LES GUIDES DE LA CNIL

GUIDE
MESURES POUR TRAITER LES RISQUES SUR LES LIBERTÉS ET LA VIE PRIVÉE

Édition 2012

CNIL
Commission Nationale de l'Informatique et des Libertés

Sommaire

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Avant propos

Ce document est un catalogue de bonnes pratiques destinées à traiter les risques que les traitements de données à caractère personnel (DCP) peuvent faire peser sur les libertés et la vie privée des personnes concernées. Il complète la méthode de gestion des risques sur les libertés et la vie privée de la CNIL. Il aide à déterminer des mesures proportionnées aux risques identifiés avec cette méthode.

Il ne se limite pas aux considérations techniques des systèmes informatiques, mais s'applique aux systèmes d'information dans leur globalité : systèmes informatiques, personnes, documents papiers, organisation, locaux…

***Attention** : ce document n'est pas exhaustif et est régulièrement mis à jour. Par ailleurs, les bonnes pratiques doivent être sélectionnées selon les risques identifiés pour bâtir un dispositif global et cohérent comprenant d'autres mesures. Enfin, il est important de les adapter au contexte particulier du traitement considéré.*

Le présent catalogue s'adresse aux responsables de traitement, et en particulier aux parties prenantes dans la création ou l'amélioration de traitement de DCP :

- les maîtrises d'ouvrage (MOA) et leur assistance, qui doivent préalablement apprécier les risques pesant sur leur système et définir des objectifs de sécurité ;
- les maîtrises d'œuvre (MOE) et leur assistance, qui doivent proposer des solutions pour traiter les risques identifiés conformément aux objectifs identifiés par les MOA ;
- les correspondants « informatique et libertés » (CIL), qui doivent accompagner les MOA dans le domaine de la protection des DCP et jouer un rôle d'interface avec la CNIL ;
- les responsables de la sécurité des systèmes d'information (RSSI), qui doivent accompagner les MOA dans le domaine de la sécurité des systèmes d'information (SSI) en respectant les libertés et la vie privée.

Il a pour but de les aider à appliquer la [Loi-I&L] dans le cadre des traitements qu'ils mettent en œuvre. Pour ce faire, il doit notamment leur permettre :

- de pouvoir choisir les mesures proportionnées aux risques (nécessaires et suffisantes pour traiter les risques identifiés) ;
- de disposer d'exemples directement exploitables ;
- de disposer de pistes pour approfondir leur réflexion.

Note : les libellés entre crochets ([libellé]) correspondent aux références normatives ou bibliographiques, qui figurent en annexe du document.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

1. Agir sur les éléments à protéger

1.1. Minimiser les DCP

Objectif : réduire la gravité des risques en limitant les données à caractère personnel (DCP) au strict nécessaire au regard d'une finalité définie, en conformité avec l'article 6 de la [Loi-I&L].

De la licéité des DCP

« Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :

1° Les données sont collectées et traitées de manière loyale et licite ;

2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'aux chapitres IX et X et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;

3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;

4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;

5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. »

(Article 6 de la [Loi-I&L])

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

- Vérifier que les DCP 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 DCP nécessaires à cette finalité et justifier en quoi chaque catégorie de DCP est indispensable, et enfin écarter toute DCP qui ne rend pas la finalité*

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

irréalisable ; si besoin, revoir la finalité si des données sont nécessaires à autre chose que la finalité initialement prévue.

- Vérifier que les DCP 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-I&L]).
- Vérifier que les DCP 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…).
- Empêcher de collecter davantage de DCP.
  - *Recommandations : seuls les champs relatifs aux DCP 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 »), vérifier régulièrement qu'aucune DCP supplémentaire n'a été collectée par rapport à ce qui était initialement prévu…*
- Limiter l'envoi des documents électroniques contenant des DCP aux personnes ayant le besoin d'en disposer dans le cadre de leur activité.
- Effacer de manière sécurisée les DCP qui ne sont plus utiles ou qu'une personne demande de supprimer, sur le système en opération et sur les sauvegardes le cas échéant.
  - *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 le guide [ANSSI-Effacement] et les logiciels d'effacement sécurisé[1] certifiés.

Note

- Certaines catégories de données font l'objet de contraintes particulières (en particulier les données sensibles au sens de l'article 8 et les données relevant de l'article 9[2] de la [Loi-I&L]).

[1] Voir la liste des produits ayant reçu une certification de sécurité de premier niveau (CSPN) : http://www.ssi.gouv.fr/site_rubrique54.html.

[2] 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.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

1.2. Gérer les durées de conservation des DCP

Objectif : réduire la gravité des risques en garantissant que les données à caractère personnel (DCP) ne seront pas conservées plus que nécessaire, en conformité avec les articles 6 et 36 de la [Loi-I&L].

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

- Définir des durées de conservation des DCP limitées dans le temps et en adéquation avec la finalité du traitement.
- Vérifier que le traitement permet de détecter la fin de la durée de conservation.
  - *Recommandations : le traitement intègre la date à laquelle chaque DCP enregistrée doit être supprimée.*
- Vérifier que le traitement permet de supprimer les DCP 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 : face à des risques faibles, une simple suppression peut suffire, alors qu'il conviendra d'utiliser des outils d'effacement sécurisés si les risques sont élevés.*
- Une fois la durée de conservation atteinte, supprimer les DCP sans délai.
  - *Recommandations : développer une fonctionnalité automatisée qui efface les DCP dont la durée de conservation est atteinte …*

Note

- D'une manière générale, la finalité des traitements ne justifie pas de conserver des DCP en prévisions d'actions de Police ou en Justice au-delà de ce qui est prévu conformément à la [Loi-I&L]. Toutefois, dans certains secteurs, il est obligatoire de conserver certaines données pendant une durée déterminée (opérateurs de télécommunication, passagers de vols aériens…).

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

1.3. Informer les personnes concernées

Objectif : garantir l'information des personnes, conformément à l'article 32 de la [Loi-I&L].

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

- Vérifier que le traitement ne fait pas l'objet d'une exception ou de conditions particulières mentionnées dans l'article 32 de la [Loi-I&L] (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).
- Déterminer les moyens pratiques qui vont être mis en œuvre pour informer les personnes concernées.
- S'assurer que l'information sera réalisée de manière complète, claire et adaptée au public visé, en fonction de la nature des DCP 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.

Outillage / Pour aller plus loin

- Voir l'article 32 de la [Loi-I&L] pour le contenu de l'information, les exceptions et les conditions particulières.

Voir les modèles de mentions légales sur le site de la CNIL[3].

[3] Voir http://www.cnil.fr/vos-responsabilites/informations-legales.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

1.3.1 Spécificités pour les salariés d'un organisme

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

- 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…*

1.3.2 Spécificités pour une collecte de DCP via un site Internet

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

- 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…*

1.3.3 Spécificités pour une collecte de DCP par téléphone

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

- 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…), 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).

1.3.4 Spécificités pour une collecte de DCP via un formulaire

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

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

1.3.5 Spécificités pour l'utilisation de techniques de publicité ciblée

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

- 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.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Outillage / Pour aller plus loin

- Voir l'avis [G29-Publicité].

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

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

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

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

1.4. Obtenir le consentement des personnes concernées

Objectif : permettre un choix libre, spécifique et éclairé, conformément à l'article 7 de la [Loi-I&L].

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

- Vérifier si le traitement ne repose pas sur une autre base légale que le consentement, tel que prévu à l'article 7 de la [Loi-I&L] (obligation légale, sauvegarde de la vie, mission de service public, contrat ou mesures prises avec la personne, intérêt légitime).
- Déterminer les moyens pratiques qui vont être mis en œuvre pour obtenir le consentement des personnes concernées.
- 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.

Outillage / Pour aller plus loin

- Voir l'article 32. II. de la [Loi-I&L].
- Voir l'article L. 34-5 du Code des postes et communications électroniques sur les dispositions spécifiques à la prospection commerciale.

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[4], 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[5] d'un lecteur…).

1.4.1 Spécificités pour les données relevant de l'article 8 de la [Loi-I&L]

Objectif : 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.

[4] *Personal Identification Number*, numéro d'identification personnel.
[5] *Near Field Communication*, communication en champ proche.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

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

- 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 DCP.

1.4.2 Spécificités pour la collecte de DCP via un site Internet

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

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

1.4.3 Spécificités pour la collecte de DCP via des *cookies*

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

- 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[6], une zone de demande de consentement en surimpression sur la page, des cases à cocher lors de l'inscription à un service en ligne,…) 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 la Fiche pratique « Ce que le "Paquet Télécom" change pour les cookies » sur le site de la CNIL[7].

1.4.4 Spécificités pour la géolocalisation via un *smartphone*

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

- 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.

[6] Solution instaurée sur le site www.ico.gov.uk.
[7] http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/ce-que-le-paquet-telecom-change-pour-les-cookies/

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- Permettre à l'usager de choisir quelles personnes peuvent accéder à l'information de géolocalisation le concernant et avec quelle précision.

1.4.5 Spécificités pour l'utilisation de techniques de publicité ciblée

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

- 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…*

1.4.6 Spécificités pour des recherches sur des prélèvements biologiques identifiants[8]

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

- 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.

[8] Par exemple l'ADN.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

1.5. Permettre l'exercice du droit d'opposition

Objectif : garantir aux personnes la possibilité de s'opposer à l'utilisation de données à caractère personnel (DCP) qui les concernent, conformément à l'article 38 de la [Loi-I&L].

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

- Vérifier que le traitement ne fait pas l'objet d'une exception mentionnée à l'article 38 de la [Loi-I&L] (obligation légale, exclusion dans l'acte portant création du traitement) interdisant à la personne de s'opposer au traitement.
- 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 DCP 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-I&L].
    - *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-I&L], 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-I&L].

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

1.5.1 Spécificités pour un traitement par téléphone

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

- 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.*

1.5.2 Spécificités pour un traitement par formulaire électronique

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

- 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).

1.5.3 Spécificités pour un traitement par courrier électronique

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

- 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.

1.5.4 Spécificités pour des recherches sur des prélèvements biologiques identifiants[9]

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

- 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.

[9] Par exemple l'ADN.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

1.6. Permettre l'exercice du droit d'accès direct

Objectif : garantir aux personnes la possibilité de prendre connaissance des données à caractère personnel (DCP) qui les concernent, conformément à l'article 39 de la [Loi-I&L].

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

- Vérifier que le traitement ne fait pas l'objet d'une exception mentionnée dans les articles 39 et 41 de la [Loi-I&L] (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).
- 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 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 DCP des tiers.

Outillage / Pour aller plus loin

- Voir les articles 92 à 95 et 98 du [Décret-I&L].
- Voir le guide [CNIL-Employeurs].

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

1.6.1 Spécificités pour l'accès aux dossiers médicaux

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

- 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-I&L].

Outillage / Pour aller plus loin

- Voir le [Décret-2002-637].

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

1.7. Permettre l'exercice du droit de rectification

Objectif : garantir aux personnes la possibilité de rectifier, compléter, mettre à jour, verrouiller ou supprimer des données à caractère personnel (DCP) qui les concernent, conformément à l'article 40 de la [Loi-I&L].

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

- Vérifier que le traitement ne fait pas l'objet d'une exception mentionnée à l'article 41 de la [Loi-I&L] (sûreté de l'État, défense ou sécurité publique).
- 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 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…*
- S'assurer que la véracité des rectifications demandées sera vérifiée.
- S'assurer qu'une confirmation sera fournie aux demandeurs.
- S'assurer que les tiers à qui des données auraient été transmises seront informés des rectifications faites.

Outillage / Pour aller plus loin

- Voir les articles 92 à 95 et 99 à 100 du [Décret-I&L].

1.7.1 Spécificités pour la publicité ciblée en ligne

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

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.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

1.8. Cloisonner les DCP

Objectif : réduire la possibilité de corréler des données à caractère personnel (DCP) et de provoquer une violation de l'ensemble des DCP.

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

- Identifier les seules DCP 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…), disposer d'un environnement informatique dédié pour les systèmes traitant des données les plus sensibles…*
- Vérifier de manière régulière que les DCP sont bien cloisonnées, et que des destinataires ou des interconnexions n'ont pas été ajoutés.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

1.9. Chiffrer les DCP

Objectif : rendre les données à caractère personnel (DCP) incompréhensibles à toute personne non autorisée à y avoir accès.

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[10], certains fichiers, des données d'une base de données, un canal de communication…) selon la forme de stockage des DCP, les risques identifiés et les performances exigées[11].
- Choisir le type de chiffrement (symétrique[12] ou asymétrique[13]) 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'ANSSI[14] 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…).

Outillage / Pour aller plus loin

- Voir les exigences relatives à la fonction « Confidentialité » du [RGS].

1.9.1 Spécificités pour un chiffrement symétrique (ou conventionnel)

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

- N'employer une clé que pour un seul usage[15].
- 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 l'algorithme AES[16], employer une taille de blocs traités au moins égale à 128 bits, un mode opératoire de chiffrement non déterministe (tel qu'un mécanisme CBC[17] avec un vecteur d'initialisation aléatoire), des clés*

[10] Un fichier est susceptible de contenir plusieurs fichiers.
[11] Les solutions peuvent être cumulées si les risques sont nombreux ou élevés.
[12] À l'intention des seules personnes disposant d'une clé secrète partagée.
[13] À l'intention des seules personnes choisies parmi celles disposant d'une clé publique connue.
[14] Sous réserve qu'il existe au moins une telle référence au catalogue des produits qualifiés par l'ANSSI. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats d'authentification doit obtenir une dérogation de l'ANSSI.
[15] L'emploi d'une même clé à plus d'un usage, par exemple pour assurer l'intégrité avec un mécanisme de HMAC et assurer la confidentialité avec un mécanisme différent, est source de nombreuses erreurs. Ceci n'interdit cependant pas de différencier localement deux clés à partir d'une même clé secrète, à condition que le mécanisme de diversification soit conforme au [RGS].
[16] *Advanced Encryption Standard*.
[17] *Cipher-block chaining*.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

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[18]*…*

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

1.9.2 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[19].
- 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*[20]*, 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*[21] *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…), 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)…*
- Formaliser la manière dont les clés vont être gérées.
  - *Recommandations : élaborer une « politique de certification » (PC)*[22] *qui précise les responsabilités, l'identification et l'authentification, les exigences*

[18] Avec DES, un exemple de clé faible est tel que l'application de la fonction de chiffrement au message chiffré permet de récupérer le message en clair.
[19] L'emploi d'une même clé à plus d'un usage, par exemple pour assurer l'authenticité avec un mécanisme de signature électronique et assurer l'authentification avec un mécanisme différent, est source de nombreuses erreurs. Ceci n'interdit cependant pas de différencier localement deux clés à partir d'une même clé secrète, à condition que le mécanisme de diversification soit conforme au [RGS].
[20] *RSA Encryption Scheme - Optimal Asymmetric Encryption Padding*.
[21] Voir http://www.lsti-certification.fr/index.php?option=com_content&view=article&id=54&Itemid=14&lang=fr.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

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.

1.9.3 Spécificités pour le chiffrement de matériels

Objectif : rendre les DCP 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[23]…).

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[24], ou des logiciels tels que dm-crypt sous Linux, FileVault sous MacOS, TrueCrypt 6.0a sous Windows.*
- Privilégier les dispositifs ne stockant pas les clés sur le matériel à chiffrer.

1.9.4 Spécificités pour le chiffrement de bases de données

Objectif : rendre les DCP 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[25].

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

- Selon les risques identifiés, chiffrer au niveau d'une base de données, de l'application qui accède à une base de données ou de certaines données d'une base de données.

1.9.5 Spécificités pour le chiffrement de partitions ou de conteneurs

Objectif : rendre les DCP 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…), 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 ou d'un conteneur).

---

[22] Des politiques de certifications types sont disponibles sur le site de l'ANSSI, notamment dans les annexes A6 à A12 du RGS.

[23] Clé USB, disque dur externe, CD-ROM, DVD-ROM, supports de sauvegarde…

[24] *Self-Encrypted Drive*.

[25] En l'absence de chiffrement, les administrateurs ont un accès immédiat à l'intégralité des données stockées en base, et ils sont capables de faire des recherches sur ces données. Ainsi, un administrateur d'une base contenant des données de santé peut très facilement faire des recherches sur un NIR ou un nom et prénom, et accéder ensuite au dossier médical de la personne.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- *Recommandations : utiliser des logiciels tels que TrueCrypt 6.0a ou Zed ! 4.0.*

1.9.6 Spécificités pour le chiffrement de fichiers isolés

Objectif : rendre les DCP 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 3.1, 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…*

1.9.7 Spécificités pour le chiffrement de courriers électroniques

Objectif : rendre les DCP 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).*

1.9.8 Spécificités pour le chiffrement d'un canal de communication

Objectif : rendre les DCP 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[26], anciennement SSL[27] (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[28] pour mettre en place un tunnel sécurisé (VPN[29]), ou encore des solutions de chiffrement IP[30] (VPN-IPSec)…*

[26] *Transport Layer Security*.
[27] *Secure Sockets Layer*.
[28] *Secure Shell*.
[29] *Virtual Private Network*, Réseau privé virtuel.
[30] Voir la liste des produits qualifiés : http://www.ssi.gouv.fr/fr/produits/produits-qualifies/.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

1.10. Anonymiser les DCP

Objectif : faire perdre le caractère identifiant des données à caractère personnel (DCP)[31].

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 DCP (champs d'une base de données, extraits de textes…) et les risques identifiés.
- Anonymiser de manière irréversible[32] ce qui doit l'être, selon la forme des données à anonymiser (base de données, documents textuels…) 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…) qui satisfont le mieux possible les besoins fonctionnels.

Outillage / Pour aller plus loin

- Il peut être utile de formaliser les exigences en matière d'anonymisation de manière plus détaillée afin de choisir les outils appropriés : la robustesse attendue face aux attaques par inférences[33] en fonction des risques identifiés et de la population concernée[34].
- La CNIL a émis des délibérations spécifiques à certains cas, il peut être utile de vérifier l'adéquation des mesures choisies vis-à-vis des recommandations de la Commission. Par exemple, l'avis de la CNIL vis-à-vis de l'anonymisation des jugements et arrêts librement accessibles sur Internet est formalisé dans la délibération 01-57 du 29 novembre 2001.

Notes

- Une « véritable » anonymisation implique nécessairement une perte (irréversible) d'information. Dans certains cas, le simple fait d'effacer ou de noircir une partie des données peut suffire à atteindre l'objectif souhaité.
- La « pseudonymisation » peut être définie comme le remplacement d'un nom par un pseudonyme. C'est le processus par lequel les données perdent leur caractère identifiant (de manière directe). Les données restent liées à la même personne dans tous les dossiers et systèmes informatiques sans que l'identité ne soit révélée. Elle peut être opérée avec ou sans la possibilité de retour vers les noms ou identités (pseudonymisation réversible ou irréversible).
- Il convient de garder à l'esprit que la corrélation de DCP anonymisées reste possible et qu'une ré-identification peut intervenir à partir d'informations partielles dès lors qu'une DCP est anonymisée et non purement supprimée. En effet, il est possible d'associer la donnée originale à la donnée anonymisée dès lors que le secret est compromis et que la complexité de la donnée originale n'est pas suffisante[35].

[31] C'est-à-dire faire en sorte qu'il ne soit pas possible de faire le lien entre une DCP et la personne physique à laquelle elle se rapporte.
[32] Les données sont anonymisées sans que qui que ce soit ne puisse retrouver les données originales.
[33] Pour limiter les attaques par inférences ou attaques sur des clés de chiffrement, on peut aussi changer régulièrement les clés d'anonymisation.
[34] À titre d'exemple, la ville et la date de naissance peuvent parfois suffire à identifier formellement une personne.
[35] Par exemple, les patronymes français sont en nombre limité (moins de 1,5 millions) et tous répertoriés.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- Il faut distinguer l'anonymisation en tant que bonne pratique de sécurité du « procédé d'anonymisation » au sens de la [Loi-I&L], notamment dans ses articles 8-III, 11-3 et 32-IV. Pour qu'un « procédé d'anonymisation » soit reconnu conforme à la loi par la CNIL, il est généralement nécessaire de pratiquer une véritable anonymisation par une suppression de données, ou de réaliser une « pseudonymisation » accompagnée de garanties organisationnelles et techniques fortes, notamment par l'utilisation de fonctions de hachage à clé secrète.

1.10.1 Spécificités pour les bases de données

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

- Anonymiser de manière irréversible les DCP qui peuvent l'être.
  - *Recommandations : supprimer une partie suffisante des données (ex. : ne garder qu'une année de naissance et non la date de naissance complète pour éviter qu'on retrouve l'identité d'une personne en connaissant en plus son lieu de naissance et son sexe, supprimer les deux derniers octets d'une adresse IPv4), appliquer une fonction de hachage à clé secrète et supprimer la ou les clés secrètes, ou encore remplacer les DCP qui permettent d'identifier les personnes par un texte neutre (étoiles, quelques lettres identiques, identifiant séquentiel…)…*
- Si ce n'est pas possible, déterminer les solutions qui satisfont le mieux possible les besoins fonctionnels.
  - *Recommandations :*
    - *s'il est nécessaire que des personnes habilitées puissent vérifier que des données anonymisées correspondent à des données originales qu'ils ont en leur possession, utiliser une fonction de hachage SHA-256 avec une clé secrète[36] (HMAC[37]), voire pratiquer une double anonymisation avec deux clés secrètes détenues par deux organismes différents[38] ;*
    - *s'il est nécessaire à des personnes habilitées de pouvoir retrouver les données originales (levée d'anonymat), utiliser une fonction de chiffrement, éventuellement en partageant une clé en trois parties confiées à trois personnes différentes (par exemple sur un CD ou une carte à puce) avec l'obligation qu'au moins deux des trois personnes se réunissent pour reconstituer la clé, afin de protéger la confidentialité du secret…*
- Utiliser uniquement des DCP anonymisées ou des données fictives pour les phases de développement et de test.

[36] Attention à la protection de la clé secrète, qui peut être utilisée pour retrouver la donnée hachée correspondant à une identité.
[37] *Keyed-Hashing for Message Authentication*.
[38] Une double anonymisation réversible consiste à appliquer une seconde anonymisation sur le résultat d'une première anonymisation. Ces deux anonymisations doivent utiliser des secrets différents, détenus par des organismes distincts. L'algorithme FOIN (Fonction d'Occultation des Informations Nominatives) est un exemple d'algorithme à double anonymisation.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- *Recommandations : utiliser des logiciels spécialisés pour créer des jeux de tests anonymisés.*

Notes

- Définir les mesures techniques et organisationnelles de protection des secrets (clés, tables de correspondance…) qui permettent si nécessaire de lever l'anonymat en garantissant que cela ne puisse être fait que par le détenteur des secrets (séparation et stockage des clés dans des coffres ignifugés, journalisation des accès…).
- Dans certains cas, il est conseillé d'appliquer une double anonymisation : c'est l'application d'une seconde fonction d'anonymisation sur la donnée anonymisée au moyen de la première fonction d'anonymisation. Ces deux fonctions doivent utiliser des secrets différents qui sont détenus par des organismes distincts.

Outillage / Pour aller plus loin

- Voir l'[ISO-25237] et l'[AFNOR-97-560].
- Voir les exigences relatives aux mécanismes cryptographiques du [RGS].

1.10.2 Spécificités pour les documents électroniques textuels

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

- Utiliser un dispositif d'anonymisation conforme au référentiel [AFCDP-Anonymisation].
- Vérifier manuellement les textes anonymisés à l'aide du dispositif choisi afin de corriger les éventuelles anomalies et d'améliorer le paramétrage du dispositif.

Outillage / Pour aller plus loin

- Voir la délibération [CNIL-DiffJurisprudence].
- Il existe plusieurs outils logiciels permettant d'identifier les DCP et de proposer une anonymisation (assistant d'anonymisation de E-DOC LABS, *Insight Discoverer Extractor* de Temis, la macro NOME de LexUm et l'Université de Montréal, le programme PIVOINE de l'Agence technique de l'information sur l'hospitalisation – ATIH…).

Notes

- Dans l'état actuel, les logiciels précités apportent une aide à l'anonymisation de documents, mais ils requièrent une action de la part de l'utilisateur (paramétrage et vérification visuelle).

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

2. Agir sur les impacts

2.1. Sauvegarder les DCP

Objectif : assurer la disponibilité et/ou l'intégrité des données à caractère personnel (DCP), tout en protégeant leur confidentialité.

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

- Effectuer une sauvegarde des DCP, 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 DCP 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…) 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…)…*
- 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 DCP sauvegardées si les besoins des métiers le nécessitent.
  - *Recommandations : la fonction de hachage SHA-256 est utilisée pour réaliser une empreinte des DCP sauvegardée, voire une signature électronique…*
- 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.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Notes

- Les transferts, et donc les sauvegardes, de DCP vers des pays situés en-dehors de l'Union européenne sont interdits sauf[39] :
  - 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 *Safe Harbor* ;
  - si l'une des exceptions prévues par l'article 69 de la [Loi-I&L] est invoquée.

Le site de la CNIL maintient une carte du monde indiquant les formalités à accomplir en fonction du pays visé[40]. Dans tous les cas, le responsable du traitement reste responsable de la sécurité des DCP sauvegardées.

[39] Chacun de ces points juridiques est détaillé sur le site de Cnil : http://www.cnil.fr/vos-responsabilites/le-transfert-de-donnees-a-letranger/
[40] http://www.cnil.fr/pied-de-page/liens/les-autorites-de-controle-dans-le-monde/

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

2.2. Protéger les archives de DCP[41]

Objectif : définir l'ensemble des modalités de conservation et gestion d'archives électroniques contenant des données à caractère personnel (DCP) destinées à garantir leur valeur, notamment juridique, pendant toute la durée nécessaire.

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…), 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 DCP archivées selon les risques identifiés.
  - *Recommandations : chiffrer systématiquement les DCP sensibles[42] 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 politique d'archivage.*

[41] Les modalités d'archivage différent de celles utilisées pour l'utilisation courante des données et leur sauvegarde du fait que l'utilisation d'une archive doit intervenir de manière ponctuelle et exceptionnelle.
[42] Données sensibles au sens de l'article 8 et les données relevant de l'article 9.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Outillage / Pour aller plus loin

- Voir le guide [ANSSI-Archivage] et la norme [NF-42-013].
- Voir le site des Archives de France[43].

2.3. Contrôler l'intégrité des DCP

Objectif : être alerté en cas de modification non désirée ou de disparition de données à caractère personnel (DCP).

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[44] (MAC[45]) 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…*
- 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)…*

2.3.1 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 [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…*

[43] http://www.archivesdefrance.culture.gouv.fr/gerer/archives-electroniques.
[44] Code accompagnant des données dans le but d'assurer l'intégrité de ces dernières, en permettant de vérifier qu'elles n'ont subi aucune modification.
[45] *Message Authentication Code*, code d'authentification de message.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

2.3.2 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[46] « 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 »).*

2.3.3 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'ANSSI[47], 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[48], ou bien ECDSA[49] en utilisant l'une des courbes P-256, P-384, P-521, B-283, B-409 ou B-571…*
- Générer les clés conformément au [RGS].
  - *Recommandations : avoir recours à un prestataire de service de certification électronique (PSCE) référencé[50] comme conforme au [RGS] dans sa version 1.0 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.

[46] *Cipher-block chaining - Message Authentication Code*.
[47] Sous réserve qu'il existe au moins une telle référence au catalogue des produits qualifiés par l'ANSSI. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats d'authentification doit obtenir une dérogation de l'ANSSI.
[48] *RSA Signature Scheme with Appendix – Provably Secure encoding method for digital Signatures*.
[49] *Elliptic Curve Digital Signature Algorithm*.
[50] Voir http://www.lsti-certification.fr/index.php?option=com_content&view=article&id=54&Itemid=14&lang=fr.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- *Recommandations : élaborer une « politique de certification » (PC) 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….*

Outillage / Pour aller plus loin

- Voir les explications de l'ANSSI sur la signature électronique[51].
- Voir les exigences relatives à la fonction « Signature électronique » du [RGS].

Note

- 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.

[51] Voir http://www.ssi.gouv.fr/site_rubrique59.html.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

2.4. Tracer l'activité sur le système informatique

Objectif : être capable de détecter les incidents concernant des données à caractère personnel (DCP) de façon précoce, et de disposer d'éléments exploitables pour les étudier ou pour fournir des preuves dans le cadre d'enquêtes.

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 journalisés en prenant comme référence le temps UTC[52], utiliser une source de temps fiable sur laquelle les équipements se synchroniseront, telle qu'un serveur NTP[53] ou une radio-synchronisation, 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…*
- Choisir les événements à journaliser en fonction du contexte, des supports (postes de travail, pare-feu, équipements réseau, serveurs…), 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[54] , avec un devoir strict de confidentialité, respecter le [Décret-LCEN] en cas de création de contenu en ligne[55]…*
- Respecter les exigences de la [Loi-I&L] si les événements journalisés comprennent des DCP.
  - *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…*
- 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.

[52] *Coordinated Universal Time*.
[53] *Network Time Protocol*.
[54] 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.
[55] 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.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

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 [RGS] est à considérer.

2.4.1 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…), 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…)…*
- 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.

2.4.2 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…*
- Exporter les journaux par un canal sécurisé vers un serveur dédié.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

2.4.3 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[56]) pour les routeurs.

2.4.4 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…
    - *Recommandations : connexions réussies, méthodes de connexion, requêtes effectuées, volumétries, répartition par pays des requêtes…*
- 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.

[56] *Access Control Lists*.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

2.5. Gérer les violations de DCP

Objectif : 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.

De la violation de données à caractère personnel (DCP)

« Violation de données à caractère personnel : une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière… »

(Modification de la [Directive-2002-58] prévue dans la [Directive-2009-136])

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 DCP.
  - *Recommandations : formaliser les responsabilités du référent « Informatique et libertés » (CIL 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 DCP.
- Élaborer un plan de réaction en cas de violation de DCP 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 DCP selon leur impact sur les libertés et la vie privée des personnes concernées.
  - *Recommandations : un simple événement est une violation de DCP sans conséquence, un incident correspond à une violation de DCP avec des conséquences isolées, un sinistre à une violation de DCP avec des conséquences immédiates importantes pour une ou plusieurs personnes, une crise à une violation de DCP avec des conséquences importantes et à plus long terme sur une ou plusieurs personnes…*
- Traiter les événements selon leur qualification (événement, incident, sinistre, crise…).
  - *Recommandations :*
    - *s'il s'agit d'un événement, le consigner et avertir le référent « Informatique et libertés » (CIL ou équivalent) ;*
    - *s'il s'agit d'un incident, le résoudre en plus et si possible[57] notifier les personnes concernées par la violation ;*

[57] La notification d'une violation des DCP n'est pas nécessaire 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

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- *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 un inventaire des violations de DCP.
  - *Recommandations : consigner le contexte des violations de DCP, leurs effets, les mesures prises pour y remédier…*
- Étudier la possibilité d'améliorer les mesures de sécurité en fonction des violations de DCP 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 DCP à la CNIL. Cette obligation pourrait à terme concerner tous les responsables de traitements et pas uniquement les « fournisseurs de services de communications électroniques accessibles au public ». Ces textes définissent la forme des notifications :
  - la notification des personnes concernées décrit au minimum la nature de la violation de DCP 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 DCP ;
  - 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.
- 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].

protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

3. Agir sur les sources de risques

3.1. S'éloigner des sources de risques

Objectif : éviter que des sources de risques, humaines ou non humaines, auxquelles il est possible de ne pas être confronté, portent atteinte aux données à caractère personnel (DCP).

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

- Placer les produits dangereux (inflammables, combustibles, corrosifs, explosifs, aérosols, humides…) dans des lieux de stockage appropriés et éloignés de ceux où sont traitées des DCP.
- Éviter les zones géographiques dangereuses (zones inondables, proximité d'aéroports, zones d'industries chimiques, zones sismiques, zones volcaniques…).
- 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 (BCR[58]) 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 *Safe Harbor* ou si l'une des exceptions prévues par l'article 69 de la [Loi-I&L] est invoquée. Dans tous les cas, le responsable du traitement reste responsable de la sécurité des DCP stockées et doit s'assurer du niveau de sécurité du stockage.

[58] *Binding Corporate Rules*.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

3.2. Marquer les documents contenant des DCP

Objectif : susciter une conduite prudente des personnes ayant accès aux documents (papier ou électroniques) en identifiant clairement ceux qui contiennent des données à caractère personnel (DCP).

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 papier ou électroniques qui contiennent des DCP sensibles[59].
  - *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 ».*
- Porter une mention visible et explicite dans l'objet des courriers électroniques qui contiennent des DCP sensibles.
  - *Recommandations : ajouter « [Données à caractère personnel] ».*
- Porter une mention visible et explicite dans les applications métiers permettant d'accéder à des DCP.
  - *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 DCP rappelant à l'expéditeur qu'il manipule des DCP 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 DCP 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.

[59] Données sensibles au sens de l'article 8 et les données relevant de l'article 9.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

3.3. Gérer les personnes internes qui ont un accès légitime

Objectif : réduire les risques liés à des personnes internes (collaborateurs, sous-traitants en régie, stagiaires, visiteurs…) ayant un accès légitime aux données à caractère personnel (DCP).

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

- Déterminer les rôles et responsabilités en matière de protection des DCP.
- Déterminer les conséquences prévues pour les personnes ayant un accès légitime aux DCP en cas de non respect des mesures.
- Rédiger une charte informatique et l'annexer au règlement intérieur de l'organisme.
- Déterminer la procédure à appliquer systématiquement à l'arrivée d'une personne ayant un accès légitime aux DCP.
    - *Recommandations : attribution d'un poste de travail, ouverture d'un compte informatique, fourniture des moyens d'accès physiques, attribution d'un profil utilisateur…*
- Obtenir l'engagement des personnes ayant un accès légitime aux DCP à respecter les mesures déterminées.
    - *Recommandations : faire signer un engagement de confidentialité ou prévoir dans les contrats de travail une clause de confidentialité spécifique concernant les données à caractère personnel…*
- Sensibiliser les personnes ayant un accès légitime aux DCP aux risques liés aux libertés et à la vie privée, aux mesures prises pour les traiter et aux conséquences prévues en cas de manquement et ce, de manière régulière.
    - *Recommandations : organiser une séance de sensibilisation annuelle, envoyer régulièrement les mises à jour des politiques et procédures pertinentes pour les fonctions des personnes, faire des rappels par messagerie électronique…*
- Former convenablement les personnes ayant un accès légitime aux DCP aux outils qu'ils manipulent dans le cadre de leur activité professionnelle.
- Documenter les procédures d'exploitation, les tenir à jour et les rendre disponibles 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).
- Déterminer la procédure à appliquer systématiquement au départ ou au changement d'affectation d'une personne ayant un accès légitime aux DCP.
    - *Recommandations : restitution du poste de travail, fermeture ou modification du compte informatique, restitution des moyens d'accès physiques, restitution des matériels et documents comportant des DCP…*

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Outillage / Pour aller plus loin

Modèle de plan d'une charte informatique

1. Le rappel des règles de protection des données et les sanctions encourues en cas de non respect de la loi.

2. Le champ d'application de la charte, qui inclut notamment :
   - ❑ les modalités d'intervention du service de l'informatique interne ;
   - ❑ les moyens d'authentification ;
   - ❑ les règles de sécurité auxquelles se conformer, ce qui peut inclure par exemple :
     - o signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ;
     - o ne jamais confier son identifiant/mot de passe à un tiers ;
     - o ne pas modifier les paramétrages du poste de travail ;
     - o ne pas installer, copier, modifier, détruire des logiciels sans autorisation ;
     - o verrouiller son ordinateur dès que l'on quitte son poste de travail ;
     - o ne pas accéder, tenter d'accéder, ou supprimer des informations qui ne relèvent pas des tâches incombant à l'utilisateur ;
     - o définir les modalités de copie de données sur un support externe, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant des règles préalablement définies.

3. Les modalités d'utilisation des moyens informatiques et de télécommunications mis à disposition comme :
   - ❑ le poste de travail ;
   - ❑ les équipements nomades ;
   - ❑ l'espace de stockage individuel ;
   - ❑ le réseau local ;
   - ❑ internet ;
   - ❑ la messagerie électronique ;
   - ❑ le téléphone.

4. Les conditions d'administration du système d'information, et l'existence, le cas échéant, de:
   - ❑ systèmes automatiques de filtrage ;
   - ❑ systèmes automatiques de traçabilité ;
   - ❑ gestion du poste de travail.

5. Les responsabilités et sanctions

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Exemple d'engagement de confidentialité relatif aux données à caractère personnel

Je soussigné Monsieur/Madame _____, exerçant les fonctions de _____ au sein de la société _____ (ci-après dénommée « la Société »), étant à ce titre amené à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.

Je m'engage par conséquent, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient modifiées, endommagées ou communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité de matérielle de ces données ;
- m'assurer, dans la limite des mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- assurer, dans la limite de mes attributions, l'exercice des droits d'information, d'accès et de rectification de ces données ;
- en cas de cessation des mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.
- [compléter si besoin]

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose notamment à des actions et sanctions disciplinaires et pénales conformément aux dispositions légales en vigueur.

Fait à xxx le xxx en xxx exemplaires

Nom :
Signature :

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

3.4. Contrôler l'accès logique des personnes

Objectif : limiter les risques que des personnes non autorisées accèdent aux données à caractère personnel (DCP) par voie électronique.

3.4.1 Gérer les privilèges[60] des utilisateurs sur les DCP

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 DCP aux seuls utilisateurs habilités, en appliquant les principes du besoin d'en connaître[61] et du moindre privilège[62].
    - *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 DCP (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…*
- 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…).*
- 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.
- 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.

[60] Droits de créer des données, d'y accéder, de les modifier, de les copier, de les transférer, de les supprimer…
[61] Chaque utilisateur n'est autorisé à accéder qu'aux ressources nécessaires à l'accomplissement de ses missions.
[62] Chaque utilisateur accède aux ressources avec le minimum de privilèges lui permettant de conduire les actions nécessaires à ses missions.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- 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.

3.4.2 Authentifier les personnes désirant accéder aux DCP

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[63] (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.
- Limiter l'authentification par identifiants et mots de passe au contrôle de l'accès au poste de travail (déverrouillage uniquement)[64].
- 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…) 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 DCP.
- La [Loi-I&L] 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…) ou l'enregistrement des empreintes digitales dans un support individuel.

[63] *One-time password*.
[64] Un tel mécanisme constitue un mécanisme de déverrouillage et non pas un réel mécanisme d'authentification.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Outillage / Pour aller plus loin

- Voir les exigences relatives à la fonction « Authentification » du [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.

3.4.3 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[65].
- 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'ANSSI[66], 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[67], ou bien ECDSA[68] en utilisant l'une des courbes P-256, P-384, P-521, B-283, B-409 ou B-571*
- Générer les clés conformément au [RGS].
  - *Recommandations : avoir recours à un prestataire de service de certification électronique (PSCE) référencé[69] 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 » (PC) qui précise les responsabilités, l'identification et l'authentification, les exigences*

[65] L'emploi d'une même clé à plus d'un usage, par exemple pour chiffrer avec un mécanisme de confidentialité et assurer l'intégrité avec un mécanisme différent, est source de nombreuses erreurs. Ceci n'interdit cependant pas de différencier localement deux clés à partir d'une même clé secrète, à condition que le mécanisme de diversification soit conforme au [RGS].

[66] Sous réserve qu'il existe au moins une telle référence au catalogue des produits qualifiés par l'ANSSI. Dans le cas contraire, le PSCE souhaitant faire qualifier son offre de certificats d'authentification doit obtenir une dérogation de l'ANSSI.

[67] *RSA Signature Scheme with Appendix – Provably Secure encoding method for digital Signatures*.

[68] *Elliptic Curve Digital Signature Algorithm*.

[69] Voir http://www.lsti-certification.fr/index.php?option=com_content&view=article&id=54&Itemid=14&lang=fr.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

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….

3.4.4 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 sont constitués de dix caractères minimum, les mots de passe doivent être renouvelés tous les trois mois, 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, ne jamais 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…), configurer les logiciels pour qu'ils ne retiennent jamais les mots de passe, 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)…*
- Donner la possibilité aux utilisateurs de changer leurs mots de passe.
- 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.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- *Recommandations : limiter les droits d'accès (lecture, écriture…) 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…) doivent être utilisés, mettre en place une solution d'authentification centralisée[70], de mots de passe à usage unique[71] 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…), affichage sécurisé des mots de passe (masquage des mots de passe dans les boîtes de connexion…), résistance aux attaques (déchiffrement, force brute, rejeu…), fermeture ou blocage automatique (après une certaine durée, lors de la mise en veille sécurisée…)…*
- 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…).

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].
- Voir les exigences relatives à la fonction « Authentification » du [RGS].

[70] *Single Sign-On* (SSO).
[71] *One-Time Password* (OTP).

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

3.5. Gérer les tiers qui ont un accès légitime aux DCP

Objectif : réduire les risques que les accès légitimes aux données à caractère personnel (DCP) par des tiers peuvent faire peser sur les libertés et la vie privée des personnes concernées.

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 DCP.
  - *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 prestataire, bien qu'il puisse être considéré comme responsable de traitement dans certains cas.*
- Déterminer les responsabilités respectives en fonction des risques liés à ces DCP.
  - *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 »).*
- Apprécier précisément les risques spécifiques que les accès aux DCP par ces personnes peuvent faire peser sur les libertés et la vie privée des personnes concernées.
- 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 DCP, selon la catégorie de personnes et les actions qu'elles vont réaliser.
- Déterminer une procédure à suivre pour les requêtes de tiers autorisés.
  - *Recommandations : s'assurer de la conformité des requêtes aux textes invoqués, décrire le(s) protocole(s) à suivre pour répondre aux requêtes en minimisant les risques induits, authentifier les émetteurs des requêtes …*

Outillage / Pour aller plus loin

- Voir [CNIL-TransfertHorsUE] et [CNIL-ExternaliserHorsUE] pour le cas de transferts de DCP en dehors de l'Union européenne.

3.5.1 Spécificités pour une sous-traitance

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

- Formaliser les règles relatives à la protection de la confidentialité des données personnelles confiées à un tiers.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- *Recommandations : le tiers ne doit réaliser aucune copie des documents et supports d'informations qui sont confiés, à l'exception de celles nécessaires à l'exécution de la prestation prévue, obtenir l'accord préalable du responsable de traitement pour toute opération, ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées, ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales, prendre toutes les mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques, prendre toutes les mesures de sécurité, notamment matérielles, pour assurer la conservation et l'intégrité des documents et des informations traités pendant la durée de la relation, et en fin de relation, procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies…*

- Prendre des dispositions afin de s'assurer de l'effectivité des garanties offertes par le sous-traitant en matière de protection des données (chiffrement des données selon leur sensibilité ou, à défaut, existence de procédures garantissant que la société de prestation n'a pas accès aux données qui lui sont confiées, chiffrement de la liaison de données en utilisant TLS, SSL ou équivalent, garanties en matière de protection du réseau, traçabilité, gestion des habilitations, authentification…).
  - *Recommandations : mener des audits de sécurité, visiter les installations, exiger une certification de la manière dont sont gérées la sécurité et/ou les DCP, obtenir des bilans réguliers ou des comptes-rendus d'audits…*
- Se donner les moyens opérationnels et contractuels pour pouvoir réellement arrêter la relation avec le prestataire notamment en cas de rupture de contrat.
- Formaliser les conditions de restitution des données et de leur destruction en cas de rupture ou à la fin du contrat.

Notes

- L'article 35 de la [Loi-I&L] dispose que « Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données » et prévoit que « le sous-traitant ne peut agir que sur instruction du responsable de traitement ».

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Outillage / Pour aller plus loin

Modèle de clauses de confidentialité pouvant être utilisées notamment en cas de sous-traitance

Les supports informatiques et documents fournis par la société X à la société Y restent la propriété de la société X.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal), il en va de même pour toutes les données dont Y prend connaissance à l'occasion de l'exécution du présent contrat.

Conformément à l'article 34 de la loi informatique et libertés modifiée, Y s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

Y s'engage donc à respecter les obligations suivantes et à les faire respecter par son personnel :

- ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la présente prestation prévue au contrat, l'accord préalable du maître du fichier est nécessaire ;
- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;
- ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- prendre toutes mesures de sécurité, notamment matérielles, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du présent contrat ;
- et en fin de contrat, à procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.

À ce titre, Y ne pourra sous-traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché sans l'accord préalable de X.

X se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par Y.

En cas de non-respect des dispositions précitées, la responsabilité du titulaire peut également être engagée sur la base des dispositions des articles 226-5 et 226-17 du nouveau code pénal.

X pourra prononcer la résiliation immédiate du contrat, sans indemnité en faveur du titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

3.5.2 Spécificités pour une externalisation

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

- Étudier les risques afin de mesurer les enjeux d'une externalisation et de vérifier qu'il n'est pas préférable de réduire le périmètre, voire de ne pas externaliser.
- Contractualiser les règles relatives à l'externalisation de tout ou partie du système d'information.
    - *Recommandations : formaliser les règles relatives à la localisation des données, au transfert des données pour l'initialisation du service, à la confidentialité, à la sécurisation du réseau, à l'accès aux services et aux moyens d'accès, à la gestion des identifiants, à la disponibilité et à la continuité de services, aux conditions de maintenance par le fournisseur, à la gestion des évolutions et à la maintenance corrective de sécurité, au traitement des données, aux audits et tests intrusifs, à la propriété des données, aux assurances, à la réversibilité, à la gestion des cascades de sous-traitants, à la gouvernance et au suivi de la relation contractuelle, à l'interdiction de diminuer le niveau de sécurité pour des raisons économiques…*

Notes

- Le recours à des services offrant des fonctionnalités d'informatique répartie (*cloud computing*) requiert des garanties quant à la localisation géographique des données (France, Union européenne, hors Union européenne).

Outillage / Pour aller plus loin

- Voir [CNIL-ExternaliserHorsUE].
- Voir le guide [ANSSI-Externalisation].

3.5.3 Spécificités pour un hébergement mutualisé

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

- Étudier les risques afin de mesurer les enjeux d'un co-hébergement et de vérifier qu'il n'est pas préférable de disposer d'une plate-forme dédiée, gérée par l'organisme.
- Contractualiser les règles d'accès aux journaux d'événements (soit dans le cas d'un incident, soit à des fins de suivi des ressources hébergées).
    - *Recommandations : pouvoir accéder aux journaux d'événements dans la journée, voire disposer d'un moyen de suivi des événements en temps réel, avoir une garantie de confidentialité relative aux journaux, obtenir la certification de l'hébergeur que toutes les informations présentes sur les journaux sont exploitables au regard de l'état de l'art…*
- Contractualiser les règles de suivi de la ressource co-hébergée.
    - *Recommandations : pouvoir disposer d'indicateurs sur l'historique de la ressource hébergée (fréquence et suivi des mises à jour effectuées, durée d'indisponibilité maximum et suivi de ces indisponibilités, fréquence des sauvegardes et tests de restauration effectués, charge réseau pour le serveur*

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

et pour la ressource, charge processeur utilisée par la ressource et pourcentage de la charge du serveur, charge mémoire utilisée par la ressource et pourcentage de la charge du serveur…), avoir connaissance de l'origine et de la teneur des ressources co-hébergées, si possible n'héberger sur un serveur donné que des DCP appartenant toutes à une même organisation ou communauté d'intérêts…

- Contractualiser les règles de gestion des attaques informatiques.
  - *Recommandations : identifier un contact technique et un contact décisionnel au sein de l'organisme et chez l'hébergeur, joignables toute l'année, 24h sur 24, 7 jours sur 7, avoir une garantie d'information immédiate en cas d'attaque, définir ce que l'on entend par incident de sécurité et les procédures de remontée d'incident…*
- Contractualiser les règles de gestion des incidents.
  - *Recommandations : pouvoir désigner l'organisme chargé de traiter l'incident, qui devra pouvoir jouir au nom du client d'un contrôle total de l'environnement de la ressource à des fins d'analyse (prélèvement de tout élément nécessaire à l'analyse conformément aux règles de l'art, analyse du système en fonctionnement…), pouvoir gérer l'incident et conduire les actions postérieures (redémarrage, arrêt, rétablissement d'une sauvegarde, isolement physique d'une machine du reste du réseau, établissement d'un périmètre de sécurité, délai d'indisponibilité de la ressource, délai d'indisponibilité du serveur et pénalités d'astreinte éventuelles, contrôle sur les règles de filtrage…)…*
- Contractualiser les règles de réversibilité.
  - *Recommandations : une clause de réversibilité, activable notamment pour des raisons de sécurité (changement dans l'actionnariat du prestataire, de délocalisation des sites d'hébergement…) doit permettre à l'organisme de récupérer la gestion de ses ressources, le prestataire doit s'engager à apporter son assistance durant toute la période de migration, à garantir la sécurité des données et des applications qui lui ont été confiées lors de leur transfert, à restituer ou à tenir à disposition tout élément correspondant à un extrait de l'ancien environnement d'hébergement (journaux d'événements déportés, sauvegardes…) pendant une période à déterminer…*

Notes

- Concernant les données de santé, il est rappelé qu'un hébergeur se doit d'obtenir un agrément préalable délivré par le ministre de la Santé. Le référentiel de constitution d'un dossier est disponible sur le site http://esante.gouv.fr/.

Outillage / Pour aller plus loin

- Voir la note [CERTA-Mutualisé].

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

3.5.4 Spécificités pour une maintenance

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

- Chiffrer ou effacer les DCP de manière sécurisée avant l'envoi en maintenance externe de toute ressource informatique (serveur, poste client, équipement réseau…).
- Si les DCP ne peuvent être chiffrées ou effacées dans leur totalité (panne d'un disque dur, dysfonctionnement…) et que les DCP ne sont pas sensibles[72], faire signer un engagement de confidentialité au fournisseur de service de maintenance, ou bien faire faire les réparations sur place en présence d'un membre du service en charge de l'informatique.
- Dans le cas de DCP sensibles[73], interdire l'envoi en maintenance externe, faire des réparations sur place en présence d'un membre du service en charge de l'informatique et enregistrer les interventions dans une main courante.
- Dans le cas d'une maintenance sur site, enregistrer les travaux de maintenance dans une main courante, faire encadrer l'intervention par un responsable de l'organisme, configurer les systèmes de telle sorte qu'une télémaintenance ne soit pas possible.

Modèle de clauses de confidentialité pouvant être utilisées en cas de maintenance par une tierce partie

Chaque opération de maintenance devra faire l'objet d'un descriptif précisant les dates, la nature des opérations et les noms des intervenants, transmis à X.

En cas de télémaintenance permettant l'accès à distance aux fichiers de X, Y prendra toutes dispositions afin de permettre à X d'identifier la provenance de chaque intervention extérieure. A cette fin, Y s'engage à obtenir l'accord préalable de X avant chaque opération de télémaintenance dont elle prendrait l'initiative.

Des registres seront établis sous les responsabilités respectives de X et Y, mentionnant les dates et natures détaillées des interventions de télémaintenance ainsi que les noms de leurs auteurs.

3.5.5 Spécificités pour une télémaintenance

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

- Faire signer un engagement de confidentialité par le tiers externe.
- Mettre en place des mots de passe robustes, spécifiques et renouvelés régulièrement.
- Activer les accès entrant en télémaintenance uniquement sur demande, les accès entrants étant inactifs par défaut.
- Chiffrer le canal de communication (ex : SSH ou équivalent).
- Journaliser les accès en télémaintenance.

[72] Données sensibles au sens de l'article 8 et les données relevant de l'article 9.
[73] Données sensibles au sens de l'article 8 et les données relevant de l'article 9.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- Interdire les possibilités de rebond depuis l'accès en télémaintenance vers le reste du réseau local et plus largement vers les réseaux interurbains (WAN) nationaux.

3.6. Lutter contre les codes malveillants

Objectif : 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 les données à caractère personnel (DCP).

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[74]…)*
- 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…).
- 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…).
- 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 [CERTA-Virus].

[74] Dans le respect des règles liées au développement durable et concernant notamment l'extinction des ordinateurs.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

3.7. Contrôler l'accès physique des personnes

Objectif : limiter les risques que des personnes non autorisées n'accèdent physiquement aux données à caractère personnel (DCP).

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…), une zone réservée au service (zone à accès contrôlé correspondant aux bureaux où sont traitées les DCP), 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…) 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…) 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…).
  - *Recommandations : refuser l'accès au visiteur, prévenir la personne en charge de la sécurité…*
- 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…*

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- Faire accompagner les visiteurs, en dehors des zones d'accueil du public[75] 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…) 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.

[75] Depuis leur entrée, pendant leur visite et jusqu'à leur sortie des locaux.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

3.8. Se protéger contre les sources de risques non humaines

Objectif : réduire ou éviter les risques liés à des sources non humaines (virus informatiques, phénomènes climatiques, incendie, dégât des eaux, accidents internes ou externes, animaux…) qui pourraient affecter la sécurité des données à caractère personnel (DCP).

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…), 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…), 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…)…*
- S'assurer que les services essentiels (électricité, eau, climatisation…) 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…) 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 (CNPP), de l'Assemblée plénière des sociétés d'assurances dommage (APSAD) et de la *National Fire Protection Association* (NFPA).

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

4. Agir sur les supports

4.1. Réduire les vulnérabilités des logiciels

Objectif : diminuer la possibilité que les caractéristiques des logiciels (systèmes d'exploitation, applications métiers, systèmes de gestion de bases de données, logiciels bureautiques, protocoles, paramétrages…) ne soient exploitées pour porter atteinte aux données à caractère personnel (DCP).

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

- Tenir les systèmes et applications à jour (versions, correctifs de sécurité…) 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…*
- 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…*
- 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…), 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…*
- 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…*
- Activer les mesures de protection offertes par le système et les applications.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- *Recommandations : activer les mots de passe d'ouverture de session, le pare-feu, 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…*

- Rechercher les vulnérabilités exploitables, notamment sur les serveurs les plus critiques.
  - *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[76], nikto[77]…), voire des systèmes de détection et prévention des attaques (Host Intrusion Prevention), s'assurer que les principales vulnérabilités sont couvertes[78]…*
- Protéger 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.
  - *Recommandations : chiffrer les codes sources pour réduire les risques de vol, appliquer une signature électronique pour protéger l'authenticité et l'intégrité, faire des sauvegardes, stocker les orignaux et les sauvegardes dans des lieux sécurisés…*
- 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[79] (utiliser des logiciels tels que Rootkit Revealer)…*

Outillage / Pour aller plus loin

- Selon la nature de l'application, il peut être nécessaire d'assurer l'intégrité des traitements 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.
- Voir les notes [CERTA-LogicielsObsolètes], [CERTA-iFrame], [CERTA-Injection], [CERTA-Correctifs], [CERTA-Messagerie] , [CERTA-CrossSiteScripting] et [CERTA-CrossSiteForgery].

4.1.1 Spécificités pour les postes de travail

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

- Interdire le partage de répertoires ou de données localement sur les postes de travail.

[76] Voir le site http://nmap.org.
[77] Voir le site http://www.cirt.net/nikto2.
[78] Voir le site http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.
[79] Ensemble de techniques et outils permettant d'obtenir l'accès et le contrôle d'un ordinateur de manière furtive.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- 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…*
- Interdire l'exécution des applications téléchargées ne provenant pas de sources sûres.

4.1.2 Spécificités pour les téléphones mobiles / *smartphones*

Objectif : 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…*) 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.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- *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[80] au niveau local et ne permettent qu'un accès en ligne à des données sensibles[81] 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…).

4.1.3 Spécificités pour les acquisitions de logiciels (achats, développements…)

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.

[80] Données sensibles au sens de l'article 8 et les données relevant de l'article 9.
[81] Données sensibles au sens de l'article 8 et les données relevant de l'article 9.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- 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 DCP 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*[82]*…*
- Vérifier que les logiciels fonctionnent correctement et conformément lors de la recette.

Outillage / Pour aller plus loin

- Voir le [RGI].

4.1.4 Spécificités pour les bases de données

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

- Ne pas utiliser les serveurs hébergeant les bases de données à d'autres fins (notamment pour naviguer sur des sites internet, accéder à la messagerie électronique…).
- Utiliser des comptes nominatifs pour l'accès aux bases de données, sauf si une contrainte technique l'empêche.
- Mettre en œuvre des mesures et/ou installer des dispositifs pour se prémunir des attaques par injection de code SQL ou de scripts.
    - *Recommandations : empêcher de saisir n'importe quelle donnée (ex. : s'assurer que seul le format prévu est peut être saisi), empêcher de saisir n'importe quel volume de données (ex. : limiter la taille des pièces jointes), empêcher de réaliser n'importe quelle action avec les données entrantes (ex. : identifier et rejeter les données susceptibles de déclencher une commande exécutable)…*
- Prévoir des mesures particulières pour les bases de données sensibles[83].
    - *Recommandations : chiffrement en base, chiffrement des sauvegardes…*

4.1.5 Spécificités pour les navigateurs Internet

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

- Sécuriser la configuration du navigateur Internet.
    - *Recommandations : la configuration doit inclure la protection des informations nominatives stockées par le navigateur (formulaires, mots de*

[82] Données sensibles au sens de l'article 8 et les données relevant de l'article 9.
[83] Données sensibles au sens de l'article 8 et les données relevant de l'article 9.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

passe, certificats…), l'utilisation d'un mot de passe principal sous Mozilla Firefox, l'impossibilité de stocker des mots de passe en cas de risques élevés…

- Déployer le navigateur dont la configuration a été sécurisée sur tous les serveurs et 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.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

4.2. Réduire les vulnérabilités des matériels

Objectif : diminuer la possibilité que les caractéristiques des matériels (serveurs, postes fixes, ordinateurs portables, périphériques, relais de communication, supports amovibles…) soient exploitées pour porter atteinte aux données à caractère personnel (DCP).

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…) 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 (exemple : serveur dédié dans une baie fermée à clé).*
- Empêcher l'accès à des DCP stockées sur des ressources informatiques mises au rebut.
  - *Recommandations : inspecter l'équipement pour s'assurer que toute DCP 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…), 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[84] 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, au qu'elle permet au moins de les arrêter normalement.
- Protéger l'accès aux matériels sensibles ou qui ont une grande valeur marchande.
- Limiter les possibilités de modification des matériels.

[84] RAID désigne des techniques de répartition de données sur plusieurs supports de stockage (par exemple des disques durs) permettant notamment de prévenir des pertes de données consécutives à la panne d'un des supports.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- *Recommandations : utiliser des scellés permettant de vérifier qu'un ordinateur a été ouvert…*

Outillage / Pour aller plus loin

- Afin de réduire les risques liés à l'interception de signaux parasites, qu'ils soient intentionnels (ex. : wifi) ou non (ex. : émission de perturbations électromagnétiques provoquées par les matériels), il peut être nécessaire de réaliser un zonage des locaux (voir la directive [ANSSI-ZonageLocaux]) et des équipements (voir le guide [ANSSI-ZonageEquip]), voire d'utiliser des matériels TEMPEST[85] ou une cage de Faraday dans le cas de traitements exposés à des risques très importants.

4.2.1 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 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.

4.2.2 Spécificités pour les postes nomades

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

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

- Chiffrer les DCP 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…*
- Limiter le stockage de DCP sur les postes nomades au strict nécessaire, et éventuellement l'interdire lors de déplacement à l'étranger.
- Assurer la disponibilité des DCP stockées sur les postes nomades.
  - *Recommandations : les copier dès que possible sur un autre poste, sur un serveur…*

[85] *Transient ElectroMagnetic Pulse Emanations Standard*.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- Purger les DCP 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 [CNIL-AU-027].
- 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.

4.2.3 Spécificités pour les supports amovibles

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

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…).
- Limiter l'utilisation des clés USB aux activités professionnelles.
- Désactiver la fonctionnalité d'exécution automatique sur tous les postes (stratégie de groupe).
- Chiffrer les DCP 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 DCP 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[86] pour les supports numériques tels que les CD et DVD…*

Outillage / Pour aller plus loin

- Voir la note [CERTA-ClésUSB].

[86] La norme allemande DIN 32757 définit 5 niveaux de sécurité pour les broyeurs selon la sensibilité des documents.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

4.2.4 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 DCP.
    - *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[87] et si elles ne peuvent pas être chiffrées ou effacées dans leur totalité (panne d'un disque dur, dysfonctionnement…) ; interdire l'envoi en maintenance externe dans le cas de données sensibles[88]…*
- 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…*
- Empêcher l'accès à des DCP 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…), 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.*

[87] Données sensibles au sens de l'article 8 et les données relevant de l'article 9.
[88] Données sensibles au sens de l'article 8 et les données relevant de l'article 9.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

4.3. Réduire les vulnérabilités des canaux informatiques

Objectif : diminuer la possibilité que les caractéristiques des canaux informatiques (réseau filaire, wifi, ondes radio, fibre optique…) soient exploitées pour porter atteinte aux données à caractère personnel (DCP).

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[89] 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[90].
    - *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…*
- Surveiller l'activité réseau après en avoir informé les personnes concernées.
    - *Recommandations : mettre en place des systèmes de détection d'intrusion[91] ou un système de prévention d'intrusion[92] 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.

[89] *DeMilitarized Zone*, zone démilitarisée.
[90] *Firewall.*
[91] *Intrusion Detection System (IDS).*
[92] *Intrusion Prevention System (IPS).*

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- *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…).*

- 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[93]) 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[94] 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…) 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 DCP (clé de déchiffrement, mot de passe…) 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 (soit des NIDS[95] qui surveillent l'état de la sécurité au niveau du réseau, soit des HIDS[96] qui surveillent l'état de la sécurité au niveau des ordinateurs reliés au réseau, soit des IDS hybrides),
  - de système de prévention d'intrusion (soit des NIPS[97] 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[98] qui

[93] *Media Access Control*.
[94] Un port physique est un emplacement permettant de brancher un câble, tandis qu'un port logique est un numéro utilisé dans un protocole de communication, notamment le protocole TCP dans le monde internet.
[95] *Network Based Intrusion Detection System*.
[96] *HostBased Intrusion Detection System*.
[97] *Network-based Intrusion Prevention*.
[98] *Network Behavior Analysis*.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

identifient les menaces générant des flux inhabituels, soit des HIPS[99] 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 [RGS].

4.3.1 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[100] 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.

4.3.2 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.
- Sécuriser le flux d'authentification sécurisé.
  - *Recommandations : aucun mot de passe en clair, séquence non rejouable…*
- Obliger à faire accepter la prise de main à distance par l'utilisateur de manière explicite par une action sur le poste de travail.
  - *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.
- Obliger à faire signaler par l'outil la fin de la prise de main à l'utilisateur ou verrouiller la session utilisateur si celui-ci n'est pas présent devant son poste à ce moment.

4.3.3 Spécificités pour les postes nomades ou se connectant à distance

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

[99] *Host-based Intrusion Prevention*.
[100] *Secure SHell*.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

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[101] (token) sans oublier de changer les mots de passe d'activation par défaut), ce que l'on a (ex. : certificat électronique, carte à puce…) 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[102] 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…*

4.3.4 Spécificités pour les interfaces sans fil (Wifi, Bluetooth, infrarouge, 3G…)

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, 3G…) 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…*

[101] *One-time password*.
[102] *Virtual Private Network*.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

4.3.5 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].
- Dans certains contextes, le filtrage par adresse MAC peut être mis en place pour protéger l'accès Wifi.

4.3.6 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].

4.3.7 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.

4.3.8 Spécificités pour les réseaux de téléphonie mobile (2G, 3G ou 3G+…)

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.

4.3.9 Spécificités pour la navigation sur Internet

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

- Utiliser le protocole SSL (HTTPS) pour assurer l'authentification des serveurs et la confidentialité des communications.
- Privilégier des clés générées conformément au [RGS].

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

- *Recommandations : avoir recours à un prestataire de service de certification électronique (PSCE) référencé[103] comme conforme au [RGS] dans sa version 1.0 pour un usage d'authentification de serveur.*

4.3.10 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[104].
- Chiffrer les fichiers avant tout transfert dans le cas de risques élevés.

4.3.11 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.

4.3.12 Spécificités pour l'ADSL

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 »).

4.3.13 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 DCP.
- 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…) 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…

[103] Voir http://www.lsti-certification.fr/index.php?option=com_content&view=article&id=54&Itemid=14&lang=fr.
[104] *Secure CoPy*.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

4.3.14 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 DCP 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].

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

4.4. Réduire les vulnérabilités des personnes

Objectif : 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 à caractère personnel (DCP).

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

- Vérifier que les personnes ayant accès aux DCP 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 DCP 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 DCP 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…), routinières (habitudes facilitant l'espionnage récurrent), influençables (naïves, crédules, obtuses, faible estime de soi, faible loyauté…) 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 DCP…*

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…) pour les personnes ayant accès aux DCP et au traitement.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

4.5. Réduire les vulnérabilités des documents papier

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

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…).
- Récupérer les documents imprimés contenant des DCP immédiatement après leur impression.
- Limiter la diffusion des documents papier contenant des DCP qu'aux personnes ayant le besoin d'en disposer dans le cadre de leur activité.
- Stocker les documents papier contenant des DCP dans un meuble sécurisé.
    - *Recommandations : utiliser une armoire ignifugée fermant à clé, un coffre…*
- Détruire les documents papier contenant des DCP 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 32757*[105].

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.

[105] La norme allemande DIN 32757 définit 5 niveaux de sécurité pour les broyeurs selon la sensibilité des documents.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

4.6. Réduire les vulnérabilités des canaux papier

Objectif : 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 (DCP).

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

- N'envoyer que les documents papier contenant des DCP nécessaires au traitement.
- Garder une trace précise de la transmission des documents papier contenant des DCP.
  - *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 DCP (liste des documents reçus, identité du destinataire et sa signature, date et heure de réception)…*
- 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…*
- Améliorer la confiance envers le transporteur de documents papier contenant des DCP.
  - *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…*
- Protéger les documents papier contenant des DCP.
  - *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…)…*

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.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

5. Actions transverses (au niveau de l'organisme)

Ce chapitre décrit des bonnes pratiques de gouvernance de la protection de la vie privée. Elles permettent d'établir des mesures générales pour diriger et contrôler la manière dont la protection de la vie privée est gérée. Elles contribuent à traiter les risques qui pèsent sur le traitement considéré de manière transverse. S'agissant de mesures organisationnelles, elles sont également utiles aux autres traitements de l'organisme.

5.1. Gérer l'organisation de protection de la vie privée

Objectif : disposer d'une organisation apte à diriger et contrôler la protection des données à caractère personnel (DCP) au sein de l'organisme.

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-I&L] et lui accorder les moyens nécessaires à l'exercice de sa mission.
    - *Recommandations : désigner un correspondant « Informatique et libertés » (CIL), 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 (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…), 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 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-I&L] 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 offre un vecteur de sécurité juridique (il permet de garantir la conformité de l'organisme à la [Loi-I&L]), un facteur de simplification des formalités administratives (exonération de l'obligation de déclaration préalable des traitements

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

ordinaires et courants), un accès personnalisé aux services de la CNIL (extranet, formations, suivi personnalisé…), 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-I&L]).

5.2. Gérer les risques sur la vie privée

Objectif : maîtriser les risques que les traitements de l'organisme font peser sur les libertés et la vie privée des personnes concernées.

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

- Réaliser une cartographie des risques sur l'ensemble des traitements 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

- Voir la méthode de gestion des risques sur les libertés et la vie privée de la CNIL.
- Voir les principes « Adopter une démarche globale », « Gérer les risques SSI », « Viser une amélioration continue », « Un engagement systématique : l'homologation de sécurité » et « Des outils spécifiques pour différentes familles de téléservices » du [RGS].
- Voir la méthode [ANSSI-EBIOS].

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

5.3. Gérer la politique de protection de la vie privée

Objectif : disposer d'une base documentaire formalisant les objectifs et les règles à appliquer dans le domaine « Informatique et libertés ».

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…) et aux différentes cibles de communication (usagers, service en charge de l'informatique, décideurs…).
    - *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…*
- 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 [RGS].
- Voir le guide [ANSSI-PSSI].

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

5.4. Intégrer la protection de la vie privée dans les projets

Objectif : prendre en compte la protection des données à caractère personnel (DCP) dans tout nouveau traitement.

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…).
    - *Recommandations : une certification de sécurité de premier niveau (CSPN), 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[106], CISM – Certified Information Security Manager[107], ISO 27001 Lead Auditor[108]…)…*
- 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…)…*
- 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 [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[109].
- Voir les guides [ANSSI-MaturitéSSI] et [ANSSI-GISSIP].

[106] Voir https://www.isc2.org/cgi-bin/content.cgi?category=97.
[107] Voir http://www.afai.fr/index.php?m=100.
[108] Voir http://www.lsti-certification.fr/index.php?option=com_content&view=article&id=50&Itemid=27.
[109] Les catalogues sont disponibles sur le site Internet de l'ANSSI :
- Certificats : http://www.ssi.gouv.fr/fr/confiance/certificats.html
- CSPN : http://www.ssi.gouv.fr/fr/confiance/certif-cspn.html
- Qualifications : http://www.ssi.gouv.fr/fr/politique_produit/catalogue/index.html

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

5.4.1 Spécificités pour les téléservices des autorités administratives

Objectif : assurer la conformité à l'[Ordonnance-Téléservices].

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

- Identifier les biens à protéger et menaces à considérer à l'aide d'une analyse de risques.
- Déterminer les objectifs de sécurité selon les critères de disponibilité, confidentialité, intégrité, traçabilité pour se protéger de manière proportionnée face aux risques.
- En déduire les fonctions de sécurité nécessaire et leur niveau, et respecter les règles fixées pour le niveau déterminé au préalable lorsque ces fonctions de sécurité sont décrites dans le [RGS] (signature électronique, authentification, chiffrement, horodatage, ainsi que d'une manière générale tout mécanisme cryptographique et processus de gestion des clés).
- Recourir à des produits de sécurité et offres de services de prestataires qualifiés.
- Faire attester formellement, par une autorité appelée dans ce cadre « autorité d'homologation », de la prise en compte de la sécurité par le biais d'une homologation de sécurité (acte par lequel l'autorité administrative engage sa responsabilité) et rendre cette décision accessible par Internet.
- Adopter des pratiques et des outils reconnus comme interopérables, conformément au [RGI] (règles sur les protocoles d'échanges à employer, sur les services web et sur l'infrastructure).

Notes

- La conformité à l'[Ordonnance-Téléservices] implique la conformité aux exigences du décret n°2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'[Ordonnance-Téléservices], ainsi qu'à celles du décret n°2007-284 du 2 mars 2007 fixant les modalités d'élaboration, d'approbation, de modification et de publication du [RGI].
- Si le téléservice nécessite l'emploi d'un identifiant propre à chaque utilisateur, qu'il s'agisse ou non du numéro d'inscription au répertoire (NIR), sa mise en œuvre par une administration relève du régime de l'avis préalable de la CNIL sur un projet d'acte réglementaire conformément à l'article 27 de la [Loi-I&L].

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

5.5. Superviser la protection de la vie privée

Objectif : disposer d'une vision globale et à jour de l'état de protection des données à caractère personnel (DCP) et de la conformité à la [Loi-I&L].

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

- Effectuer régulièrement des contrôles des traitements de DCP afin de vérifier leur conformité à la [Loi-I&L] 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 DCP 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 DCP 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…*
- 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…*

Notes

- La CNIL prévoit de labelliser 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.

Outillage / Pour aller plus loin

- Voir le guide [ANSSI-TDBSSI].

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Annexes

Tableau de synthèse des mesures

Mesures	Principaux chapitres correspondants dans l'[ISO-27002]
1. Minimiser les DCP	15. Conformité
2. Gérer les durées de conservation des DCP	15. Conformité
3. Informer les personnes concernées	15. Conformité
4. Obtenir le consentement des personnes concernées	15. Conformité
5. Permettre l'exercice du droit d'opposition	15. Conformité
6. Permettre l'exercice du droit d'accès direct	15. Conformité
7. Permettre l'exercice du droit de rectification	15. Conformité
8. Cloisonner les DCP	10. Gestion de l'exploitation et des télécommunications
9. Chiffrer les DCP	10. Gestion de l'exploitation et des télécommunications
10. Anonymiser les DCP	15. Conformité
11. Sauvegarder les DCP	10. Gestion de l'exploitation et des télécommunications
12. Protéger les archives de DCP	10. Gestion de l'exploitation et des télécommunications
13. Contrôler l'intégrité des DCP	10. Gestion de l'exploitation et des télécommunications
14. Tracer l'activité sur le système informatique	10. Gestion de l'exploitation et des télécommunications
15. Gérer les violations de DCP	13. Gestion des incidents liés à la sécurité de l'information 14. Gestion du plan de continuité de l'activité
16. S'éloigner des sources de risques	9. Sécurité physique et environnementale
17. Marquer les documents contenant des DCP	7. Gestion des biens
18. Gérer les personnes internes qui ont un accès légitime	6. Organisation de la sécurité de l'information 8. Sécurité liée aux ressources humaines
19. Contrôler l'accès logique des personnes	11. Contrôle d'accès
20. Gérer les tiers qui ont un accès légitime aux DCP	6. Organisation de la sécurité de l'information
21. Lutter contre les codes malveillants	10. Gestion de l'exploitation et des télécommunications
22. Contrôler l'accès physique des personnes	9. Sécurité physique et environnementale
23. Se protéger contre les sources de risques non humaines	9. Sécurité physique et environnementale
24. Réduire les vulnérabilités des logiciels	10. Gestion de l'exploitation et des télécommunications 11. Contrôle d'accès 12. Acquisition, développement et maintenance des systèmes d'information
25. Réduire les vulnérabilités des matériels	7. Gestion des biens 9. Sécurité physique et environnementale 10. Gestion de l'exploitation et des télécommunications 11. Contrôle d'accès
26. Réduire les vulnérabilités des canaux informatiques	10. Gestion de l'exploitation et des télécommunications 11. Contrôle d'accès
27. Réduire les vulnérabilités des personnes	8. Sécurité liée aux ressources humaines
28. Réduire les vulnérabilités des documents papier	7. Gestion des biens
29. Réduire les vulnérabilités des canaux papier	7. Gestion des biens
30. Gérer l'organisation de protection de la vie privée	6. Organisation de la sécurité de l'information
31. Gérer les risques sur la vie privée	6. Organisation de la sécurité de l'information
32. Gérer la politique de protection de la vie privée	5. Politique de sécurité
33. Intégrer la protection de la vie privée dans les projets	12. Acquisition, développement et maintenance des systèmes d'information
34. Superviser la protection de la vie privée	15. Conformité

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Acronymes

AFNOR	Association Française de Normalisation
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
APSAD	Assemblée Plénière des Sociétés d'Assurances Dommage
CERTA	Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques
CIL	Correspondant Informatique et Liberté
CLUSIF	CLUb de la Sécurité de l'Information Français
CNPP	Centre National de Prévention et de Protection
CNIL	Commission Nationale de l'Informatique et des Libertés
DCP	Données à Caractère Personnel
DIN	*Deutsches Institut für Normung* (Institut de normalisation allemand)
ENISA	*European Network and Information Security Agency*
G29	Groupe de travail article 29 sur la protection des données
ISO	*International Organization for Standardization* (Organisation internationale de normalisation)
NFPA	*National Fire Protection Association*
RGI	Référentiel Général d'Interopérabilité
RGS	Référentiel Général de Sécurité
SSI	Sécurité des Systèmes d'Information

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

Références bibliographiques

[AFCDP-Anonymisation] *Référentiel AFCDP des dispositifs d'anonymisation*, Association française des correspondants à la protection des données à caractère personnel (AFCDP), 2008.
http://www.afcdp.net/L-AFCDP-publie-un-Referentiel-des

[AFNOR-97-560] FD S 97-560:2000, Informatique de santé – Anonymisation – Glossaire et démarche d'analyse et expression de besoins.
http://www.abs92.com/documents/boite_a_outils/notions_fondamentales/notions_de_stat/2_anomysation.pdf

[ANSSI-Archivage] *Archivage électronique sécurisé – Mémento*, 16 mai 2006, ANSSI.
http://www.ssi.gouv.fr/site_article48.html

[ANSSI-EBIOS] *Expression des Besoins et Identification des Objectifs de Sécurité – EBIOS – Méthode de gestion des risques*, 25 janvier 2010, ANSSI.
http://www.ssi.gouv.fr/site_article173.html

[ANSSI-Effacement] *Guide technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter (Problématique de « l'effacement » des signaux magnétiques)*, n°972-1/SGDN/DCSSI, 17 juillet 2003, ANSSI.
http://www.ssi.gouv.fr/archive/fr/documentation/Guide_effaceur_V1.12du040517.pdf

[ANSSI-Externalisation] *Maîtriser les risques de l'infogérance – Externalisation des systèmes d'information*, décembre 2010, ANSSI.
http://www.ssi.gouv.fr/site_article270.html

[ANSSI-GISSIP] *Guide d'intégration de la sécurité des systèmes d'information dans les projets – GISSIP*, 11 décembre 2006, ANSSI.
http://www.ssi.gouv.fr/site_article86.html

[ANSSI-MaturitéSSI] *Maturité SSI – Approche méthodologique*, 2 novembre 2007, ANSSI.
http://www.ssi.gouv.fr/site_article85.html

[ANSSI-PSSI] *Guide pour l'élaboration d'une politique de sécurité de système d'information – PSSI – Méthodologie*, 3 mars 2004, ANSSI.
http://www.ssi.gouv.fr/site_article46.html

[ANSSI-TDBSSI] *Élaboration de tableaux de bord SSI – TDBSSI – Méthodologie*, 5 février 2004, ANSSI.
http://www.ssi.gouv.fr/site_article47.html

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

[ANSSI-Voyageurs] *Passeport de conseils aux voyageurs*, ANSSI, janvier 2010. http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf

[ANSSI-ZonageEquip] *Guide n°430 relatif à l'évaluation des équipements commerciaux au sens du zonage TEMPEST*, Direction centrale de la sécurité des systèmes d'information (DCSSI), 1999.

[ANSSI-ZonageLocaux] *Directive n°495 du 19 septembre 1997 relative au concept de zonage TEMPEST, Protection contre les signaux compromettants.*

[CERTA-Backscatting] *E-mail backscatting, pollution par des rapports de non-livraison de courriels*, Note d'information n°CERTA-2008-INF-004, 19 décembre 2008, ANSSI. http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-004.pdf

[CERTA-Bluetooth] *Sécurité des réseaux sans fil Bluetooth*, Note d'information n°CERTA-2007-INF-003, 1er août 2007, ANSSI. http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-003.pdf

[CERTA-Canulars] *Les canulars par messagerie*, Note d'information n°CERTA-2000-INF-005, 14 juin 2000, ANSSI. http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-005.pdf

[CERTA-ClésUSB] *Risques associés aux clés USB*, Note d'information n°CERTA-2006-INF-006-004, 11 février 2009, ANSSI. http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006.pdf

[CERTA-Correctifs] *Acquisition des correctifs*, Note d'information n°CERTA-2001-INF-004, 4 octobre 2001, ANSSI. http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004.pdf

[CERTA-CrossSiteForgery] *Les attaques de type « cross-site request forgery »*, Note d'information n°CERTA-2008-INF-003, 17 décembre 2008, ANSSI. http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-003.pdf

[CERTA-CrossSiteScripting] *Vulnérabilité de type « Cross Site Scripting »*, Note d'information n°CERTA-2002-INF-001-001, 14 septembre 2010, ANSSI. http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001.pdf

[CERTA-DNS] *Du bon usage du DNS*, Note d'information n°CERTA-2008-INF-002, 25 juillet 2008, ANSSI. http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-002.pdf

[CERTA-Filtrage] *Filtrage et pare-feux*, Note d'information n°CERTA-2005-INF-006,

10 janvier 2006, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-001.pdf

[CERTA-iFrame] *iFRAME, fonctionnement et protection*, Note d'information n°CERTA-2008-INF-001, 17 juillet 2008, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-001.pdf

[CERTA-Indexation] *Outils d'indexation et de recherche*, Note d'information n°CERTA-2006-INF-009, 21 novembre 2006, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009.pdf

[CERTA-Injection] *Sécurité des applications Web et vulnérabilité de type « injection de données »*, Note d'information n°CERTA-2004-INF-001-001, 3 janvier 2005, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001.pdf

[CERTA-Intrusion] *Les bons réflexes en cas d'intrusion sur un système d'information*, Note d'information n°CERTA-2002-INF-002-003, 7 janvier 2008, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002.pdf

[CERTA-IPv6] *Migration IPv6 : enjeux de sécurité*, Note d'information n°CERTA-2006-INF-004-004, 9 janvier 2008, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004.pdf

[CERTA-IRC] *Usage de la messagerie instantanée ou de l'IRC*, Recommandation n°CERTA-2002-REC-001, 28 mars 2002, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-001.pdf

[CERTA-Journaux] *Gestion des journaux d'événements*, Note d'information n°CERTA-2008-INF-005, 31 décembre 2008, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-005.pdf

[CERTA-LogicielsObsolètes] *Les systèmes et logiciels obsolètes*, Note d'information n°CERTA-2005-INF-003-010, 16 juillet 2010, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003.pdf

[CERTA-Messagerie] *Mesures de prévention relatives à la messagerie*, Note d'information n°CERTA-2000-INF-002-001, 27 mars 2009, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002.pdf

[CERTA-MotsDePasse] *Les mots de passe*, Note d'information n°CERTA-2005-INF-001, 12 avril 2007, ANSSI.
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001.pdf

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

[CERTA-Mutualisé] *Bonnes pratiques concernant l'hébergement mutualisé*, Note d'information n°CERTA-2005-INF-005, 19 décembre 2005, ANSSI. http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005.pdf

[CERTA-PHP] *Du bon usage de PHP*, Note d'information n°CERTA-2007-INF-002, 20 mars 2007, ANSSI. http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002.pdf

[CERTA-Spam] *Limiter l'impact du SPAM*, Note d'information n°CERTA-2005-INF-004, 3 octobre 2005, ANSSI. http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004.pdf

[CERTA-SSL] *La bonne utilisation des protocoles SSL/TLS*, Note d'information n°CERTA-2005-REC-001, 1er mars 2005, ANSSI. http://www.certa.ssi.gouv.fr/site/CERTA-2005-REC-001.pdf

[CERTA-Tunnels] *Tunnels et pare-feux : une cohabitation difficile*, Note d'information n°CERTA-2001-INF-003-001, 5 octobre 2005, ANSSI. http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-003.pdf

[CERTA-Virus] *Rappel sur les virus et chevaux de Troie*, Note d'information n°CERTA-2000-INF-007, 8 novembre 2000, ANSSI. http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-007.pdf

[CERTA-Wifi] *Sécurité des réseaux sans fil (Wi-Fi)*, Note d'information n°CERTA-2002-REC-002, 21 novembre 2008, ANSSI. http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002.pdf

[CLUSIF-Victime] *Vous êtes victime d'une malveillance informatique : à quel service d'État vous adresser en France ?*, Club de la sécurité de l'information français (CLUSIF). http://www.clusif.asso.fr/fr/production/cybervictime/

[CLUSIF-Voix] *Moyens de Communication Voix : Présentation et Enjeux de Sécurité*, mars 2010, Club de la sécurité de l'information français (CLUSIF). http://www.clusif.fr/fr/production/ouvrages/pdf/CLUSIF-2010-Communication-Voix-Enjeux-de-Securite.pdf

[CNIL-AU-027] Autorisation unique n° AU-027 - Délibération n° 2011-074 du 10 mars 2011 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux postes informatiques portables professionnels.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/254/

[CNIL-DiffJurisprudence] Délibération de la CNIL n°01-057 du 29 novembre 2001 portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence. http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/17/

[CNIL-Employeurs] *Guide pour les employeurs et les salariés*, CNIL, 2010. http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_employeurs_salaries.pdf

[CNIL-Empreinte] Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, CNIL, 2007. http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf

[CNIL-ExternaliserHorsUE] Les questions posées pour la protection des données personnelles par l'externalisation hors de l'Union européenne des traitements informatiques, CNIL, 2010. http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/20100909-externalisation.pdf

[CNIL-Smartphones] Les smartphones en questions, CNIL, 2010. http://www.cnil.fr/la-cnil/actu-cnil/article/article/les-smartphones-en-questions/

[CNIL-TransfertHorsUE] Les clauses contractuelles types – Des modèles de contrats adoptés par la Commission européenne, CNIL. http://www.cnil.fr/vos-responsabilites/transferer-des-donnees-a-letranger/contrats-types-de-la-commission-europeenne/

[Décret-2002-637] Décret n°2002-637 du 29 avril 2002 relatif à l'accès aux informations personnelles détenues par les professionnels et les établissements de santé en application des articles L. 1111-7 et L. 1112-1 du code de la santé publique. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000773559&dateTexte

[Décret-I&L] Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n°78-17 relative à l'informatique, aux fichiers et aux libertés modifié par le décret 2007-451 du 25 mars 2007. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEX

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

T000000824352&dateTexte

[Décret-LCEN] Décret n°2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023646013&categorieLien=id

[Directive-2002-58] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:FR:PDF

[Directive-2009-136] Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n°2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs. *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:FR:PDF*

[ENISA-Smartphone] *Smartphones: Information security risks, opportunities and recommendations for users*, décembre 2010, ENISA. http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport

[G29-Publicité] *Avis 2/2010 sur la publicité comportementale en ligne*, Groupe de travail « Article 29 » sur la protection des données, 22 juin 2010. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_fr.pdf

[ISO-25237] ISO TR 25237:2008, *Informatique de santé – Pseudonymisation*.

[ISO-27001] ISO/IEC 27001:2005, *Technologies de l'information – Techniques*

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

de sécurité – Systèmes de management de la sécurité de l'information – Exigences.

[ISO-27002] ISO/IEC 27002:2005, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information*.

[ISO-27005] ISO/IEC 27005:2008, *Technologies de l'information – Techniques de sécurité – Gestion des risques en sécurité de l'information*.

[ISO-29100] Projet de norme ISO/IEC 29100, *Information technology – Security techniques – Privacy framework*.

[ISO-31000] ISO 31000:2009, *Management du risque – Principes et lignes directrices*.

[ISO-Guide73] ISO Guide 73:2009, *Management du risque – Vocabulaire*.

[LCEN] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
http://www.legifrance.gouv.fr/html/actualite/actualite_legislative/decrets_application/2004-575.htm

[Loi-I&L] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[110].
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20110224

[NF-42-013] NF Z 42-013 :2009, *Archivage électronique – Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes.*

[Ordonnance-Téléservices] Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232

[RGI] *Référentiel Général d'Interopérabilité* (version 1.0), 12 mai 2009, Direction générale de la modernisation de l'État du ministère du Budget, des comptes publics et de la réforme de l'État.

[110] 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.

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00

http://references.modernisation.gouv.fr/sites/default/files/RGI_Version1%200.pdf

[RGS] *Référentiel Général de Sécurité* (version 1.0), 6 mai 2010, ANSSI & Direction générale de la modernisation de l'État du ministère du Budget, des comptes publics et de la réforme de l'État. http://www.ssi.gouv.fr/site_article38.html

Attention : ces bonnes pratiques sont illustratives et doivent être adaptées aux risques à traiter.

RÉPUBLIQUE FRANÇAISE
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02 – Tél. : 01 53 73 22 22 – Fax : 01 53 73 22 00