ spécifique ou un VLAN, utiliser un anti-virus à jour, un anti-spyware et un anti-spam, installer immédiatement les mises à jour de sécurité du système d'exploitation, authentifier les appareils par certificat électronique (si possible).*
- Sécuriser la fin de vie de l'appareil.
    - ♦ Recommandations : avant élimination ou recyclage du téléphone, effacer toutes les données et les paramètres, appliquer une procédure approfondie de démantèlement, y compris d'effacement de la mémoire.

Outillage / Pour aller plus loin

- Voir l'article CNIL Smartphones.
- Voir le guide CLUSIF Voix.
- Voir le rapport ENISA Smartphone.
- Des mesures plus rigoureuses peuvent être envisagées si les risques sont jugés trop importants (bloquer les pièces jointes, tracer et vérifier les flux avec une sonde, vérifier l'effectivité du chiffrement, ne pas stocker des données sensibles au niveau local et ne permettent qu'un accès en ligne à des données sensibles à partir d'un smartphone grâce à une application non-mise en cache, ne pas envoyer de fichiers sensibles sur les smartphones par courrier électronique en cas de risques élevés, utiliser un logiciel de chiffrement de confidentialité SMS de bout en bout, définir une liste blanche d'applications utilisables, ré-installer régulièrement une image du disque spécialement préparée et testée.).

20 Gestion des projets

Objectifs : prendre en compte la protection des données à caractère personnel dans tout nouveau traitement (labels de confiance, référentiels, gestion de risques CNIL, formalités CNIL, etc.).

20.1 Mesures génériques

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Utiliser la démarche de gestion des risques de la CNIL dès l'élaboration d'un service ou la conception d'une application.
- Privilégier le recours à des labels de confiance dans les domaines de la SSI et « Informatique et libertés » (procédures, produits, systèmes de management, organismes, personnes, etc.).
    - ♦ *Recommandations : une certification de sécurité de premier niveau, une qualification (au niveau standard, renforcé ou élevé), une certification en vertu du décret n°2002-535 du 18 avril 2002, selon sept niveaux d'assurance croissante, un agrément ou caution (jugeant de l'aptitude à assurer la protection d'informations classifiées de défense ou d'informations sensibles non classifiées de défense), une certification de système de management de la sécurité de l'information ISO-27001, une certification de personne dans le domaine de la SSI*
      (CISSP ? Certified Information Systems Security Professional, CISM ? Certified Information Security Manager, ISO 27001 Lead Auditor, etc.).
- Privilégier le recours à des référentiels éprouvés et reconnus.
    - ♦ *Recommandations : Recourir de préférence à des normes internationales, des guides publiés par des institutions (CNIL, ANSSI, etc.).*
- Effectuer les formalités CNIL avant le lancement d'un nouveau traitement.

Outillage / Pour aller plus loin

- Voir les principes « Adapter la SSI selon les enjeux », « Utiliser des produits et prestataires labellisés pour leur sécurité » et « Des efforts proportionnés aux enjeux SSI » du référentiel général de sécurité (RGS).
- Voir les règles et recommandations relatives aux « Accusé d'enregistrement et accusé de réception » du RGS et les annexes associées.
- Voir les catalogues de produits labellisés par l'ANSSI.
- Voir les guides ANSSI Maturité SSI et ANSSI GISSIP.

20.2 Spécificités pour les acquisitions de logiciels (achats, développements, etc.)

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Vérifier que les développeurs et les mainteneurs disposent des ressources suffisantes pour maîtriser leurs actions.
    - ♦ Recommandations : vérifier l'existence de spécifications claires, d'une documentation adéquate, des compétences suffisantes.
- Privilégier les applications interopérables et ergonomiques.
- Effectuer les développements informatiques dans un environnement informatique distinct de celui de la production
    - ♦ *Recommandations : effectuer les développements sur des ordinateurs différents et dans des salles différentes du système en production.*
- Protéger la disponibilité, l'intégrité et si besoin la confidentialité des codes sources.
- Imposer des formats de saisie et d'enregistrement des données qui minimisent les données collectées.
    - ♦ *Recommandations : s'il s'agit de collecter l'année de naissance d'une personne, le champ du formulaire correspondant ne doit pas permettre la saisie du mois et du jour de naissance (mise en œuvre d'un menu déroulant limitant les choix pour un champ d'un formulaire).*
- S'assurer que les formats de données sont compatibles avec la mise en œuvre d'une durée de conservation.
- Intégrer le contrôle d'accès aux données par des catégories d'utilisateurs au moment du développement.
- Éviter le recours à des zones de texte libre, et si de telles zones sont requises, faire apparaître soit en filigrane, soit comme texte pré-rempli s'effaçant sitôt que l'utilisateur décide d'écrire dans la zone, les mentions suivantes : « Les personnes disposent d'un droit d'accès aux informations contenues dans cette zone de texte. Les informations que vous y inscrivez doivent être PERTINENTES au regard du contexte. Elles ne doivent pas comporter d'appréciation subjective, ni faire apparaître, "directement ou indirectement les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelles de celles-ci" ».
- Interdire l'utilisation de données réelles avant la mise en opération, et les anonymiser si nécessaire.
    - ♦ *Recommandations : anonymiser les données de production lors des tests de recette, effacer de manière sécurisée tout support ayant servi à stocker des données sensibles (voir la page Anonymisation)*
- Vérifier que les logiciels fonctionnent correctement et conformément lors de la recette.

Outillage / Pour aller plus loin

- Voir le référentiel général d'interopérabilité.

21 Gestion des risques

Objectifs : maîtriser les risques que les traitements de l'organisme font peser sur les droits et libertés des personnes concernées (recensement des traitements de données à caractère personnel, des données, des supports, appréciation des risques, déterminer les mesures existantes ou prévues, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Recenser les traitements de données à caractère personnel, automatisés ou non, les données traitées (ex : fichiers client, contrats) et les supports sur lesquels ils reposent :
  - ♦ les matériels (ex : serveur de gestion des ressources humaines, ordinateur portable, CD-ROM) ;
  - ♦ les logiciels (ex : système d'exploitation, logiciel métier) ;
  - ♦ les canaux de communication (ex : fibre optique, Wifi, Internet) ; ♦ les supports papier (ex : document imprimé, photocopie).
- Évaluer la manière dont les principes fondamentaux (information, consentement, droit d'accès...) sont respectés.
- Apprécier les risques de chaque traitement.
  - ♦ Identifier les impacts potentiels (quels pourraient être les conséquences sur les droits et libertés des personnes concernées ?) pour les trois risques suivants :
    - ◊ Accès illégitime à des données (ex : usurpations d'identités consécutives à la divulgation des fiches de paie de l'ensemble des salariés d'une entreprise) ;
    - ◊ modification non désirée de données (ex : accusation à tort d'une personne suite à la modification des journaux d'accès) ;
    - ◊ disparition de données (ex : non détection d'une interaction médicamenteuse du fait de l'impossibilité d'accéder au dossier électronique du patient).
  - ♦ Identifier les sources de risques (qui ou quoi pourrait être à l'origine de chaque risque ?), en prenant en compte :
    - ◊ les sources humaines internes et externes, de manière accidentelle ou délibérée (ex : administrateur informatique, utilisateur, attaquant externe, concurrent) ;
    - ◊ les sources non humaines internes ou externes (ex : eau, matériaux dangereux, virus informatique non ciblé).
  - ♦ Identifier les menaces réalisables (qu'est-ce qui pourrait permettre que chaque risque survienne ?). Ces menaces se réalisent via les supports des données (matériels, logiciels, canaux de communication, supports papier, etc.), qui peuvent être :

- ◊ utilisés de manière inadaptée (ex : abus de droits, erreur de manipulation) ;
- ◊ modifiés (ex : piégeage logiciel ou matériel ? *keylogger*, installation involontaire d'un logiciel malveillant) ;
- ◊ perdus (ex : vol d'un ordinateur portable, perte d'une clé USB) ;
- ◊ observés (ex : d'un écran à l'insu de son utilisateur dans un train, photographie d'un écran, géolocalisation d'un matériel) ;
- ◊ détériorés (ex : vandalisme, dégradation du fait de l'usure naturelle) ;
- ◊ surchargés (ex : unité de stockage pleine, attaque par dénis de service).

♦ Déterminer les mesures existantes ou prévues (techniques et organisationnelles) qui permettent de traiter chaque risque (ex : contrôle d'accès, sauvegardes, traçabilité, sécurité des locaux, chiffrement, anonymisation).

♦ Estimer la gravité et la vraisemblance des trois risques, au regard des éléments précédents, compte tenu des mesures existantes ou prévues (exemple d'échelle utilisable pour l'estimation : négligeable, modérée, importante, maximale).

♦ *Recommandations : le tableau suivant peut être utilisé pour formaliser cette réflexion :*

Risques	Impacts sur les personnes	Principales sources de risques	Principales menaces	Mesures existantes ou prévues	Gravité	Vraisemblance
Accès illégitime à des données						
Modification non désirée de données						
Disparition de données						

- Mettre en œuvre et vérifier les mesures prévues. Si les mesures existantes et prévues sont jugées comme appropriées afin de garantir un niveau de sécurité adapté aux risques, il convient de s'assurer qu'elles soient appliquées et contrôlées.
- Faire réaliser des audits de sécurité périodiques, si possible annuels. Chaque audit devrait donner lieu à un plan d'action dont la mise en œuvre devrait être suivie au plus haut niveau de l'organisme.
- Ajuster la cartographie à chaque évolution majeure et de manière périodique.

♦ *Recommandations : quand un nouveau traitement est créé, et au moins une fois par an au sein d'un comité dédié.*

Outillage / Pour aller plus loin

- Le règlement n°2016/679 du 27 avril 2016 introduit la notion d' « analyse d'impact relative à la protection des données » et précise que celle-ci doit au moins contenir « *une description du traitement et de ses finalités, une évaluation de la nécessité et de la proportionnalité, une appréciation des risques sur les droits et libertés des personnes concernées, et les mesures envisagées pour traiter ces risques et se conformer au règlement* » (cf. article 35.7). La réflexion sur les risques dont il est question dans la présente fiche permet d'alimenter l'analyse d'impact.
- L'emploi d'une véritable méthode permet de disposer d'outils pratiques et d'améliorer l'exhaustivité et la profondeur de l'étude des risques. À cet effet, les guides PIA (*Privacy Impact Assessment*) de la CNIL permettent de mener une analyse d'impact relative à la protection des données.
- L'étude des risques sur la sécurité de l'information peut être menée en même temps que l'étude des risques sur la vie privée. Les approches étant compatibles, il n'est pas difficile de les factoriser.
- L'étude des risques permet de déterminer des mesures techniques et organisationnelles à mettre en place. Il convient donc de prévoir un budget pour leur mise en œuvre .
- Voir le référentiel général de sécurité (RGS).
- Voir la méthode EBIOS.

22 Information des personnes concernées (traitement loyal et transparent)

22.1 Mesures génériques

Objectifs : être conforme à l'article 32 de la loi informatique et libertés et les articles 12, 13 et 14 du règlement général sur la protection des données (RGPD) ; garantir l'information des personnes et donc éviter la collecte de données à leur insu ; vérifier que le traitement ne fait pas l'objet d'une exception ou de conditions particulières mentionnées dans l'article 32 de la loi informatique et libertés (utilisateur des réseaux de communication électronique, statistiques, anonymisation, sûreté de l'État, défense, sécurité publique, exécution de condamnations pénales, mesures de sûreté, prévention, recherche, constatation ou poursuite d'infractions pénales).

Bonnes pratiques

- Déterminer et justifier les moyens pratiques qui vont être mis en œuvre pour informer les personnes concernées, ou justifier de l'impossibilité de leur mise en œuvre :
  - ♦ présentation des conditions d'utilisation/confidentialité ;
  - ♦ possibilité d'accéder aux conditions d'utilisation/confidentialité ;
  - ♦ 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.) ;
  - ♦ présentation détaillée des données personnelles collectées ;
  - ♦ présentation des éventuels accès à des identifiants de l'appareil, en précisant si ces identifiants sont communiqués à des tiers ;
  - ♦ présentation des droits de la personne concernée (retrait du consentement, suppression de données, etc.) ;
  - ♦ information sur le mode de stockage sécurisé des données, notamment en cas d'externalisation ;
  - ♦ modalités de contact de l'entreprise (identité et coordonnées) pour les questions de confidentialité ;
  - ♦ le cas échéant, information de la personne concernée 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 entreprises tierces.
- S'assurer que l'information sera réalisée de manière complète, claire et adaptée au public visé, en fonction de la nature des données et des moyens pratiques choisis.

- ♦ *Recommandations : formuler l'information dans un langage compréhensible du point de vue d'une personne non formée aux technologies informatiques ou de l'Internet.*

- S'assurer que l'information sera réalisée au plus tard au moment où seront collectées les données.
- S'assurer que la collecte ne puisse pas être effectuée sans information.
  - ♦ *Recommandations : déterminer des solutions alternatives au cas où les moyens pratiques choisis ne seraient plus opérationnels.*
- Si possible, prévoir un moyen de prouver que l'information a été faite.
  - ♦ *Recommandations : placer l'information sur un panneau que tous les employés ont forcément vu, faire signer un émargement ou un document...*

Notes

- L'information doit être individuelle (échange verbal, fenêtre pop-up?), mais peut être collective (note, affichette dans un local?) si le responsable de traitement est certain que toutes les personnes concernées auront accès facilement au moyen d'information.
- L'information doit porter sur l'identité du responsable de traitement, la finalité du traitement, le caractère obligatoire ou facultatif des informations collectées, les conséquences en cas de défaut de réponse, les destinataires de ces informations, les droits et la personne auprès de qui les faire valoir, et les transmissions envisagées.
- Attention : dans le cas de transmission de données à des sociétés tierces 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.

Outillage / Pour aller plus loin

- Voir l'article 32 de la loi informatique et libertés et les articles 12, 13 et 14 du RGPD pour le contenu de l'information, les exceptions et les conditions particulières.
- Voir les modèles de mentions légales sur le site de la CNIL (https://www.cnil.fr/fr/modeles/mention).
-

22.2 Spécificités pour les salariés d'un organisme

Bonnes pratiques

- Obtenir l'avis préalable des institutions représentatives du personnel dans les cas prévus par le Code du travail.

- Utiliser le moyen le plus approprié à la culture de l'organisme.
    - ♦ *Recommandations : affichage, note interne, courrier électronique, formulaire spécifique, contrat de travail, règlement intérieur, charte informatique?*

22.3 Spécificités pour une collecte de données via un site Internet

Bonnes pratiques

- Faire figurer une information à destination des internautes directement ou facilement accessible.
    - ♦ *Recommandations : afficher ou rendre accessible l'information sur la page d'accueil, ou au sein de la rubrique du site ou du service consulté traitant du respect de la vie privée?*

22.4 Spécificités pour une collecte de données via un objet connecté ou une application mobile

Bonnes pratiques

- Faire figurer une information à destination des utilisateurs directement ou facilement accessible.
    - ♦ *Recommandations : afficher un message au premier démarrage de l'objet ou de l'application mobile, et rendre l'information accessible ensuite par un menu spécifique ; placer un « QR Code » d'information sur l'objet s'il n'a pas d'écran.*
- Informer l'utilisateur si l'application est susceptible d'accéder à des identifiants de l'appareil, en précisant s'ils sont communiqués à des tiers.
- Informer l'utilisateur si l'application est susceptible de fonctionner en arrière-plan.
- Présenter à l'utilisateur les protections d'accès à l'appareil.

22.5 Spécificités pour une collecte de données par téléphone

Bonnes pratiques

- Délivrer un message automatique avant que la conversation soit engagée, précisant notamment les droits des personnes, et le cas échéant, les finalités de l'enregistrement de la conversation (formation, enquête sur la qualité du service rendu, etc.), en leur offrant la possibilité de s'opposer à l'enregistrement (pour motif légitime).
- Mettre en place des moyens permettant l'authentification de l'appelant (ex : par une information connue seulement de l'organisme et de la personne concernée).

22.6 Spécificités pour une collecte de données via un formulaire

Bonnes pratiques

• Placer la mention appropriée sur le formulaire avec une typographie identique au reste du document.

22.7 Spécificités pour l'utilisation de techniques de publicité ciblée

Bonnes pratiques

- Rendre accessible l'information des internautes de manière à ce qu'elle soit parfaitement visible et lisible.
- Informer les internautes sur les différentes formes de publicité ciblée auxquelles ils sont susceptibles d'être exposés via le service qu'ils consultent et les divers procédés utilisés, les catégories d'informations traitées aux fins d'adapter le contenu publicitaire et, en tant que de besoin, les informations non recueillies, leurs possibilités pour consentir à l'affichage de publicités comportementales ou personnalisées. L'information et le recueil du consentement doivent être effectués avant tout stockage d'information ou obtention de l'accès à des informations déjà stockées dans l'équipement terminal.

Outillage / Pour aller plus loin

- Voir l'avis G29-Publicité.

22.8 Spécificités pour la mise à jour d'un traitement existant

Bonnes pratiques

• Informer plus particulièrement sur les nouveautés du traitement (nouvelles finalités, nouveaux destinataires?).

23 Lutte contre les logiciels malveillants

Objectifs : protéger les accès vers des réseaux publics (Internet) ou non maîtrisés (partenaires), ainsi que les postes de travail et les serveurs contre les codes malveillants qui pourraient affecter la sécurité des données à caractère personnel (antivirus, firewall, proxy, anti-spyware, remontée des événements de sécurité, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Installer un antivirus sur les serveurs et postes de travail et le configurer
  - ♦ *Recommandations : assurer une analyse en temps réel du système selon les règles définies par le service en charge de l'informatique, l'utilisateur ne doit pas pouvoir désactiver l'antivirus de son poste ni modifier ses paramètres, réaliser une analyse complète des disques locaux au moins de façon hebdomadaire et automatique tout en perturbant au minimum le fonctionnement du service (par exemple en heures creuses ou en limitant la charge système allouée à l'analyse, ou en heures non ouvrées, etc.).*
- Tenir les logiciels antivirus à jour.
  - ♦ *Recommandations : déployer automatiquement les mises à jour des bases antivirales et des moteurs d'antivirus sur les serveurs et les postes de travail de manière régulière et pouvoir réaliser des mises à jour d'urgence.*
- Mettre en œuvre des mesures de filtrage permettant de filtrer les flux entrants/sortants du réseau (firewall, proxy, etc.).
- Faire remonter les événements de sécurité de l'antivirus sur un serveur centralisé pour analyse statistique et gestion des problèmes a posteriori (dans le but de détecter un serveur infecté, un virus détecté et non éradiqué par l'antivirus, etc.).
- Installer un programme de lutte contre les logiciels espions (anti-spyware) sur les postes de travail, le configurer et le tenir à jour.

Outillage / Pour aller plus loin

- Voir la note rappel sur les virus et chevaux de Troie du CERTA.
- Voir la note rappel sur les virus de messageriedu CERTA.

24 Maintenance

24.1 Mesures génériques

Objectifs : limiter la vraisemblance des menaces liées aux opérations de maintenance sur les matériels et logiciels (contrat de sous-traitance, télémaintenance, accord de l'utilisateur, effacement des données, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Encadrer par un contrat de sous-traitance la réalisation des opérations de maintenance lorsqu'elles sont effectuées par des prestataires (voir la page Relations avec les tiers).
- Enregistrer toutes les opérations de maintenance dans une main courante.
- Encadrer les opérations de télémaintenance.
    - ♦ *Recommandations : utiliser systématiquement des canaux de communications chiffrés, utiliser des mots de passe ou des clés d'authentification robustes, journaliser les accès (voir la page Traçabilité (journalisation)).*
- Chiffrer ou effacer les données présentes sur les matériels (poste de travail fixe ou nomades, serveurs, etc.) envoyés en maintenance externe. En cas d'impossibilité déposer les supports de stockage de l'équipement avant l'envoi en maintenance ou gérer la maintenance en interne.

24.2 Spécificités pour les postes de travail (ordinateurs fixes et mobiles, *smartphones*, tablettes)

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Lors des opérations de maintenance nécessitant une prise en main à distance sur un poste de travail, ne réaliser l'opération qu'après avoir obtenu l'accord de l'utilisateur, et lui indiquer à l'écran si la prise en main est effective.
- Lorsqu'une opération de maintenance nécessite une intervention physique sur un poste de travail contenant des données sensibles au sens de l'article 8 de la loi informatique et libertés et des données relevant de l'article 9 de la même loi, supprimer les données pendant la maintenance.
- Configurer les téléphones via avant de les remettre aux utilisateurs.
    - ♦ *Recommandations : il faut que les téléphones soient verrouillés automatiquement après une période d'inactivité (1 à 5 minutes), la carte mémoire (microSD) sur laquelle les courriers électroniques sont stockés doit être chiffrée, le verrou distant doit être activé afin de pouvoir effacer le contenu en cas de perte ou de vol, l'installation de nouvelles applications est*

limitée (si possible), et l'ensemble de ces mesures doit être gérée par un système de gestion de flotte permettant de forcer l'application de ces règles.

- Informer les utilisateurs, par exemple sous la forme d'une note accompagnant la livraison, sur l'usage du téléphone, des applications (ex : *business mail, Exchange?*) et des services fournis, ainsi que sur les règles de sécurité à respecter.
    - ♦ *Recommandations : les utilisateurs ne doivent pas ouvrir les courriers d'origine inconnue, ils ne doivent pas stocker de fichiers sensibles (en dehors de la lecture des courriers), ils doivent effacer régulièrement le cache et les cookies, ils doivent immédiatement avertir le service en charge de l'informatique en cas de perte, de vol ou de comportement anormal du téléphone, ils ne doivent pas installer de logiciels sur l'appareil, sauf s'ils proviennent d'une source de confiance (vérifier la réputation avant d'installer ou d'utiliser des applications ou des services) envoyant un contenu qu'ils s'attendent à recevoir, etc.*
- Sécuriser la fin de vie de l'appareil.
    - ♦ *Recommandations : avant élimination ou recyclage du poste de travail, effacer toutes les données et les paramètres, appliquer une procédure approfondie de démantèlement, y compris d'effacement de la mémoire, etc.*

24.3 Spécificités pour les supports de stockage

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Effacer de façon sécurisée ou bien détruire physiquement les supports de stockage mis au rebut.
    - ♦ *Recommandation : effacer les supports de stockage magnétiques (disques durs, bandes, etc.) à l'aide de logiciels d'effacement sécurisés (consulter notamment la liste des logiciels d'effacement certifiés par l'ANSSI) ou bien d'un dégausseur, ou bien faire appel à un prestataire spécialisé dans la destruction de supports de stockage.*
- Lors des opérations de maintenance nécessitant une prise en main à distance sur un poste de travail, ne réaliser l'opération qu'après avoir obtenu l'accord de l'utilisateur.

24.4 Spécificités pour les imprimantes et copieurs multifonctions

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Dans le cas d'une maintenance par un tiers, prévoir les mesures destinées à empêcher l'accès aux données.
    - ♦ *Recommandations : les données doivent être chiffrées ou effacées de manière sécurisée avant l'envoi en maintenance externe ; faire signer un engagement de confidentialité au mainteneur ou faire des réparations sur place en présence d'un membre du service en charge de l'informatique si les données sont sensibles et si elles ne peuvent pas être chiffrées ou effacées dans leur*

totalité (panne d'un disque dur, dysfonctionnement, etc.) ; interdire l'envoi en maintenance externe dans le cas de données sensibles, etc.

- Dans le cas d'une télémaintenance par un tiers à une imprimante ou copieur multifonctions hébergé localement, prendre des mesures spécifiques pour protéger chaque accès.
  - ♦ *Recommandations : faire signer un engagement de confidentialité par le tiers externe, mettre en place de mots de passe robustes, spécifiques et renouvelés régulièrement, pour l'accès en télémaintenance, activer les accès entrant en télémaintenance uniquement sur demande, les accès entrant étant inactifs par défaut, journaliser les accès en télémaintenance, interdire les possibilités de rebond depuis l'accès en télémaintenance vers le reste du réseau local et plus largement vers internet, etc.*
- Empêcher l'accès à des données stockées sur des imprimantes ou copieurs multifonctions mis au rebut.
  - ♦ *Recommandations : entreposer l'équipement sur site dans un local sécurisé en attendant qu'il quitte l'organisme, utiliser un dispositif d'effacement sécurisé sur les données stockées sur les disques durs ou la mémoire intégrée ou détruire physiquement l'équipement si ce n'est pas possible (panne, dysfonctionnement, etc.), faire signer un accord de confidentialité dans le cas où la mise au rebut est réalisée par un tiers, émettre un procès-verbal de destruction des supports et le conserver pendant 10 ans.*

25 Minimisation des données : adéquates, pertinentes et limitées

25.1 Minimisation de la collecte

Objectifs : être conforme à l'article 6 de la loi informatique et libertés et l'article 5.1(c) du règlement général sur la protection des données (RGPD) ; réduire la gravité des risques en limitant la collecte des données à caractère personnel au strict nécessaire au regard d'une finalité définie ; éviter la collecte de données non nécessaires, l'utilisation de données sans lien avec la finalité et des impacts excessifs pour les personnes.

Bonnes pratiques

- Justifier de la collecte de chaque donnée.
- Bien faire la distinction entre les données anonymes et pseudonymes.
- 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.).

- Vérifier que les données sont adéquates, pertinentes et non excessives au regard de la finalité poursuivie, et ne pas les collecter dans le cas contraire.
    - ♦ *Recommandations : définir la finalité du traitement, puis identifier les données nécessaires à cette finalité et justifier en quoi chaque catégorie de données est indispensable, et enfin écarter toute données qui ne rend pas la finalité irréalisable ; si besoin, revoir la finalité si des données sont nécessaires à autre chose que la finalité initialement prévue.*
- Vérifier que les données ne font pas apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale, ainsi que les données relatives à la santé ou à la vie sexuelle, et ne pas les collecter dans le cas contraire à moins d'être dans des circonstances d'exception (consentement, intérêt public? conformément à l'article 8 de la loi informatique et libertés et à l'article 9 du RGPD).
- Vérifier que les données ne sont pas relatives à des infractions, condamnations ou mesures de sûreté, et ne pas les collecter dans le cas contraire, à moins d'être dans des circonstances d'exception (juridictions, auxiliaires de justice? conformément à l'article 9 de la loi informatique et libertés et à l'article 10 du RGPD).
- Empêcher de collecter davantage de données.
    - ♦ *Recommandations : seuls les champs relatifs aux données déterminées sont créés et peuvent être renseignés dans une base de données et aucun autre champ ne peut être ajouté (ne pas prévoir de champ « texte libre » mais des listes déroulantes ; si on ne peut éviter la saisie de texte libre, mettre en garde les utilisateurs), vérifier régulièrement qu'aucune données supplémentaire n'a été collectée par rapport à ce qui était initialement prévu?*

Notes

- Certaines catégories de données font l'objet de contraintes particulières (en particulier les données dites « sensibles » et les données « relatives aux infractions, condamnations et mesures de sûreté », dont le traitement ne peut être mis en œuvre que par certaines catégories de personnes morales, selon les articles 8 et 9 de la loi informatique et libertés et les article 9 et 10 du RGPD).
- En raison du caractère sensible des données relatives à un mineur et en tenant compte du principe de loyauté de collecte vis-à-vis d'un utilisateur vulnérable, la collecte de données concernant un enfant, ses parents ou sa famille devra être particulièrement limitée et justifiée.

25.2 Minimisation des données elles-mêmes

Objectifs être conforme à l'article 6 de la loi informatique et libertés et l'article 5.1(c) du RGPD ; réduire la gravité des risques en minimisant les données elles-mêmes, par des mesures destinées à réduire leur sensibilité.

Bonnes pratiques

- Filtrer et retirer les données inutiles.
  - ♦ *Recommandations : 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.*
- Réduire la sensibilité par transformation.
  - ♦ *Recommandations : 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.*
- Réduire le caractère identifiant des données (Voir la rubrique Anonymisation).
  - ♦ *Recommandations : le système peut faire en sorte que :*
    - ◊ *l'utilisateur peut utiliser une ressource ou un service sans risque de divulguer son identité (données anonymes) ;*
    - ◊ *l'utilisateur peut utiliser une ressource ou un service sans divulguer son identité, mais reste identifiable et responsable de cette utilisation (données pseudonymes) ;*
    - ◊ *l'utilisateur peut faire de multiples utilisations des ressources ou des services sans risque que ces utilisations puissent être reliées ensemble (données non corrélables) ;*
    - ◊ *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.*
- Réduire l'accumulation de données.
  - ♦ *Recommandations : 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.

- Restreindre l'accès aux données.
  - ♦ *Recommandations : 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.*
- Limiter l'envoi des documents électroniques contenant des données aux personnes ayant le besoin d'en disposer dans le cadre de leur activité.
- Effacer de manière sécurisée les données qui ne sont plus utiles ou qu'une personne demande de supprimer, sur le système en opération et sur les sauvegardes le cas échéant (voir également la page Durées de conservation : limitées).
  - ♦ *Recommandations : utiliser un outil d'effacement sécurisé pour les documents électroniques, un « dégausseur » pour les unités de stockage à technologie magnétique...*

Outillage/Pour aller plus loin

- Voir la liste des produits ayant reçu une certification de sécurité de premier niveau (CSPN) de l'agence nationale de la sécurité des systèmes d'information (ANSSI) sur http://www.ssi.gouv.fr/).
- Voir le guide ANSSI-Effacement et les logiciels d'effacement sécurisé certifiés.

26 Organisation

Objectifs : disposer d'une organisation apte à diriger et contrôler la protection des données à caractère personnel au sein de l'organisme (désigner un CIL/DPO, créer un comité de suivi, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Faire désigner par le responsable des traitements une personne en charge de l'assister dans la mise en application de la loi informatique et libertés et du règlement général sur la protection des données (RGPD)t lui accorder les moyens nécessaires à l'exercice de sa mission.
    - ♦ *Recommandations : désigner un correspondant « Informatique et libertés » (CIL) / data Protection Officer (DPO), fixer ses missions dans une lettre de mission, lui attribuer les ressources humaines et financières, lui permettre d'exercer sa fonction directement auprès du responsable des traitements, avec une liberté organisationnelle et décisionnelle, en dehors de tout conflit d'intérêt, informer les instances représentatives du personnel de son rôle, organiser sa consultation avant la mise en œuvre de tout nouveau traitement?*
- Définir les rôles, responsabilités et interactions entre toutes les parties prenantes dans le domaine « Informatique et libertés ».
    - ♦ *Recommandations : définir les activités du CIL / DPO (tenir la liste des traitements et assurer son accessibilité, veiller en toute indépendance au respect de la loi, rendre compte de son action au responsable de traitement, etc.), séparer les rôles entre l'administrateur ayant accès aux données et celui ayant accès aux traces, décrire les interactions entre les maîtrises d'ouvrages, le responsable SSI et le CIL / DPO notamment dans le cadre de tout nouveau projet, définir les responsabilités spécifiques à la gestion des risques pesant sur les libertés et la vie privée, décrire la manière dont les violations de données à caractère personnel sont traitées.*
- Créer un comité de suivi, composé du responsable des traitements, de la personne en charge de l'assister dans la mise en application de la loi informatique et libertés / du RGPD et des parties intéressées, et se réunissant de manière régulière (au moins une fois par an) pour fixer des objectifs et faire un point sur l'ensemble des traitements de l'organisme.

Notes

- Désigner un CIL / DPO offre un vecteur de sécurité juridique (il permet de garantir la conformité de l'organisme à la loi informatique et libertés et au RGPD), un facteur de simplification des formalités administratives (exonération de l'obligation de déclaration préalable des traitements ordinaires et courants), un accès personnalisé aux services de la CNIL (extranet, formations, suivi personnalisé, etc.), la preuve d'un engagement éthique et citoyen et un outil de valorisation du patrimoine

informationnel (possibilité de céder, transmettre ou louer les fichiers détenus par l'organisme dans le respect de la loi informatique et libertés).

27 Politique (gestion des règles)

Objectifs : disposer d'une base documentaire formalisant les objectifs et les règles à appliquer dans le domaine « Informatique et libertés » (plan d'action, révision régulière de la politique « Informatique et libertés », etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Formaliser les éléments importants relatifs au domaine « Informatique et libertés » au sein d'une base documentaire qui constitue la politique « Informatique et libertés », dans une forme adaptée aux différents contenus (risques, grands principes à respecter, objectifs à atteindre, règles à appliquer, etc.) et aux différentes cibles de communication (usagers, service en charge de l'informatique, décideurs, etc.).
    - ♦ *Recommandations : des exigences dans un cahier des charges, une lettre au personnel exprimant l'engagement de la direction, une charte pour les usagers des moyens informatiques et de communication, une procédure pour l'intégration des questions « Informatique et libertés » dans les projets, etc.*
- Faire connaître la politique « Informatique et libertés » aux personnes qui doivent l'appliquer.
- Permettre aux personnes qui doivent appliquer la politique « Informatique et libertés » de demander formellement une dérogation en cas de difficulté de mise en œuvre , étudier chaque demande de dérogation en termes d'impact sur les risques, et le cas échéant, faire valider les dérogations acceptables par le responsable de traitement et faire évoluer la politique « Informatique et libertés » en conséquence.
- Établir un plan d'action pluriannuel et suivre sa mise en œuvre .
- Prévoir les dérogations aux règles de la politique « Informatique et libertés ».
- Prévoir de prendre en compte les difficultés rencontrées dans l'application de la politique « Informatique et libertés ».
- Vérifier la conformité aux règles de la politique « Informatique et libertés » et la mise en œuvre du plan d'action de manière régulière.
    - ♦ *Recommandations : vérifier cette conformité au moins une fois par an.*
- Réviser la politique « Informatique et libertés » de manière régulière.

Outillage / Pour aller plus loin

- Voir le principe « Élaborer une politique SSI » du référentiel général de sécurité (RGS).
- Voir le guide ANSSI PSSI.

28 Protection contre les sources de risques non humaines

Objectifs : réduire ou éviter les risques liés à des sources non humaines (phénomènes climatiques, incendie, dégât des eaux, accidents internes ou externes, animaux, etc.) qui pourraient affecter la sécurité des données à caractère personnel (mesures de prévention, détection, protection, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Mettre en place des moyens de prévention, détection et protection contre l'incendie.
  - ♦ *Recommandations : ranger les locaux (retirer cartons, matériels inutilisés, substances inflammables, etc.), les équiper en nombre suffisant d'extincteurs adaptés au type de feu (extincteurs à poudre, à liquide ou à gaz), en systèmes de détection de fumée sous alarme, et en système de détection de chaleur sous alarme, remontant les alertes de manière centralisée (gardiennage local, prestations externalisée, etc.), mettre en place une extinction par gaz inerte ou extraction d'air dans les salles informatique.*
- Mettre en place des moyens de surveillance de la température.
  - ♦ *Recommandations : équiper les locaux de systèmes de climatisation sous alarme (en cas de dépassement du seuil de température), remontant les alertes de manière centralisée.*
- Mettre en place des moyens de surveillance et de secours de l'alimentation électrique.
  - ♦ *Recommandations : protéger les équipements informatiques et de téléphonie des variations et coupures d'électricité par un groupe électrogène ou par des onduleurs gérant l'arrêt normal ou le fonctionnement en continu, placés sous alarme (en cas de coupure) et remontant les alertes de manière centralisée.*
- Mettre en place des moyens de prévention des dégâts des eaux.
  - ♦ *Recommandations : surélever les équipements informatiques et de téléphonie d'au moins 15cm par rapport au niveau du sol pour les salles informatiques situées en rez-de-chaussée, les éloigner des installations d'eau qui risqueraient de se rompre (plomberie, climatiseur, radiateur, etc.).*
- S'assurer que les services essentiels (électricité, eau, climatisation, etc.) sont correctement dimensionnés pour les systèmes pris en charge.
- Préciser dans les contrats de maintenance des équipements de fonctionnement des services essentiels et de sécurité (extincteurs, climatisation, eau, détection de fumée et de chaleur, détection d'ouverture et d'effraction, groupe électrogène, etc.) un délai d'intervention adapté en cas de défaillance, et les contrôler au moins une fois par an.
- En cas de fortes exigences de disponibilité, connecter l'infrastructure de télécommunications par au moins deux accès différents et indépendants, et faire en sorte de pouvoir basculer de l'un à l'autre très rapidement. Si les besoins de disponibilité sont très élevés, le recours à un site de secours doit être envisagé.

Outillage / Pour aller plus loin

- Voir les référentiels du centre national de prévention et de protection, de l'assemblée plénière des sociétés d'assurances dommage et de la *National Fire Protection Association*.

29 Qualité des données : exactes et tenues à jour

Objectifs : être conforme à l'article 6 de la loi informatique et libertés et l'article 5.1(d) du règlement général sur la protection des données (RGPD) ; maintenir la qualité des données pour éviter des calculs à partir de données erronées ou obsolètes.

Bonnes pratiques

- Vérifier régulièrement l'exactitude des données personnelles de l'utilisateur.
- Inviter l'utilisateur à contrôler et, si nécessaire, mettre à jour ses données régulièrement.
- Assurer la traçabilité de toute modification des données.

Notes

- L'exigence de qualité porte également sur le lien entre les données qui identifient les personnes et les données qui les concernent.

30 Recueil du consentement

30.1 Mesures génériques

Objectifs : être conforme à l'article 7 de la loi informatique et libertés et les articles 7 et 8 du règlement général sur la protection des données (RGPD) ; permettre un choix libre, spécifique et éclairé ; vérifier que le traitement ne repose pas sur une autre base légale que le consentement, tel que prévu à l'article 7 de la loi informatique et libertés et à l'article 6 du RGPD (obligation légale, sauvegarde de la vie, mission de service public, contrat ou mesures prises avec la personne, intérêt légitime).

Bonnes pratiques

• Déterminer et justifier les moyens pratiques qui vont être mis en œuvre pour obtenir le consentement des personnes concernées ou justifier de l'impossibilité de les mettre en œuvre :

- ♦ consentement exprès à l'inscription ;
- ♦ consentement segmenté par catégorie de données ou types de traitement ;
- ♦ consentement exprès avant le partage de données avec des tiers ;
- ♦ consentement présenté de manière compréhensible et adapté à la personne cible (notamment pour les enfants) ;
- ♦ recueil du consentement des parents pour les mineurs de moins de 13 ans ;
- ♦ pour une nouvelle personne, mise en œuvre d'un nouveau recueil de consentement ;
- ♦ après une longue période sans utilisation, demande à la personne concernée 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 de contrat, les paramètres liés à son consentement sont maintenus.

- S'assurer que le traitement ne puisse pas être mis en œuvre sans consentement.
  - ♦ *Recommandations : étudier les cas où les moyens pratiques choisis ne sont plus opérationnels et déterminer des solutions de secours le cas échéant.*
- S'assurer que le consentement sera obtenu de manière libre.
  - ♦ *Recommandations : vérifier qu'il existe une alternative qui ne soit pas trop contraignante (un choix doit être possible) et qu'il n'y a pas de lien de subordination (par exemple entre un employé et son employeur).*
- S'assurer que le consentement sera obtenu de manière éclairée et transparente quant aux finalités du traitement.
- S'assurer que le consentement sera obtenu de manière spécifique à une finalité.

- En cas de sous-traitance, encadrer les obligations de chacun dans un document écrit, explicite et accepté des deux parties.
- Recueillir le consentement des parents pour les mineurs de moins de 13 ans.

Notes

- La CNIL considère que le consentement d'un salarié vis-à-vis d'un traitement mis en place par son employeur n'est pas libre, compte tenu du rapport de subordination.
- Les moyens pratiques permettant d'obtenir le consentement comprennent des actions que les personnes doivent réaliser (taper son code PIN - *Personal Identification Number* ou numéro d'identification personnel, approcher son téléphone mobile d'un panneau publicitaire dans le cas de l'envoi de publicités d'un panneau à un téléphone en Bluetooth, requérir d'approcher son périphérique NFC - *Near Field Communication o*u communication en champ proche, d'un lecteur?).
- Pour toute offre directe de services de la société de l'information à destination des mineurs, la charge de la preuve du consentement incombe au responsable de traitement (ou au sous-traitant), qui doit s'efforcer de vérifier que celui-ci est bien donné par le responsable parental (raisonnablement, compte tenu des moyens technologiques disponibles).

Outillage / Pour aller plus loin

- Voir l'article 32. II. de la loi informatique et libertés .
- Voir l'article L. 34-5 du Code des postes et communications électroniques sur les dispositions spécifiques à la prospection commerciale.

30.2 Spécificités pour les données relevant de l'article 8 de la loi informatique et libertés

Objectifs : permettre un choix libre, spécifique et éclairé, dans le cas de données relatives aux origines raciales ou ethniques, aux opinions politiques, philosophiques ou religieuses, à l'appartenance syndicale ou à la santé ou à la vie sexuelle des personnes.

Bonnes pratiques

• Obtenir le consentement éclairé et exprès des personnes concernées préalablement à la mise en œuvre du traitement, sauf dans le cas où le traitement repose sur une autre base légale ou que la loi prévoit qu'il est interdit de collecter ou de traiter ces données.

30.3 Spécificités pour la collecte de données via un site Internet

Bonnes pratiques

• Prévoir un formulaire avec des cases à cocher et qui ne sont pas cochées par défaut (dit « *opt-in* »).

30.4 Spécificités pour la collecte de données via des cookies

Bonnes pratiques

- Dans le cas où le cookie n'est pas strictement nécessaire à la fourniture du service expressément demandé par l'utilisateur, recueillir le consentement de l'internaute (ex :
  via une bannière en haut d'une page web
  (https://www.cnil.fr/fr/exemple-de-bandeau-cookie), une zone de demande de consentement en surimpression sur la page, des cases à cocher lors de l'inscription à un service en ligne, etc.) après information de celui-ci et avant le dépôt du cookie.
  - ♦ Recommandations : s'assurer que l'information est rédigée en termes simples et compréhensibles du grand public, tout en étant précise (ex : si le cookie a pour finalité de "créer des profils d'utilisateurs afin d'adresser des publicités ciblées", l'information devra reprendre l'ensemble de ces termes et non se limiter à indiquer "publicité").

Notes

- Pour qu'il y ait consentement libre et spécifique exprimé à travers les paramètres du navigateur, ce dernier doit pouvoir permettre à l'utilisateur de choisir quels cookies il accepte et pour quelle finalité. Un navigateur qui accepterait par principe tous les cookies sans distinguer leur finalité ne pourra pas être considéré comme permettant de donner un accord valable puisqu'il ne serait pas spécifique.

Outillage / Pour aller plus loin

- Voir les fiches pratiques https://www.cnil.fr/fr/cookies-comment-mettre-mon-site-web-en-conformite et
  https://www.cnil.fr/fr/recommandation-sur-les-cookies-quelles-obligations-pour-les-responsable sur le site de la CNIL.

30.5 Spécificités pour une collecte de données via un objet connecté ou une application mobile

Bonnes pratiques

- Recueillir le consentement de l'utilisateur au premier démarrage de l'objet ou de l'application mobile.

- ♦ *Recommandations : mettre en œuvre un nouveau recueil de consentement lors de la prise en main par un nouvel utilisateur ; après une longue période sans utilisation, demander à l'utilisateur de réaffirmer son consentement ; maintenir les paramètres liés au consentement en cas de changement d'appareil ou de réinstallation de l'application.*

- Proposer un consentement segmenté par catégorie de données ou types de traitement, en distinguant notamment le partage de données avec d'autres utilisateurs ou avec des sociétés tierces.
  - ♦ *Recommandations : si l'utilisateur a consenti au traitement de données particulières (par ex. sa localisation), l'interface doit signaler clairement quand ce traitement a lieu (icône, voyant lumineux) ; laisser à l'utilisateur la possibilité d'accéder à tout moment aux réglages de son consentement.*

30.6 Spécificités pour la géolocalisation via un smartphone

Bonnes pratiques

- Permettre à l'usager de refuser qu'une application puisse le géolocaliser de manière systématique.
- Permettre à l'usager de sélectionner quelle application peut utiliser la géolocalisation.
- Permettre à l'usager de choisir quelles personnes peuvent accéder à l'information de géolocalisation le concernant et avec quelle précision.
-

30.7 Spécificités pour l'utilisation de techniques de publicité ciblée

Bonnes pratiques

• Mettre à disposition des utilisateurs des moyens simples et non payants pour accepter ou refuser la diffusion à leur égard de contenus publicitaires adaptés à leur comportement de navigation, et choisir les centres d'intérêts à propos desquels ils souhaiteraient voir s'afficher des offres publicitaires adaptées à leurs souhaits.

- ♦ *Recommandations : mettre une plateforme à disposition des internautes pour accepter ou refuser, totalement ou partiellement, l'affichage de publicités ciblées comportementales, expliquer comment supprimer les fichiers cookies et les historiques de navigation, choisir d'autoriser ou d'interdire le stockage de cookies, permettre de créer et stocker des cookies manifestant la volonté de ne pas faire l'objet de publicités comportementales de la part de tiers?*

30.8 Spécificités pour des recherches sur des prélèvements biologiques identifiants (i.e. l'ADN)

Bonnes pratiques

- Si les prélèvements sont conservés pour un traitement ultérieur différent du traitement initial, s'assurer également du consentement éclairé et exprès de la personne concernée pour cet autre traitement.

31 Relations avec les tiers

31.1 Mesures génériques

Objectifs : réduire les risques que les accès légitimes aux données par des tiers peuvent faire peser sur les libertés et la vie privée des personnes concernées (identification des tiers, contrat de sous-traitance, convention, BCR, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Identifier tous les tiers qui ont ou pourraient avoir un accès légitime aux données.
  - ♦ *Recommandations : certaines catégories de personnels, un prestataire en régie, la maintenance informatique, des partenaires métiers, les tiers autorisés.*
- Déterminer leur rôle vis-à-vis du traitement (administrateur informatique, sous-traitant, destinataire, personnes chargées de traiter les données, tiers autorisé) en fonction des actions qu'ils vont réaliser.
  - ♦ *Recommandations : en cas de recours à un fournisseur de service de cloud computing, celui-ci est généralement sous-traitant, bien qu'il puisse être considéré comme responsable de traitement dans certains cas.*
- Déterminer les responsabilités respectives en fonction des risques liés à ces données.
- Déterminer la forme appropriée pour fixer les droits et obligations selon la forme juridique des tiers et leur localisation géographique.
  - ♦ *Recommandations : un contrat de sous-traitance, une convention, un arrêté, des règles internes contraignantes (Binding Corporate Rules ? BCR).*
- Formaliser les règles que les personnes doivent respecter durant tout le cycle de vie de la relation liée au traitement ou aux données, selon la catégorie de personnes et les actions qu'elles vont réaliser.

Outillage / Pour aller plus loin

- Voir les notes CNIL Transfert Hors UE et CNIL Externaliser Hors UE pour le cas de transferts de données en dehors de l'Union européenne.

31.2 Spécificités pour les tiers prestataires de service travaillant dans les locaux de l'organisme

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques :

- Appliquer à ces prestataires les mêmes mesures que pour les salariés de l'organisme : formation aux enjeux Informatique et libertés, obligation de respecter les règles d'usage des ressources informatiques de l'organisme annexées au règlement intérieur.

- Fournir à ces prestataires un poste de travail interne à l'organisme ou s'assurer que l'utilisation du poste de travail fourni par leur employeur est compatible avec les objectifs de sécurité de l'organisme.
- S'assurer que ces prestataires sont bien engagés auprès de leur employeur par une clause de confidentialité applicable aux organismes clients de leur employeur.
- Gérer les habilitations de ces prestataires de façon spécifique en leur attribuant des habilitations limitées dans le temps prenant fin automatiquement à la date prévisionnelle de la fin de leur mission.
-

31.3 Spécificités pour les tiers destinataires

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Encadrer contractuellement la transmission des données à ces tiers, en précisant :
  - ♦ Les données transmises.
  - ♦ La ou les finalités pour lesquelles les personnes ont consenti à la transmission de leurs données au tiers (abonnement à une newsletter, prospection commerciale...).
  - ♦ Les modalités suivant lesquelles les personnes pourront exercer leurs droits.
  - ♦ Les mesures techniques mises en œuvre pour assurer la sécurité des données lors de leur transmission au tiers.
- Imposer au tiers de publier une politique de protection de la vie privée couvrant les traitements alimentés par les données transmises et précisant les objectifs de sécurité issus de la politique de sécurité des systèmes d'information.
- Si la transmission de données est faite via Internet toujours chiffrer les flux de données.
- Systématiquement informer le tiers lorsque des personnes exercent leur droit de rectification.

31.4 Spécificités pour les tiers autorisés

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Ne répondre qu'aux demandes transmises de façon formelle (courrier postal, fax) et répondre via le même canal de communication. Ne pas prendre en compte les demandes adressées par mail ni ne répondre par ce canal de communication.
- Vérifier la base légale de chaque demande de communication.
- Authentifier les émetteurs et ne répondre qu'à eux.
- Répondre de façon stricte à la demande en ne fournissant que les données mentionnées dans la demande.

32 Sauvegardes

Objectifs : assurer la disponibilité et/ou l'intégrité des données à caractère personnel, tout en protégeant leur confidentialité (régularité des sauvegardes, chiffrement du canal de transmission des données, test d'intégrité, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Effectuer une sauvegarde des données, qu'elles soient sous forme papier ou électronique, de manière régulière, selon les besoins de disponibilité et d'intégrité des métiers.
  - ♦ *Recommandations : une sauvegarde incrémentale peut être effectuée quotidiennement, une sauvegarde complète peut être effectuée avec une fréquence hebdomadaire et une copie des documents papiers peut être réalisée dès qu'ils sont édités ; la vérification des sauvegardes peut être effectuée automatiquement après celle-ci permettant de garantir l'intégrité par la production d'un rapport de fin de sauvegarde.*
- Mettre en œuvre des mécanismes de chiffrement du canal de transmission des données dans le cas où la sauvegarde est automatisée par le réseau.
- Protéger les données sauvegardées au même niveau de sécurité qu'en exploitation.
  - ♦ *Recommandations : les données sauvegardées sont déjà chiffrées, les sauvegardes sont chiffrées, ou le lieu de stockage des sauvegardes non chiffrées dispose d'un accès suffisamment protégé ; stocker les supports de sauvegardes physiques (bandes, cartouches, disques,etc.) dans des locaux différents de ceux où sont stockées les données traitées, et ce, dans une armoire ignifugée et étanche ; protéger le transport des supports de sauvegardes (transfert par agent habilité, transport dans un conteneur sécurisé, etc.).*
- Tester les sauvegardes de manière régulière.
  - ♦ *Recommandations : la récupération d'un échantillon de données peut être testée avec une fréquence mensuelle et la récupération de l'ensemble de données avec une fréquence annuelle.*
- Tester l'intégrité des données sauvegardées si les besoins des métiers le nécessitent.
  - ♦ *Recommandations : la fonction de hachage SHA-256 est utilisée pour réaliser une empreinte des données sauvegardée, voire une signature électronique, etc.*
- Formaliser le niveau d'engagement du service en charge de l'informatique vis-à-vis du recouvrement des informations chiffrées en cas de perte ou d'indisponibilité des secrets assurant le chiffrement (mots de passe, certificats?) et contrôler régulièrement les procédures en cohérence avec l'engagement pris.
- S'assurer que l'organisation, les personnels, systèmes et locaux nécessaires au traitement sont disponibles dans un délai correspondant aux besoins des métiers.
- S'assurer de la localisation géographique des sauvegardes, notamment vérifier dans quel(s) pays les données seront stockées.

Notes

- Les transferts, et donc les sauvegardes, de données vers des pays situés en-dehors de l'Union européenne sont interdits sauf :
  - ♦ si le transfert a lieu vers un pays reconnu comme « adéquat » par la Commission européenne ;
  - ♦ si des clauses contractuelles types, approuvées par la Commission européenne, sont signées entre l'émetteur et le destinataire des données ;
  - ♦ au sein d'un groupe, si des règles internes d'entreprises (BCR) sont adoptées ;
  - ♦ si dans le cas d'un transfert vers les États-Unis, l'entreprise destinataire a adhéré au Privacy Shield ;
  - ♦ si l'une des exceptions prévues par l'article 69 de la loi informatique et libertés est invoquée.
- Le site de la CNIL maintient une carte du monde indiquant les formalités à accomplir en fonction du pays visé. Dans tous les cas, le responsable du traitement reste responsable de la sécurité des données sauvegardées.
- La mise en place d'un plan et d'une procédure de sauvegarde doivent permettre d'assurer l'intégrité et la pérennité des données à caractère personnel, sans pour autant mettre en cause leur confidentialité. Le plan de sauvegarde doit mettre en évidence les objectifs généraux attendus des sauvegardes en matière de protection des données et déterminer les mesures organisationnelles nécessaires pour les atteindre. La procédure de sauvegarde détermine les moyens opérationnels et techniques qui doivent être mis en œuvre pour satisfaire au plan de sauvegarde.

33 Sous-traitance : identifiée et contractualisée

33.1 Mesures génériques

Objectifs : être conforme à l'article 28 du règlement général sur la protection des données (RGPD) ; encadrer la sous-traitance.

Bonnes pratiques

- 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 et périmètre de la sous-traitance,
  - ♦ finalité de la sous-traitance,
  - ♦ instructions de traitement documentées,
  - ♦ autorisation préalable en cas de recours à un autre sous-traitant,
  - ♦ mise à disposition de toute documentation apportant la preuve du respect du RGPD,
  - ♦ notification immédiate de toute violation de données, ♦ etc.

33.2 Spécificités pour les sous-traitants (hébergeur, mainteneur, administrateur, prestataires spécialisés...) hors fournisseurs de services de *cloud computing*

Bonnes pratiques

- Encadrer la relation de sous-traitance via un contrat conclu intuitu personæ.
- Exiger du sous-traitant la transmission de sa Politique de Sécurité des Systèmes d'Information (PSSI) ainsi que de toute les preuves de ses certifications en matière de sécurité de l'information et annexer ces documents au contrat. S'assurer que les mesures issues de sa PSSI sont conformes avec les recommandations de la CNIL en matière.
- Déterminer et fixer contractuellement de façon très précise les opérations que le sous-traitant sera amené à effectuer sur les données à caractère personnel :
  - ♦ Les données auxquelles il aura accès ou qui lui seront transmises.
  - ♦ les opérations qu'il doit réaliser sur les données.
  - ♦ La durée pendant laquelle il pourra conserver les données.
  - ♦ Les éventuels destinataires auxquels le responsable de traitement lui demande de transmettre les données.

- ♦ Les opérations à réaliser à la fin de la prestation (suppression définitive des données ou restitution des données dans le cadre d'une réversibilité puis destruction des données chez le sous-traitant).
- ♦ Les objectifs de sécurité fixés par le responsable de traitement.

- Déterminer contractuellement la répartition des responsabilité vis à vis des processus légaux visant à permettre l'exercice des droits des personnes.
- Interdire explicitement ou encadrer le recours à des sous-traitants de rang 2.
- Préciser dans le contrat que le respect des obligations Informatique et Libertés est une obligation essentielle du contrat.

33.3 Spécificités pour les fournisseurs de services de *cloud computing*

Bonnes pratiques

En plus des bonnes pratiques applicables en cas de recours à un sous-traitant, les mesures suivantes pourraient être mise en œuvre :

- Imposer au fournisseur une séparation a minima logique entre les données de l'organisme et les données de ses autres clients.
- Définir très précisément les lieux dans lesquels les données sont susceptibles d'être stockées, et les pays depuis lesquels les données stockées dans le *cloud* sont susceptibles d'être accessibles.
  - ♦ *Recommandation : les fournisseurs de services de cloud computing précisent souvent le lieux de stockage des données, mais n'indiquent que rarement les zones géographiques depuis lesquelles leur administrateurs accèdent à leur plateforme ; ce point doit être précisé dans le contrat.*
- Consulter la recommandation de la CNIL sur le *cloud computing*

34 Supervision

Objectifs : disposer d'une vision globale et à jour de l'état de protection des données et de la conformité à la loi informatique et libertés (contrôler la conformité des traitements, objectifs et indicateurs, responsabilités, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Effectuer régulièrement des contrôles des traitements de données afin de vérifier leur conformité à la loi informatique et libertés ainsi que l'effectivité et l'adéquation des mesures prévues.
  - ♦ *Recommandations : réaliser des vérifications sur les traitements les plus sensibles, sur ceux qui ont fait l'objet de violations de données ou de plaintes, et au hasard afin de tous les contrôler de manière récurrente ; faire réaliser un audit par une tierce partie de manière occasionnelle notamment sur les traitements les plus sensibles.*
- Fixer des objectifs dans le domaine « Informatique et libertés » et des indicateurs permettant de vérifier l'atteinte de ces objectifs.
  - ♦ *Recommandations : disposer d'une cartographie des traitements de données et des risques associés, réaliser les formalités préalables auprès de la CNIL pour l'ensemble des traitements et ce, avant leur mise en œuvre opérationnelle.*
- Déterminer les responsabilités respectives en fonction des risques liés à ces données.
  - ♦ *Recommandations : faire un « RACI », c'est-à-dire déterminer qui réalise chaque action (R pour « Responsible »), qui en est responsable (A pour « Accountable »), qui participe (C pour « Consulted ») et qui doit en être informé (I pour « Informed »).*
- Faire un bilan « Informatique et libertés » de manière régulière.
  - ♦ *Recommandations : présenter de manière annuelle une cartographie globale des risques pesant sur tous les traitements à leur responsable, une évaluation de la conformité à la politique « Informatique et libertés », un avancement des actions prévues.*

Outillage / Pour aller plus loin

- La CNIL labellise des procédures d'audit « Informatique et libertés ».
- Afin de connaître les formalités préalablement réalisées auprès de la CNIL par son organisme, il est possible de demander à la CNIL une « liste article 31 » par télécopie au 01 53 73 22 00, en précisant le numéro de SIREN et les coordonnées de l'organisme.
- Voir le guide d'élaboration de tableaux de bord de sécurité des systèmes d'information (TDBSSI) mis en ligne par l'ANSSI.

35 Surveillance

35.1 Mesures génériques

Objectifs : être capable de détecter les incidents concernant des données à caractère personnel de façon précoce, et de disposer d'éléments exploitables pour les étudier ou pour fournir des preuves dans le cadre d'enquêtes (architecture et politique de journalisation, respect des obligation en matière de protection des données à caractère personnel, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Mettre en place une architecture de journalisation permettant de conserver une trace des événements de sécurité et du moment où ils ont eu lieu.
    - ♦ *Recommandations : horodater les événements journalismes en prenant comme référence le temps UTC (Coordinated Universal Time), utiliser une source de temps fiable sur laquelle les équipements se synchroniseront, telle qu'un serveur NTP (Network Time Protocol) ou une radiosynchronisation, centraliser localement (regrouper tous les journaux sur une machine de collecte relativement isolée et accompagnée d'un poste de travail de consultation dédié), exporter les journaux (envois planifiés, transfert automatique ou utilisation d'un réseau d'administration), disposer d'une capacité de stockage suffisante, se doter d'un système d'archivage et de sauvegarde pour les journaux d'événements, protéger les équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés, etc.*
- Choisir les événements à journaliser en fonction du contexte, des supports (postes de travail, pare-feu, équipements réseau, serveurs, etc.), des risques et du cadre légal.
    - ♦ *Recommandations : journaliser les actions sur les postes de travail en cas de risques élevés uniquement, respecter le code des postes et des communications électroniques en cas de mise en place d'un accès public à Internet (conserver pendant un an les données de connexion si elles sont collectées dans le cadre du service, les informations permettant d'identifier l'utilisateur ainsi que le ou les destinataires de la communication, données relatives aux équipements terminaux de communication utilisés, caractéristiques techniques, la date, l'horaire et la durée de chaque communication, et les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs), avec un devoir strict de confidentialité, respecter le décret LCEN (Loi pour la confiance dans l'économie numérique) en cas de création de contenu en ligne (conserver pendant un an, si elles sont collectées dans le cadre du service : données de connexion, données de création de contenu, données relatives au contrat, données relatives au paiement), etc.*
- Respecter les exigences de la loi informatique et libertés si les événements journalisés comprennent des données à caractère personnel.

- ♦ *Recommandations : les dispositifs utilisés doivent faire l'objet d'une information des utilisateurs, d'une déclaration à la CNIL, l'utilisation des données collectées doit respecter la finalité initialement déclarée, etc.*

- Procéder périodiquement à l'analyse des informations journalisées, voire mettre en place un système de détection automatique de signaux faibles.
- Conserver les journaux d'événements sur six mois, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques.

Outillage / Pour aller plus loin

- Voir la note CERTA Journaux.
- En fonction de l'étude des risques et des contraintes légales, la fonction "Horodatage" du référentiel général de sécurité (RGS) est à considérer.

35.2 Spécificités pour un poste client

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- S'assurer que la taille maximale des journaux d'événements est suffisante, et notamment que les événements les plus anciens ne sont pas supprimés automatiquement si la taille maximale est atteinte.
- Journaliser les événements relatifs aux applications, à la sécurité et au système.
  - ♦ *Recommandations : connexions au système (enregistrer l'identifiant, la date et l'heure de leur tentative de connexion, le fait que la connexion ait réussi ou non, ainsi que la date et l'heure de la déconnexion), modification de paramètres de sécurité, de privilèges, de comptes utilisateurs et de groupes, événements système (arrêt / redémarrage de processus système sensibles), accès/modification de données système, échec lors d'un accès à une ressource (fichier système, objet, réseau, etc.), exécution de transactions sensibles, l'application des correctifs de sécurité, actions d'administration et de prise de main à distance, journaux du logiciel antivirus (activation/désactivation, mises à jour, détection de codes malveillants), etc.*
- Exporter les journaux à l'aide des fonctionnalités de gestion du domaine ou via un client *syslog*.
- Analyser principalement les heures de connexions et déconnexions, le type de protocole utilisé pour se connecter et le type d'utilisateur qui y a recours, l'adresse IP d'origine de la connexion, les échecs successifs de connexions, les arrêts inopinés d'applications ou de tâches.

35.3 Spécificités pour un pare-feu

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Mettre en place une politique de filtrage interdisant toute communication directe entre des postes internes et l'extérieur (ne permettre les connexions que via le pare-feu) et ne laisser passer que les flux explicitement autorisés (blocage par le pare-feu de toute connexion sauf celles identifiées comme nécessaires).
- Journaliser toutes les connexions autorisées réussies et toutes les tentatives de connexions rejetées.
    - ♦ *Recommandations : pour chaque connexion, horodater les journaux à la milliseconde près, journaliser au moins les adresses IP source et destination, le protocole de transport, et les drapeaux et états de connexion associés aux segments pour le protocole TCP, etc.*
- Exporter les journaux par un canal sécurisé vers un serveur dédié.

35.4 Spécificités pour un équipement réseau

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Journaliser l'activité sur chaque port d'un commutateur ou d'un routeur.
- Exporter les journaux vers un serveur dédié à l'aide d'un client *syslog* intégré ou via un flux *netflow*.
- Contrôler la volumétrie en fonction des heures, ainsi que le respect des éventuelles listes de contrôle d'accès (ACL : *Access Control Lists*) pour les routeurs.

35.5 Spécificités pour un serveur

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Journaliser le maximum d'informations sur les requêtes effectuées par les clients sur les serveurs web dans le but d'identifier les défauts de configuration, les injections de requêtes SQL, etc.
    - ♦ *Recommandations : connexions réussies, méthodes de connexion, requêtes effectuées, volumétries, répartition par pays des requêtes, etc.*
- Journaliser l'activité des usagers sur les serveurs *proxy*.
- Journaliser l'ensemble des requêtes qui sont faites aux serveurs DNS, qu'elles soient émises par des internautes ou par des clients du réseau interne.
- Journaliser les données d'authentification horodatées et la durée de chaque connexion sur les serveurs d'accès distant.
- Journaliser la réception et la gestion des messages sur les serveurs de messagerie.

36 Sécurité de l'exploitation

Objectifs : limiter la vraisemblance et la gravité des risques visant les biens supports utilisés en exploitation (documenter les procédures d'exploitation, inventaire et mise à jour des logiciels et matériels, correction des vulnérabilités, duplication des données, limiter l'accès physique au matériel, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Documenter les procédures d'exploitation, les tenir à jour et les communiquer à tous les utilisateurs concernés (toute action sur le système, qu'il s'agisse d'opérations d'administration ou de la simple utilisation d'une application, doit être expliquée dans des documents auxquels les utilisateurs peuvent se référer).
- Tenir à jour un inventaire des logiciels et matériels utilisés en exploitation.
    - ♦ *Recommandations : maintenir une liste exhaustive des logiciels, des serveurs physiques et virtuels, des éléments d'infrastructures, des services gérés par des tiers et des équipements réseaux et de télécommunications utilisés pour l'exploitation des traitements de données personnelles. Inclure dans cette liste les informations matérielles, les types de système d'exploitation, les informations réseau (adresse IP, adresse MAC), les applications utilisées, les versions présentes et les correctifs appliqués, et les versions des firmwares pour les équipements pour lesquels ceux-ci peuvent être mis à jour).*
- Réaliser une veille sur vulnérabilités découvertes dans les logiciels (y compris les firmwares) utilisés en exploitation, et les corriger dès que possible.
    - ♦ *Recommandations : dans la mesure du possible activer les systèmes de mise à jour automatique des logiciels. Lorsque cela n'est pas possible, installer les mises à jour correctives dès leur disponibilité. A défaut mettre en place des mécanismes visant à prévenir l'exploitation des vulnérabilités découvertes.*
- Formaliser les procédures de mises à jour matérielles et logicielles.
- Interdire l'usage des serveurs de production (serveurs de base de données, serveur web, serveur de messagerie, etc.) pour d'autres fins que celles prévues initialement
    - ♦ *Recommandations : n'installer que les logiciels strictement nécessaires sur les serveurs, limiter le trafic réseau aux ports strictement nécessaires.*
- Utiliser des unités de stockage de données utilisant des mécanismes de redondance matérielle (tel que le RAID), ou bien des mécanismes de duplication des données entre plusieurs serveurs et/ou sites.
- Vérifier que le dimensionnement des capacités de stockage et de calcul est suffisant pour assurer le fonctionnement correct des traitements, même en cas de pic d'activité.
- Vérifier que les conditions physiques d'hébergement (température, humidité, fourniture d'énergie, etc.) sont appropriés à l'usage prévu des matériels, et incluent des mécanismes de secours (onduleur et/ou alimentation de secours et/ou groupe électrogène).

- Limiter l'accès physique aux matériels sensibles et/ou qui ont une grande valeur marchande.
- Limiter les possibilités de modification des matériels
    - ♦ *Recommandations : utiliser des scellés permettant de vérifier qu'un ordinateur a été ouvert, cadenasser les boîtiers des machines lorsque cela est possible, verrouiller les baies de stockage.*
- Prévoir un Plan de Reprise d'Activité (PRA) ou un Plan de Continuité d'Activité (PCA), en fonction des objectifs de disponibilité des traitements mis en œuvre .
    - ♦ *Recommandations : formaliser le PRA ou le PCA, le diffuser auprès des personnels concernés (internes, externes, prestataires), tester régulièrement son efficacité.*
- Mettre en place une procédure de gestion des incidents de sécurité permettant de les détecter, les enregistrer, les qualifier et les traiter (voir la page Gestion des incidents et des violations de données).

37 Sécurité des canaux informatiques (réseaux)

37.1 Mesures génériques

Objectifs : diminuer la possibilité que les caractéristiques des canaux informatiques (réseau filaire, wifi, ondes radio, fibre optique, etc.) soient exploitées pour porter atteinte aux données à caractère personnel (cartographie du réseau, pare-feu, détection et prévention d'intrusion, protocole SSH, chiffrement des flux, authentification forte, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Maintenir à jour une cartographie détaillée du réseau.
- Recenser tous les accès Internet, les intégrer dans la cartographie du réseau et s'assurer que les mesures prévues sont bien appliquées à chacun d'entre eux.
- Assurer la disponibilité des canaux informatiques.
    - ♦ *Recommandations : vérifier que les canaux informatiques sont correctement dimensionnés par rapport aux flux prévus, prévoir des solutions alternatives en cas de dysfonctionnement.*
- Segmenter le réseau en sous-réseaux logiques étanches selon les services censés y être déployés.
    - ♦ *Recommandations : cloisonner les réseaux dans des réseaux virtuels (VLAN) pour regrouper certains matériels selon des critères logiques, ou éventuellement en contrôlant les flux de données sur la base des adresses réseau en mettant en place des réseaux physiques distincts, dans le but de séparer les trafics réseau entre les différents groupes ainsi constitués.*
- Interdire toute communication directe entre des postes internes et l'extérieur.
    - ♦ *Recommandations : différencier un réseau interne pour lequel aucune connexion venant d'Internet n'est autorisée, et un réseau dit DMZ accessible depuis Internet.*
- N'utiliser que les flux explicitement autorisés (limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées) à l'aide d'un pare-feu.
    - ♦ *Recommandations : si l'accès à un serveur web passe obligatoirement et uniquement par l'utilisation du protocole SSL, il faut autoriser uniquement les flux réseau IP entrants sur cette machine sur le port de communication 443 et bloquer tous les autres ports de communication, etc.*
- Surveiller l'activité réseau après en avoir informé les personnes concernées.
    - ♦ *Recommandations : mettre en place des systèmes de détection d'intrusion ou un système de prévention d'intrusion en vue d'analyser le trafic réseau en temps réel pour détecter toute activité suspecte évoquant un scénario d'attaque informatique.*
- Prévoir un plan de réponse en cas d'intrusion majeure contenant les mesures organisationnelles et techniques pour délimiter et circonscrire la compromission.

- ♦ *Recommandations : préparation des documents nécessaires à la gestion de crise (cartographie du réseau, liste des personnels en mesure d'intervenir sur les systèmes, coordonnées des administrations ou organisations susceptibles de porter assistance, etc.).*

- Identifier les matériels de manière automatique comme moyen d'authentification des connexions à partir de lieux et matériels spécifiques.
  - ♦ *Recommandations : utiliser les identifiants uniques des cartes réseau (l'adresse MAC) afin de détecter et d'empêcher la connexion d'un dispositif non répertorié.*
- Sécuriser les flux d'administration et restreindre, voire interdire, l'accès physique et logique aux ports de diagnostic et de configuration à distance.
  - ♦ *Recommandations : les opérations d'administration sur les ressources locales doivent s'appuyer sur des protocoles d'administration sécurisés, et dans le cas où le recours à de tels protocoles est techniquement impossible, l'administration doit être accomplie directement sur l'équipement concerné, restreindre l'usage du protocole SNMP qui permet la configuration des équipements réseau par connexion sur les ports UDP 161 et 162.*
- Interdire le raccordement d'équipements informatiques non maîtrisés.
  - ♦ *Recommandations : seuls les équipements (ordinateurs, assistants personnels, smartphones, etc.) dont la configuration a été expressément validée par le service en charge de l'informatique peuvent être raccordés ou synchronisés au réseau ou aux postes de travail.*
- Transmettre les secrets garantissant la confidentialité de données (clé de déchiffrement, mot de passe, etc.) dans une transmission distincte, si possible via un canal de nature différente de celui ayant servi à la transmission des données.
  - ♦ *Recommandations : envoyer un fichier chiffré par mail et communiquer le mot de passe par téléphone ou SMS.*

Outillage / Pour aller plus loin

- La surveillance de l'activité du réseau peut être réalisée à l'aide :
  - ♦ de systèmes de détection d'intrusions ou IDS (soit des NIDS qui surveillent l'état de la sécurité au niveau du réseau, soit des HIDS qui surveillent l'état de la sécurité au niveau des ordinateurs reliés au réseau, soit des IDS hybrides),
  - ♦ de système de prévention d'intrusion ou IPS (soit des NIPS qui détectent les flux réseau suspects au niveau des protocoles, soit des WIPS qui détectent les flux réseau sans fil suspects au niveau des protocoles, soit des NBA qui identifient les menaces générant des flux inhabituels, soit des HIPS qui surveillent des événements inhabituels au niveau des machines).
- Voir les notes CERTA Filtrage, CERTA SSL, CERTA Canulars, CERTA Spam, CERTA Tunnels, CERTA Indexation, CERTA PHP, CERTA IPv6, CERTA DNS et CERTA Backscatting.
- Voir les exigences relatives à la fonction « Authentification » du référentiel général de sécurité (RGS).

37.2 Spécificités pour les connexions aux équipements actifs du réseau

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

• Utiliser le protocole SSH ou une connexion directe à l'équipement pour la connexion aux équipements actifs du réseau (pare-feu, routeurs, commutateurs) et proscrire l'utilisation du protocole Telnet sauf en cas de connexion directe.

37.3 Spécificités pour les outils de prise de main à distance

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Limiter la prise de main à distance d'une ressource informatique locale aux agents du service en charge de l'informatique, sur les ressources informatiques de leur périmètre.
- Identifier les utilisateurs de l'outil de prise de main à distance de manière unique.
- Authentifier les utilisateurs de l'outil de prise de main à distance au moins par un mot de passe robuste et si possible par certificat électronique.
- Journaliser les actions des utilisateurs de l'outil de prise en main à distance (voir la page Traçabilité (journalisation)).
- Sécuriser le flux d'authentification sécurisé.
    - ♦ *Recommandations : aucun mot de passe en clair, séquence non rejouable.*
- La prise de main à distance doit être soumise à un accord préalable de l'utilisateur.
    - ♦ *Recommandations : validation sur une fenêtre pop-up.*
- Interdire la modification du paramétrage de sécurité de l'outil et la visualisation des mots de passe ou secrets utilisés.
- Empêcher la récupération des secrets utilisés pour établir la connexion à partir d'un poste de travail.
- Chiffrer l'ensemble des flux échangés.
- L'utilisateur doit être informé qu'une prise de main à distance est en cours sur son poste de travail (par exemple à l'aide d'une icône).

37.4 Spécificités pour les postes nomades ou se connectant à distance

Objectifs : réduire les risques liés à l'utilisation distante des postes nomades (PC portables, assistants personnels, etc.) ou se connectant à distance.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Mettre en place une solution d'authentification forte des utilisateurs accédant à distance au système d'information interne (quand cela est possible).
    - ♦ *Recommandations : requérir au minimum deux éléments d'authentification distincts parmi ce que l'on sait (ex. : mot de passe, boitier électronique générateur de mots de passe à usage unique OTP (token) sans oublier de*

changer les mots de passe d'activation par défaut), ce que l'on a (ex. : certificat électronique, carte à puce, etc.) et une caractéristique qui nous est propre (ex. :
empreinte digitale, autre caractéristique biométrique).

- Chiffrer les communications entre le poste nomade et le système d'information interne.
  - ♦ *Recommandations : utiliser des lignes privées dédiées, mettre en place des connexions VPN reposant sur des algorithmes cryptographiques réputés forts, recourir au chiffrement de la communication par l'usage du protocole SSL avec une clé de 128 bits lors de la mise en œuvre de services web.*
- Installer un pare-feu local pour sécuriser les échanges réseau entrant et sortant sur le poste de travail en situation de nomadisme, qui doit être activé dès que le poste nomade sort de l'organisme.
  - ♦ *Recommandations : connecter le poste de travail sur une infrastructure d'accès distant spécifique, interdire les connexions simultanées au système d'information interne et à un réseau sans fil, interdire la possibilité de désactiver le pare-feu ou de modifier ses paramètres par les utilisateurs.*

37.5 Spécificités pour les interfaces sans fil (Wifi, Bluetooth, infrarouge, 4G, etc.)

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Dans le cas de connexions à l'aide d'interfaces sans fil, interdire les communications non sécurisées.
- Interdire la connexion simultanée à un réseau via une interface sans fil et par l'interface Ethernet.
- Désactiver les interfaces de connexion sans fil (Wifi, Bluetooth, infrarouge, 4G, etc.) dès lors qu'elles ne sont pas utilisées, de manière matérielle ou logicielle.
- Maîtriser les réseaux sans fil.
  - ♦ *Recommandations : n'autoriser que la mise en place d'infrastructures sans fil permettant l'accès à des ressources locales par les collaborateurs (extension du réseau local) et d'accès publics à Internet totalement isolés de l'infrastructure réseau locale de l'organisme, authentifier les utilisateurs, chiffrer les flux.*

37.6 Spécificités pour le Wifi

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Utiliser le protocole WPA ou WPA2 avec un mode de chiffrement AES/CCMP ou, le mode « Enterprise » des protocoles WPA et WPA2 (utilisant un serveur Radius, ainsi que les sous-protocoles EAP-TLS ou PEAP).

- Interdire les réseaux ad-hoc.
- Utiliser et configurer un pare-feu au point d'entrée/sortie du réseau, afin de cloisonner les équipements connectés en fonction des besoins.

Outillage / Pour aller plus loin

- Voir la note CERTA Wifi.
- Voir le guide pratique spécifique pour la mise en place d'un accès Wifi de l'ASIP
- Dans certains contextes, le filtrage par adresse MAC peut être mis en place pour protéger l'accès Wifi.

37.7 Spécificités pour le Bluetooth

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Imposer une authentification mutuelle avec l'appareil distant.
- Limiter l'utilisation à l'échange de fichiers avec des matériels maîtrisés par le service en charge de l'informatique.
- Chiffrer les échanges.

Outillage / Pour aller plus loin

- Voir la note CERTA Bluetooth.

37.8 Spécificités pour l'infrarouge

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Réaliser une authentification avant la connexion, l'émission et la réception d'un fichier ou d'une commande.

37.9 Spécificités pour les réseaux de téléphonie mobile (2G, 3G ou 4G, etc.)

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Protéger la carte SIM par un code PIN demandé à chaque utilisation.

37.10 Spécificités pour la navigation sur Internet

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Utiliser le protocole TLS (HTTPS) pour assurer l'authentification des serveurs et la confidentialité des communications.
- Privilégier des clés générées conformément au RGS.
    - ♦ *Recommandations : avoir recours à un prestataire de service de certification électronique référencé comme conforme au RGS dans sa version 1.0 pour un usage d'authentification de serveur.*

37.11 Spécificités pour le transfert de fichiers

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Utiliser le protocole SFTP ou éventuellement le protocole SCP.
- Chiffrer les fichiers avant tout transfert dans le cas de risques élevés.

37.12 Spécificités pour le fax

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Positionner le fax dans un local physiquement contrôlé et accessible uniquement au personnel habilité.
- Mettre en place un contrôle par code d'accès personnel pour l'impression des messages.
- Faire afficher l'identité du fax destinataire lors de l'émission des messages, afin d'être assuré de l'identité du destinataire.
- Doubler l'envoi par fax d'un envoi des documents originaux au destinataire.
- Préenregistrer dans le carnet d'adresse des fax (si cette fonctionnalité existe) les destinataires potentiels.

37.13 Spécificités pour l'ADSL/Fibre

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Recenser les points d'accès locaux à Internet.
- Isoler physiquement les points d'accès locaux à Internet du réseau interne.
- Ne les utiliser qu'en cas de besoins spécifiques et justifiés (exemple : perte de disponibilité de l'accès au réseau inter-urbain).
- Ne les activer que lors de leur utilisation.
- Désactiver leur éventuelle interface sans fil (« wifi »).

37.14 Spécificités pour la messagerie électronique

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer les pièces jointes contenant des données.
- Sensibiliser les utilisateurs au fait qu'ils doivent éviter d'ouvrir des courriers électroniques d'origine inconnue et encore plus les pièces jointes à risque (extensions .pif, .com, .bat, .exe, .vbs, .lnk, etc.) ou configurer le système de telle sorte qu'il ne soit pas possible de les ouvrir.
- Sensibiliser les utilisateurs au fait qu'il convient de ne pas relayer les canulars.

Outillage / Pour aller plus loin

- Définir une politique de gestion de l'authentification des courriers électroniques et recourir au protocole DMARC (*Domain-based Message Authentication, Reporting and Conformance*) pour réduire leur usage abusif.

37.15 Spécificités pour les messageries instantanées

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Sensibiliser les utilisateurs.
  - ♦ *Recommandations : demander aux utilisateurs de faire attention à ce qu'ils écrivent, d'éviter de donner des vraies données dans les formulaires d'information sur les utilisateurs, de ne pas faire confiance aux pièces jointes (ne pas lancer des fichiers provenant d'inconnus), de ne pas suivre tous les liens hypertextes.*
- Interdire l'installation et l'utilisation de logiciels de messagerie instantanée, et si cela est néanmoins nécessaire, sensibiliser les utilisateurs aux risques et bonnes pratiques à adopter.
  - ♦ *Recommandations : leur demander de n'installer que les logiciels téléchargés depuis le site de l'éditeur.*

Outillage / Pour aller plus loin

- Voir la note CERTA IRC.

38 Sécurité des documents papier

Objectifs : limiter les risques que des personnes non autorisées accèdent aux documents papiers contenant des données à caractère personnel (mention de classification, procédés d'impression, limitation de la diffusion, traçage des transmissions, etc.).

38.1 Marquer les documents contenant des données

Objectifs : susciter une conduite prudente des personnes ayant accès aux documents en identifiant clairement ceux qui contiennent des données à caractère personnel.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Porter une mention visible et explicite sur chaque page des documents contenant des données sensibles.
  - ♦ *Recommandations : ajouter en en-tête ou en pied de page des modèles de documents utilisés dans le cadre du traitement la mention « Données à caractère personnel sensibles », voire « Ce document contient des données à caractère personnel, protégées par la Loi ».*
  - ♦ *Recommandations : ajouter « [Données à caractère personnel] » dans le titre des courriels en contenant au cas où ces derniers soient imprimés.*
- Porter une mention visible et explicite dans les applications métiers permettant d'accéder à des données et permettant de les imprimer.
  - ♦ *Recommandations : ajouter en en-tête ou en pied de page de l'application la mention « Cette application permet d'accéder à des données à caractère personnel, protégées par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », afficher une mention dans les courriers auxquels sont joints des données rappelant à l'expéditeur qu'il manipule des données qui ne doivent être transmises qu'aux destinataires prévus initialement et qui doivent être détruites à l'issue de la durée de conservation prévue.*

Notes

- Bien que des mentions visibles puissent attirer l'attention de personnes malveillantes, le gain escompté surpasse généralement le risque induit. En effet, une mention dans des courriers auxquels sont joints des fichiers contenant des données permet d'améliorer l'attention des expéditeurs et des destinataires, qui seront ainsi plus prudents en les manipulant. En outre, il sera plus aisé d'identifier des documents ou des courriers marqués afin de les détruire en fin de durée de conservation.

38.2 Réduire les vulnérabilités des documents papier

Objectifs : diminuer la possibilité que les caractéristiques des documents papier ne soient exploitées pour porter atteinte aux données à caractère personnel.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Choisir des supports papier et des procédés d'impression appropriés aux conditions de conservation (selon la durée de conservation, l'humidité ambiante, etc.).
- Récupérer les documents imprimés contenant des données immédiatement après leur impression ou effectuer, lorsque c'est possible, une impression sécurisé.
- Limiter la diffusion des documents papier contenant des données qu'aux personnes ayant le besoin d'en disposer dans le cadre de leur activité.
- Stocker les documents papier contenant des données dans un meuble sécurisé.
  - ♦ *Recommandations : utiliser une armoire ignifugée fermant à clé, un coffre, etc.*
- Détruire les documents papier contenant des données et qui ne sont plus utiles à l'aide d'un broyeur approprié.
  - ♦ *Recommandations : utiliser un broyeur certifié au minimum classe 3 de la norme DIN 32757105 (La norme allemande DIN 32757 définit 5 niveaux de sécurité pour les broyeurs selon la sensibilité des documents).*

Outillage / Pour aller plus loin

- Pour les documents les plus sensibles, il est conseillé d'en faire une copie et de les stocker de manière sécurisée et dans un lieu différent. Il est aussi possible de les placer sous scellé afin de détecter le fait que quelqu'un y ait accédé.

38.3 Réduire les vulnérabilités des canaux papier

Objectifs : diminuer la possibilité que les caractéristiques des canaux papier (circulation au sein de l'organisme, transport en véhicule, envoi par la Poste?) ne soient exploitées pour porter atteinte aux données à caractère personnel.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- N'envoyer que les documents papier contenant des données nécessaires au traitement.
- Garder une trace précise de la transmission des documents papier contenant des données.
  - ♦ *Recommandations : noter sur un document prévu à cet effet une trace de l'envoi (liste des documents envoyés, identité de l'expéditeur et sa signature, canal de transmission, identité du transporteur le cas échéant et sa signature, date et heure d'envoi) et de la réception de documents contenant des données (liste des documents reçus, identité du destinataire et sa signature, date et heure de réception), etc.*

- Choisir un canal de transmission adapté aux risques et à la fréquence de transmission. ♦ *Recommandations : envoi par la Poste, emploi des ressources de l'organisme (véhicules et chauffeurs), recours à une entreprise spécialisée, etc.*
- Améliorer la confiance envers le transporteur de documents papier contenant des données.
    - ♦ *Recommandations : sensibiliser les personnes transportant les documents papier aux risques s'ils appartiennent à l'organisme, prévoir des clauses relatives à la protection de la disponibilité, de l'intégrité et de la confidentialité des documents papier dans le contrat établi avec un transporteur tiers, contrôler l'identité du transporteur, etc.*
- Protéger les documents papier contenant des données.
    - ♦ *Recommandations : envoyer les documents sous double enveloppe en recommandé, apposer une marque « Confidentiel » sur les enveloppes, prévoir des enveloppes, boîtes ou autres contenants plus ou moins sécurisés contre les menaces de nature non humaine (accidents, incendie, etc.), etc.*

Outillage / Pour aller plus loin

- Si les risques sont importants, il peut également être utile de conserver une copie des documents transmis, de prévoir la réaction en cas de vol, disparition ou modification sous la forme d'une procédure, et de placer les documents sous scellé afin de détecter les éventuellement compromissions.

39 Sécurité des matériels

39.1 Mesures génériques

Objectifs : diminuer la possibilité que les caractéristiques des matériels (serveurs, postes fixes, ordinateurs portables, périphériques, relais de communication, supports amovibles, etc.) soient exploitées pour porter atteinte aux données à caractère personnel (inventaire, cloisonnement, redondance matérielle, limiter l'accès, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Tenir à jour un inventaire des ressources informatiques utilisées.
  - ♦ *Recommandations : maintenir la liste des postes de travail et utilisateurs, des serveurs gérés localement, des équipements réseaux et de télécommunications et des autres périphériques (imprimantes, fax, etc.) en précisant les informations matérielles, le type de système d'exploitation, les informations réseau (adresse IP, adresse MAC), les principales applications portées, les versions présentes et correctifs appliqués.*
- Cloisonner les ressources de l'organisme en cas de partage de locaux.
  - ♦ *Recommandations : le réseau local utilisé par les collaborateurs doit s'appuyer sur des ressources réseau dédiées, isolées des ressources utilisées par les autres utilisateurs des locaux, et placées sous la responsabilité du service en charge de l'informatique ; en cas de partage des locaux techniques, l'accès aux ressources informatiques de l'organisme doit être restreint au service en charge de l'informatique (ex.: serveur dédié dans une baie fermée à clé).*
- Empêcher l'accès à des données stockées sur des ressources informatiques mises au rebut.
  - ♦ *Recommandations : inspecter l'équipement pour s'assurer que toute donnée a bien été effacée, entreposer l'équipement sur site dans un local sécurisé en attendant qu'il quitte l'organisme, utiliser un dispositif d'effacement sécurisé sur les données stockées sur les disques durs ou la mémoire intégrée ou détruire physiquement l'équipement si ce n'est pas possible (panne, dysfonctionnement, etc.), faire signer un accord de confidentialité dans le cas où la mise au rebut est réalisée par un tiers, émettre un procès verbal de destruction des supports et le conserver pendant 10 ans.*
- Prévoir une redondance matérielle des unités de stockage par une technologie RAID ou équivalente.
- Vérifier que le dimensionnement des capacités de stockage et de traitement, ainsi que les conditions d'utilisation, sont appropriés à l'usage prévu des matériels, notamment en terme de place, d'humidité et de température.
- Vérifier que l'alimentation des matériels les plus critiques est protégée contre les variations de tension et qu'elle est secourue, ou qu'elle permet au moins de les arrêter normalement.
- Limiter l'accès aux matériels sensibles et/ou qui ont une grande valeur marchande.

- Limiter les possibilités de modification des matériels
    - ♦ *Recommandations : utiliser des scellés permettant de vérifier qu'un ordinateur a été ouvert, cadenasser les boîtiers des machines lorsque cela est possible, verrouiller les baies de stockage.*

39.2 Spécificités pour les postes de travail

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Assurer la mise à disposition et le maintien en conditions opérationnelles et de sécurité des postes de travail des utilisateurs par le service en charge de l'informatique.
- Protéger les postes peu volumineux, donc susceptibles d'être facilement emportés, et notamment les ordinateurs portables, à l'aide d'un câble physique de sécurité, dès que l'utilisateur ne se trouve pas à proximité et que le local n'est pas sécurisé physiquement.
- Récupérer les données, à l'exception des données signalées comme étant privées ou personnelles, présentes sur un poste préalablement à sa réaffectation à une autre personne.
- Effacer les données présentes sur un poste préalablement à sa réaffectation à une autre personne ou pour les postes partagés.
- Supprimer les données temporaires à chaque reconnexion des postes partagés.
- En cas de compromission d'un poste, rechercher toute trace d'intrusion dans le système afin de détecter si l'attaquant a compromis d'autres éléments.
-

39.3 Spécificités pour les postes nomades

Objectifs : réduire les risques liés au format, au caractère attractif et à l'utilisation des postes nomades (PC portables, assistants personnels, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer les données stockées sur les postes nomades en respectant les mesures préconisées sur la page Chiffrement.
    - ♦ *Recommandations : chiffrement du disque dur dans sa totalité au niveau matériel, chiffrement du disque dur dans sa totalité à un niveau logique via le système d'exploitation ou un autre logiciel, chiffrement fichier par fichier, création de conteneurs chiffrés, etc.*
- Limiter le stockage de données sur les postes nomades au strict nécessaire, et éventuellement l'interdire lors des déplacements à l'étranger.
- Assurer la disponibilité des données stockées sur les postes nomades.
    - ♦ *Recommandations : les copier dès que possible sur un autre poste, sur un serveur, etc.*

- Purger les données collectées sur le poste nomade sitôt qu'elles ont été introduites dans le système d'information de l'organisme.
- Positionner un filtre de confidentialité sur les écrans des postes nomades dès qu'ils sont utilisés en dehors de l'organisme.
- Verrouiller l'appareil au bout de quelques minutes d'inactivité.

Notes

- De plus en plus d'ordinateurs portables sont équipés d'un dispositif de lecture d'empreinte digitale. La mise en œuvre de tels dispositifs est soumise à l'autorisation de la CNIL, sauf s'ils rentrent dans le cadre de l'Autorisation unique 52.
- Les utilisateurs ne doivent pas pouvoir désactiver le chiffrement de disque et de veiller à conserver une copie des clés quand le chiffrement est utilisé.

Outillage / Pour aller plus loin

- Voir le guide de l'ANSSI pour les voyages à l'étranger.

39.4 Spécificités pour les supports amovibles

Objectifs : réduire les risques liés au format et à l'utilisation des supports amovibles (clés USB, disques durs externes, CD, DVD, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Limiter l'usage des supports amovibles à ceux fournis par le service en charge de l'informatique.
- Interdire l'utilisation de clés USB à connexion sans fil (ex : Bluetooth).
- Interdire la connexion de clés USB sur des matériels non sécurisés (antivirus, pare-feu, etc.).
- Limiter l'utilisation des clés USB aux activités professionnelles.
- Désactiver la fonctionnalité d'exécution automatique sur tous les postes (stratégie de groupe).
- Chiffrer les données stockées sur un support amovible.
- Restituer les supports amovibles défectueux ou plus utiles au service en charge de l'informatique.
- Détruire de manière sécurisée les supports de données qui sont inutiles.
    - ♦ *Recommandations : utiliser un "dégausseur" pour les unités de stockage à technologie magnétique, un broyeur certifié au minimum classe 3 de la norme DIN 32757 pour les supports numériques tels que les CD et DVD, une technique appropriée pour les disques SSD / mémoires flash (ex : chiffrer le disque, le reformater, le re-chiffrer avec une clé différente), etc.*

Outillage / Pour aller plus loin

- Voir la note du CERTA sur les risques associés aux clés USB.

39.5 Spécificités pour les imprimantes et copieurs multifonctions

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Changer les mots de passe "constructeur" par défaut.
- Désactiver les interfaces réseau inutiles.
- Désactiver ou supprimer les services inutiles.
- Chiffrer les données sur le disque dur lorsque cette fonction est disponible.
- Limiter l'envoi de documents numérisés aux adresses de messagerie internes et dans certains cas limiter l'envoi de documents numérisés à une seule adresse de messagerie.
- Dans le cas d'une maintenance par un tiers, prévoir les mesures destinées à empêcher l'accès aux données.
    - ♦ *Recommandations : les données doivent être chiffrées ou effacées de manière sécurisée avant l'envoi en maintenance externe ; faire signer un engagement de confidentialité au mainteneur ou faire des réparations sur place en présence d'un membre du service en charge de l'informatique si les données sont sensibles et si elles ne peuvent pas être chiffrées ou effacées dans leur totalité (panne d'un disque dur, dysfonctionnement, etc.) ; interdire l'envoi en maintenance externe dans le cas de données sensibles, etc.*
- Dans le cas d'une télémaintenance par un tiers à une imprimante ou copieur multifonctions hébergé localement, prendre des mesures spécifiques pour protéger chaque accès.
    - ♦ *Recommandations : faire signer un engagement de confidentialité par le tiers externe, mettre en place de mots de passe robustes, spécifiques et renouvelés régulièrement, pour l'accès en télémaintenance, activer les accès entrant en télémaintenance uniquement sur demande, les accès entrant étant inactifs par défaut, journaliser les accès en télémaintenance, interdire les possibilités de rebond depuis l'accès en télémaintenance vers le reste du réseau local et plus largement vers internet, etc.*
- Empêcher l'accès à des données stockées sur des imprimantes ou copieurs multifonctions mis au rebut.
    - ♦ *Recommandations : entreposer l'équipement sur site dans un local sécurisé en attendant qu'il quitte l'organisme, utiliser un dispositif d'effacement sécurisé sur les données stockées sur les disques durs ou la mémoire intégrée ou détruire physiquement l'équipement si ce n'est pas possible (panne, dysfonctionnement, etc.), faire signer un accord de confidentialité dans le cas où la mise au rebut est réalisée par un tiers, émettre un procès-verbal de destruction des supports et le conserver pendant 10 ans.*

40 Sécurité des sites web

Objectifs : diminuer la possibilité que les caractéristiques des sites web soient exploitées pour porter atteinte aux données à caractère personnel (référentiel général de sécurité, chiffrement TLS des flux, politique de dépôt de cookies, audits de sécurité, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Si le site est un téléservice, celui-ci doit être conforme au référentiel général de sécurité (RGS). Pour cela, le site doit notamment utiliser un certificat signé par une autorité racine de confiance "qualifiée" (ex : LSTI, voir la liste des prestataires de certification électronique qualifiés) ;
  - ♦ *Recommandation : le certificat de conformité au RGS doit être présent sur le site.*
- Le chiffrement des flux doit être garanti par TLS, Dès lors, il est nécessaire de configurer le serveur web afin que celui-ci n'accepte que ce type de protocole (exclure notamment le protocole SSL et rendre le chiffrement obligatoire lors de la négociation SSL)
- Si vous utilisez des cookies :
  - ♦ Assurez vous d'avoir obtenu un consentement à leur dépôt, ♦ Pour les cookies, déposez depuis votre domaine :
    - ◊ Assurez vous de limiter la durée de validité des cookies à 13 mois,
    - ◊ Utilisez le flag HTTP-ONLY,
    - ◊ Utilisez le flag Same-Site pour les cookies qui n'ont pas besoin d'être accessible depuis une tierce partie.
- Définissez un Content-Secuirty-Policy n'incluant que les acteurs que vous autorisez à déposer des contenus sur votre site.
- Effectuez des audits de sécurité sur le site.

Outillage / Pour aller plus loin

- L'agence nationale de la sécurité des systèmes d'information (ANSSI) a mis à disposition un guide sur ce sujet, il est conseillé d'en suivre les recommandations.

41 Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne

Objectifs : être conforme aux articles 68 et 69 de la loi informatique et libertés et les articles 44 à 50 du règlement général sur la protection des données (RGPD) ; respecter les obligations en matière de transfert de données en dehors de l'Union européenne.

Bonnes pratiques

- Détailler le lieu géographique de stockage des différentes données du traitement.
- En fonction du pays concerné, 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.

42 Traçabilité (journalisation)

Objectifs : assurer l'enregistrement et l'imputabilité des consultations et actions des utilisateurs du traitement, afin de pouvoir fournir des preuves dans le cadre d'enquêtes (système de journalisation, protection, analyse, conservation, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Mettre en place un système de journalisation applicative permettant de conserver une trace des accès et modifications de données opérés par les utilisateurs et du moment où ils ont eu lieu.
    - ♦ *Recommandations : horodater les événements en prenant comme référence le temps UTC (Coordinated Universal Time), utiliser une source de temps fiable sur laquelle les systèmes se synchroniseront, telle qu'un serveur NTP (Network Time Protocol) ou une radiosynchronisation, centraliser localement (regrouper tous les journaux sur une machine de collecte relativement isolée et accompagnée d'un poste de travail de consultation dédié), exporter les journaux (envois planifiés, transfert automatique ou utilisation d'un réseau d'administration), disposer d'une capacité de stockage suffisante, se doter d'un système d'archivage et de sauvegarde pour les journaux d'événements, protéger les équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés, assurer la stricte confidentialité des journaux, etc.*
- Mettre en place une authentification des utilisateurs permettant d'assurer l'imputabilité des événements journalisés.
    - ♦ *Recommandations : interdire les identifiants génériques ou partagés, respecter les recommandations de la CNIL concernant les mots de passe, privilégier une authentification forte à deux facteurs, etc.*
- Respecter les exigences de la loi informatique et libertés concernant les événements journalisés rattachés à un utilisateur identifié.
    - ♦ *Recommandations : il est nécessaire d'informer les utilisateurs de la traçabilité mise en place, de l'inclure dans la déclaration du traitement à la CNIL et de ne pas utiliser les traces collectées pour d'autres finalités, etc.*
- Procéder périodiquement à l'analyse des informations journalisées, voire mettre en place un système de détection automatique de comportements anormaux.
- Conserver les journaux d'événements sur six mois, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques.

Outillage / Pour aller plus loin

- En fonction de l'étude des risques et des contraintes légales, assurer la valeur probante des journaux par des mesures techniques (horodatage, signature

électronique, calcul d'empreinte?) conformes au référentiel général de sécurité (RGS).

Analyse d'impact relative à la protection des données

Privacy Impact Assessment (PIA)

ÉTUDE DE CAS « CAPTOO »



CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Édition février 2018

Table des matières

Avant-propos 2

1 Étude du contexte 3

1.1 Vue d'ensemble 3
Présentation du (des) traitement(s) considéré(s) 3
Recensement des référentiels applicables au traitement 3

1.2 Données, processus et supports 3
Description des données, destinataires et durées de conservation 3
Description des processus et supports 4

2 Étude des principes fondamentaux 6

2.1 Évaluation des mesures garantissant la proportionnalité et la nécessité du traitement 6
Explication et justification des finalités (art.5.1 (b) 6
Explication et justification du fondement (art.6) 6
Explication et justification de la minimisation (adéquates, pertinentes, non excessives) des données (art.5 (c) 8
Données exactes et tenus à jour (art.5.1 (d) 8
Explication et justification des durées de conservation (art.5.1 (e) 8
Évaluation des mesures 9

2.2 Évaluation des mesures protectrices des droits des personnes des personnes concernées 11
Détermination et description des mesures pour l'information des personnes (art.12) 11
Détermination et description des mesures pour le recueil du consentement (art.7) 12
Détermination et description des mesures pour les droits d'accès et à la portabilité (art.15 & art.20) 13
Détermination et description des mesures pour les droits de rectification et d'effacement (art.16 & art.17) 13
Détermination et description des mesures pour les droits de limitation du traitement et d'opposition (art.18 & art.21) 15
Détermination et description des mesures pour la sous-traitance (art. 28) 16
Détermination et description des mesures pour le transfert de données en dehors de l'Union européenne (chap.5) 16
Évaluation des mesures 16

3 Étude des risques liés à la sécurité des données 20

3.1 Évaluation des mesures 20
Description et évaluation des mesures contribuant à traiter des risques liés à la sécurité des données (art.32) 20
Description et évaluation des mesures générales de sécurité 23
Description et évaluation des mesures organisationnelles (gouvernance) 25

3.2 Appréciation des risques : les atteintes potentielles à la vie privée 27
Analyse et estimation des risques 27
Évaluation des risques 29

4 Validation du PIA 31

4.1 Préparation des éléments utiles à la validation 31
Élaboration de la synthèse relative à la conformité au [RGPD] des mesures permettant de respecter les principes fondamentaux 31
Élaboration de la synthèse relative à la conformité aux bonnes pratiques des mesures des mesures contribuant à traiter les risques liés à la sécurité des données 32
Élaboration de la cartographie des risques liés à la sécurité des données 32
Élaboration du plan d'action 34
Formalisation du conseil de la personne en charge des aspects « Informatique et libertés » 36
Formalisation de l'avis des personnes concernées ou de leurs représentants 36

4.2 Validation formelle 37
Formalisation de la validation 37

Avant-propos

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

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

Ils sont téléchargeables sur le site de la CNIL :







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

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

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

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

1 Étude du contexte

1.1 Vue d'ensemble

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

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

Recensement des référentiels applicables au traitement[2]

Référentiels applicables au traitement	Prise en compte
Aucun référentiel spécifique	

1.2 Données, processus et supports

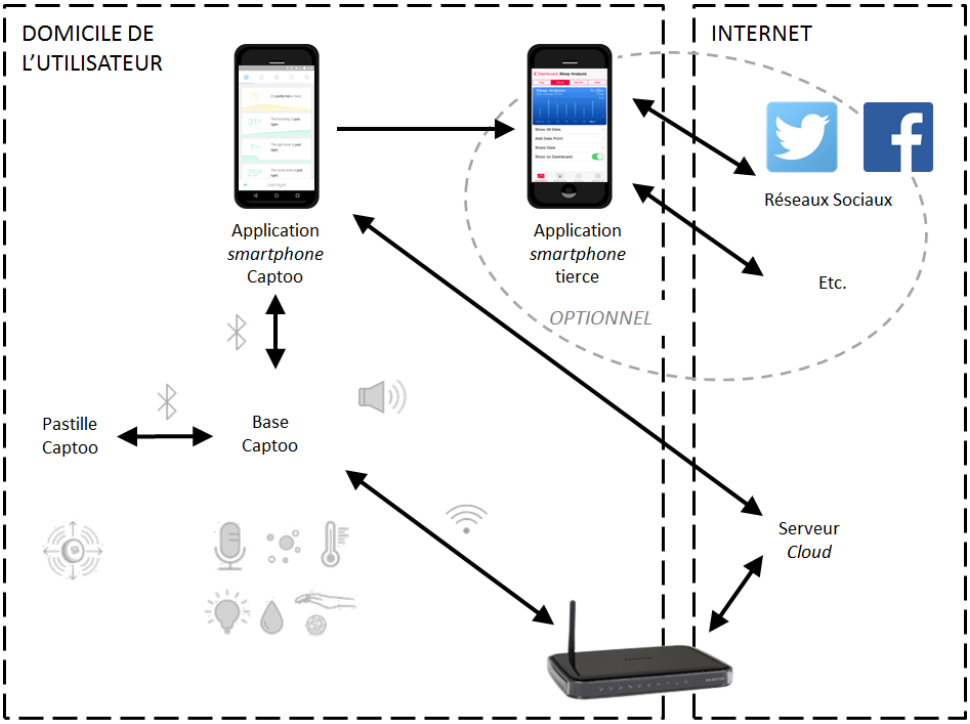
Description des données[3], destinataires et durées de conservation

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

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

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

Description des processus et supports[4]



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

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

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

2 Étude des principes fondamentaux

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

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

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

Explication et justification du fondement (art.6)

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

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

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

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

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

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

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

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

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

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

Évaluation des mesures

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

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

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

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

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

Dispense d'information des personnes concernées	Justification

Dans le cas contraire :

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

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

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

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

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

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

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

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

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

Dans le cas contraire :

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

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

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

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

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

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

Dans le cas contraire :

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

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

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

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

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

Dans le cas contraire :

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

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

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

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

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

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

Évaluation des mesures

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

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

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

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

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

3 Étude des risques liés à la sécurité des données

3.1 Évaluation des mesures

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

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

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

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

Description et évaluation des mesures générales de sécurité

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

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

Description et évaluation des mesures organisationnelles (gouvernance)

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

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

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

Analyse et estimation des risques

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

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

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

Évaluation des risques

Risques	Acceptable / améliorable ?	Mesures correctives	Gravité résiduelle	Vraisemblance résiduelle
Accès illégitime à des données	Améliorable. Des données pourraient encore être volées par un employé de Dreamland, ou consultées par l'entourage usurpant le compte via le *smartphone* dans le but de caractériser une situation relevant de la vie privée des personnes (par exemple un adultère).	- Préciser, et le cas échéant adapter, la manière dont les enregistrements audio sont réalisés, sauvegardés et restitués aux utilisateurs ; - 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	Importante	Négligeable

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

4 Validation du PIA

4.1 Préparation des éléments utiles à la validation

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

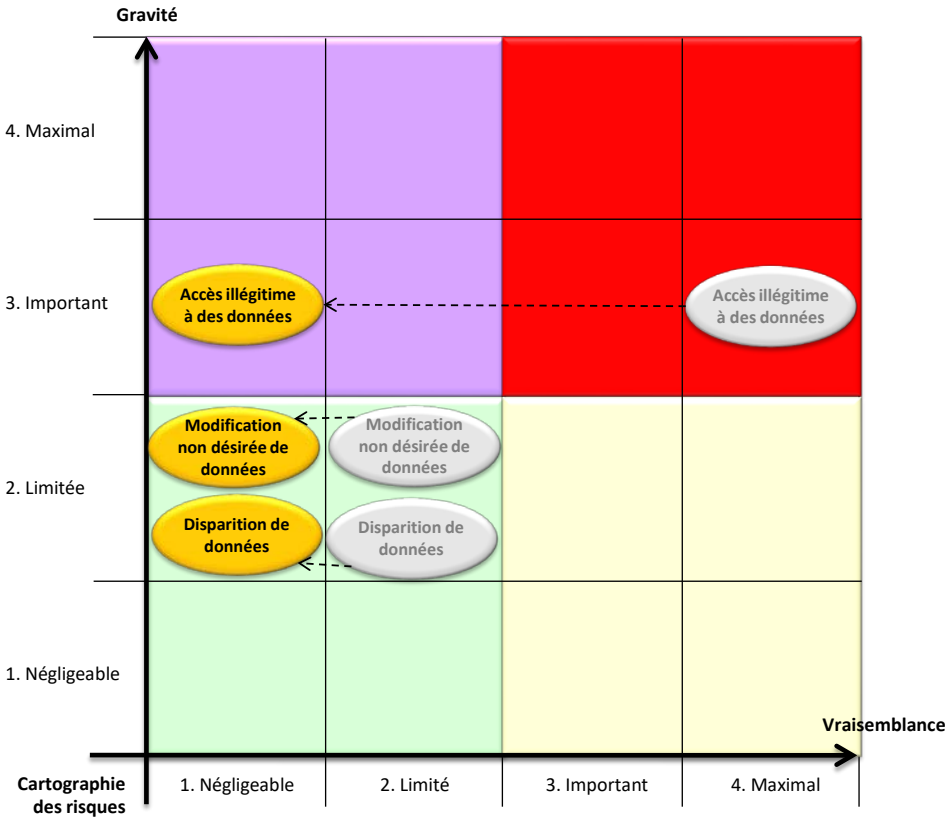
Légende				
Symbole :	●●●	●○○	○●○	○○●
Signification :	Non applicable	Insatisfaisant	Amélioration prévue	Satisfaisant

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

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

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

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


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

Élaboration du plan d'action[9]

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

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

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

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

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

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

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

[Signature]

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

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

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

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

4.2 Validation formelle

Formalisation de la validation

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

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

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

[Signature]

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise

La mise en œuvre d'un traitement figurant sur la présente liste ne dispense pas le responsable de traitement du respect de ses autres obligations prévues par le RGPD. Les traitements, même exonérés d'analyse d'impact, doivent faire l'objet d'une évaluation de leur conformité au RGPD tant sur le plan juridique qu'en matière de sécurité. Conformément aux lignes directrices du CEPD en cas de doute quant à la nécessité d'effectuer une AIPD il est recommandé d'en effectuer une.

Types d'opérations de traitement	Exemples
Traitements, mis en œuvre uniquement à des fins de ressources humaines et dans les conditions prévues par les textes applicables, pour la seule gestion du personnel des organismes qui emploient moins de 250 personnes, à l'exception du recours au profilage.	Les traitements permettant : - la gestion de la paye, l'émission des bulletins de salaire ; - la gestion des formations ; - la gestion du restaurant d'entreprise, la délivrance des chèques repas ; - le remboursement des frais professionnels ; - le contrôle du temps de travail ; - le suivi des entretiens annuels d'évaluation ; - la tenue des registres obligatoires ; - l'utilisation d'outils de communication (messagerie électronique, téléphonie, vidéoconférences, outils collaboratifs en ligne) sans recours au profilage ni à la biométrie ; - le contrôle du temps de travail (sans dispositif biométrique, sans données sensibles ni à caractère hautement personnel).

Traitements de gestion de la relation fournisseurs.	Les traitements permettant : - d'effectuer les opérations administratives liées : aux contrats ; aux commandes ; aux réceptions ; aux factures ; aux règlements ; à la comptabilité pour ce qui a trait à la gestion des comptes fournisseurs : - d'établir les titres de paiement (traites, chèques, billets à ordre…) ; - d'établir des statistiques financières et de chiffre d'affaires par fournisseur ; - de fournir des sélections de fournisseurs pour les besoins de l'entreprise ou de l'organisme ; - d'entretenir une documentation sur les fournisseurs.
Traitements mis en œuvre dans les conditions prévues par les textes relatifs à la gestion du fichier électoral des communes.	Les traitements permettant : - de gérer les demandes d'inscription sur les listes électorales qui sont déposées ou adressées dans les communes et de procéder à leur instruction ; - d'instruire et de procéder à la radiation de la liste électorale des électeurs ne répondant plus aux conditions pour y figurer ; - de gérer les demandes de communication et de copie de la liste électorale.
Traitements destinés à la gestion des activités des comités d'entreprise et d'établissement.	Les traitements permettant : - de gérer les programmes socio-culturels de l'entreprise, communication interne ; - la formation des élus ; - l'exercice du droit d'alerte de l'article L2312-59 du Code du travail ; - la gestion des agendas et réunions ; - la gestion de leurs membres.

Traitements mis en œuvre par une association, une fondation ou toute autre institution sans but lucratif pour la gestion de ses membres et de ses donateurs dans le cadre de ses activités habituelles dès lors que les données ne sont pas sensibles.	Les traitements permettant : - la gestion administrative des membres et donateurs, en particulier la gestion des cotisations ; - d'établir pour répondre à des besoins de gestion, des états statistiques ou des listes de membres ou de contacts, notamment en vue d'adresser bulletins, convocations, journaux. (les critères retenus devant être objectifs et de fonder uniquement sur des caractéristiques qui correspondent à l'objet statutaire de l'organisme) ; - d'établir des annuaires de membres, y compris lorsque ces annuaires sont mis à la disposition du public ou sur le réseau internet ; - d'effectuer par tout moyen de communications des opérations relatives à des actions de prospection auprès des membres, donateurs et prospects.
Traitements de données de santé nécessaires à la prise en charge d'un patient par un professionnel de santé exerçant à titre individuel au sein d'un cabinet médical, d'une officine de pharmacie ou d'un laboratoire de biologie médicale.	Les traitements permettant: - la gestion des rendez-vous ; - la gestion des dossiers médicaux et l'édition des ordonnances ; - la gestion et la tenue des dossiers nécessaires au suivi du patient ; - l'établissement et la télétransmission des feuilles de soins ; - les communications entre professionnels identifiés participant à la prise en charge de la personne concernée ; - la tenue de la comptabilité.
Traitements mis en œuvre par les avocats dans le cadre de l'exercice de leur profession à titre individuel.	Les traitements de gestion des clients, y compris ceux comprenant des données sensibles pouvant concerner des personnes vulnérables (mineurs par exemple).
Traitements mis en œuvre par les greffiers des tribunaux de commerce aux fins d'exercice de leur activité.	Les traitements ayant pour objectif :

	- le contrôle de la légalité des actes ; - la tenue des différents registres et répertoires légaux.
Traitements mis en œuvre par les notaires aux fins d'exercice de leur activité notariale et de rédaction des documents des offices notariaux.	Les traitements ayant pour finalité : - l'envoi dématérialisé des copies et extraits des actes de l'état civil, dans le cadre du traitement de gestion de l'état civil des services compétents des communes et de celui du ministère des affaires étrangères ; - la conservation pour le compte de clients de pièces justificatives de leurs demandes de déductions du revenu global, de réductions ou de crédits d'impôts, dans le cadre de leur mission de tiers de confiance telle que prévue par le code général des impôts.
Traitements mis en œuvre par les collectivités territoriales et les personnes morales de droit public et de droit privé aux fins de gérer les services en matière d'affaires scolaires, périscolaires et de la petite enfance.	Cette exonération s'applique aux traitements relatifs à : - la préinscription, l'inscription, le suivi et la facturation des services en matière d'affaires scolaires, périscolaires, extrascolaires et de petite enfance (la scolarisation en école maternelle et élémentaire) ; - le recensement des enfants soumis à l'obligation scolaire ; - la restauration scolaire et extrascolaire ; les transports scolaires ; - les accueils et activités périscolaires et extrascolaires ; les accueils collectifs de mineurs ; - la participation à l'organisation matérielle et financière des sorties scolaires, les séjours scolaires courts et classes de découvertes dans le premier degré ; - l'accueil de la petite enfance au sein des établissements et services d'accueil des enfants de moins de six ans.
Traitements mis en œuvre aux seules fins de gestion des contrôles d'accès physiques et des horaires pour le calcul du temps de travail, en dehors de tout dispositif biométrique.	Les traitements ayant pour finalité :

A l'exclusion des traitements des données qui révèlent des données sensibles ou à caractère hautement personnel.	- la mise en place d'un dispositif par badge sans biométrie pour entrer dans les locaux d'un organisme à des fins de sécurité ; - la mise en place d'un dispositif de contrôle du temps de travail effectué par les salariés, à l'exclusion de toute autre finalité.
Traitements relatifs aux éthylotests, strictement encadrés par un texte et mis en œuvre dans le cadre d'activités de transport aux seules fins d'empêcher les conducteurs de conduire un véhicule sous l'influence de l'alcool ou de stupéfiants.	Les traitements ayant pour finalité la mise en place d'éthylotests « anti-démarrage » dans des camions de transport.

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise

Types d'opérations de traitement	Critères issus des lignes directrices du CEPD qu'ils remplissent	Exemples
Traitements de données de santé mis en œuvre par les établissements de santé ou les établissements médico-sociaux pour la prise en charge des personnes.	- collecte de données sensibles - personnes dites « vulnérables »	- traitements « de santé » mis en œuvre par les établissements de santé (hôpital, CHU, cliniques, etc.) : • dossier « patients » ; • algorithmes de prise de décision médicale ; • dispositifs de vigilances sanitaires et de gestion du risque ; • dispositifs de télémédecine ; • gestion du laboratoire de biologie médicale et de la pharmacie à usage intérieur, etc. - traitement portant sur les dossiers des résidents pris en charge par un centre communal d'action sociale (CCAS) ou par un établissement d'hébergement pour personnes âgées dépendantes (EPHAD).
Traitements portant sur des données génétiques de personnes dites « vulnérables » (patients, employés, enfants, etc.).	- collecte de données sensibles - personnes dites « vulnérables »	- mise en œuvre d'une recherche médicale portant sur des patients et incluant le traitement de leurs données génétiques ; - traitement utilisé pour la gestion d'une consultation de génétique dans un établissement de santé.

Traitements établissant des profils de personnes physiques à des fins de gestion des ressources humaines	- évaluation ou notation - personnes dites « vulnérables »	- traitement de détection et de gestion de « hauts potentiels » ; - traitement visant à faciliter le recrutement, notamment grâce à un algorithme de sélection ; - traitement visant à proposer des actions de formations personnalisées grâce à un algorithme, - traitement visant détecter et à prévenir les départs de salariés sur la base de corrélations établies entre divers facteurs.
Traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés	- personnes dites « vulnérables » - surveillance systématique	- dispositif de cyber surveillance tels que ceux procédant à une analyse des flux de courriels sortants afin de détecter d'éventuelles fuites d'information (dispositifs dits de *Data Loss Prevention*) ; - vidéosurveillance portant sur les employés manipulant de l'argent ; - vidéosurveillance d'un entrepôt stockant des biens de valeur au sein duquel travaillent des manutentionnaires ; - chronotachygraphe des véhicules de transport routier.
Traitements ayant pour finalité la gestion des alertes et des signalements en matière sociale et sanitaire	- personnes dites « vulnérables » - évaluation ou notation - collecte de données sensibles	- dispositif de signalement de mineurs en danger ; - traitement utilisé par une agence sanitaire pour la gestion d'une crise sanitaire ou d'une alerte sanitaire ; - dispositif de signalement de situations de maltraitance sur des personnes vulnérables (personnes âgées, en situation de handicap, etc.).
Traitements ayant pour finalité la gestion des alertes et des signalements en matière professionnelle	- personnes dites « vulnérables » - évaluation ou notation - collecte de données sensibles	- dispositif de recueil d'alertes professionnelles pour les organismes privés ou publics concernés ;

		- dispositif de recueil de signalements concernant des faits de trafic d'influence ou de corruption commis au sein de l'organisme ; - dispositif d'alerte mis en œuvre dans le cadre du devoir de vigilance.
Traitements des données de santé nécessaires à la constitution d'un entrepôt de données ou d'un registre	- collecte de données sensibles - personnes dites « vulnérables »	- entrepôt de données de santé mis en œuvre par un établissement de santé ou une personne privée, pour servir des finalités de recherche.
Traitements impliquant le profilage des personnes pouvant aboutir à leur exclusion du bénéfice d'un contrat ou à la suspension voire à la rupture de celui-ci	- évaluation ou notation - croisement ou combinaison d'ensembles de données	- traitement établissant un score pour l'octroi de crédit ; - traitement reposant sur une analyse comportementale visant à détecter des comportements « interdits » sur un réseau social ; - traitement de lutte contre la fraude aux moyens de paiement.
Traitements mutualisés de manquements contractuels constatés, susceptibles d'aboutir à une décision d'exclusion ou de suspension du bénéfice d'un contrat	- croisement ou combinaison d'ensembles de données - prise de décision automatisée avec effet juridique ou effet similaire significatif	- traitement recensant les impayés et souscriptions irrégulières partagé par un secteur d'activité ; - traitement des résiliations automobiles qui permet aux sociétés d'assurances de vérifier les antécédents d'un futur assuré lors de la demande de souscription d'un contrat d'assurance automobile.
Traitements de profilage faisant appel à des données provenant de sources externes	- évaluation ou notation - croisement ou combinaison d'ensembles de données - usage innovant ou application de nouvelles solutions technologiques - collecte de données sensibles	- combinaison de données opérée par des courtiers en données (*data brokers*) ; - traitement visant à personnaliser les publicités en ligne.
Traitements de données biométriques aux fins d'identifier une personne physique de manière unique parmi	- collecte de données sensibles - personnes dites « vulnérables »	- traitement basé sur la reconnaissance de l'empreinte digitale ayant pour finalité le contrôle de l'identité des patients ;

lesquelles figurent des personnes dites « vulnérables » *(élèves, personnes âgées, patients, demandeurs d'asile, etc.)*		- contrôle d'accès à la cantine scolaire par reconnaissance du contour de la main ;
Instruction des demandes et gestion des logements sociaux	- collecte de données sensibles - évaluation ou notation	- traitement visant à permettre l'instruction des demandes de logement social en location ou en accession à la propriété.
Traitements ayant pour finalité l'accompagnement social ou médico-social des personnes	- collecte de données sensibles - évaluation ou notation - personnes dites « vulnérables »	- traitement mis en œuvre par un établissement ou une association dans le cadre de la prise en charge de personnes en insertion ou réinsertion sociale et professionnelle ; - traitement mis en œuvre par les maisons départementales des personnes handicapées dans le cadre de l'accueil, l'hébergement, l'accompagnement et le suivi de ces personnes ; - traitement mis en œuvre par un centre communal d'action sociale dans le cadre du suivi de personnes atteintes de pathologies chroniques invalidantes en situation de fragilité sociale.
Traitements de données de localisation à large échelle	- collecte de données sensibles - données traitées à grande échelle - surveillance systématique - Personnes dites « vulnérables » - usage innovant ou application de nouvelles solutions technologiques	- Application mobile permettant de collecter les données de géolocalisation des utilisateurs ; - fourniture d'un service de géolocalisation de mobilité urbaine utilisé par un grand nombre de personnes ; - base de données « clients » des opérateurs de communication électronique ; - mise en œuvre d'un système de billettique par des opérateurs de transport.