ARTCI
AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

CONSEIL DE REGULATION

DECISION N°2014-0020

DU CONSEIL DE REGULATION

DE L'AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE

EN DATE DU 03 SEPTEMBRE 2014

PORTANT ADOPTION DES REGLES DE CONDUITE RELATIVES AU TRAITEMENT ET A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL (DCP)

LE CONSEIL DE REGULATION,

Vu l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

Vu la loi n° 2013-450 du 19 juin 2013 relative à la Protection des Données à Caractère Personnel ;

Vu le décret n° 2012-934 du 19 septembre 2012 portant organisation et fonctionnement de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) ;

Vu le décret n°2013-333 du 22 mai 2013 portant nomination des membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) ;

Vu le décret n°2013-332 du 22 mai 2013 portant nomination du Directeur Général de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) ;

Considérant qu'en application des dispositions de l'article 47 de la loi n°2013 – 450 du 19 juin 2013 relative à la protection des données à caractère personnel, l'Autorité de Régulation des Télécommunications est chargée d'élaborer les règles générales de conduite relative au traitement et à la protection des données à caractère personnel.

Après en avoir délibéré,

DECIDE :

Article 1

Le Conseil de Régulation adopte les règles de conduite annexées à la présente décision.

Ces règles de conduite sont un guide destiné aux acteurs de la protection des données à caractère personnel, aux personnes dont les informations font l'objet de traitements, aux responsables de traitements, et aux parties prenantes dans la création ou l'amélioration de traitement des données à caractère personnel, notamment :

- 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 à la protection des données à caractère personnel (DCP), qui doivent accompagner les MOA dans le domaine de la protection des DCP et jouer un rôle d'interface avec l'Autorité de protection (ARTCI) ;

- 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 la loi sur la protection des données à caractère personnel.

Article 2

L'Autorité de protection met à jour, régulièrement, le contenu des règles de conduites relatives au traitement et à la protection des données à caractère personnel.

Article 3

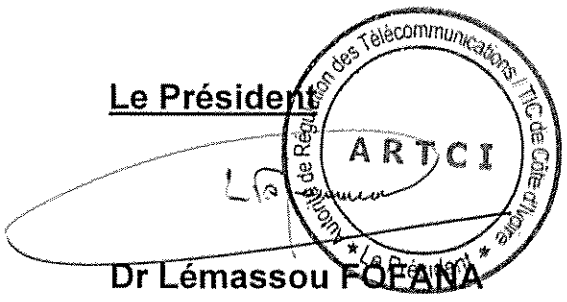
La présente décision prend effet à compter de la date de sa publication

Article 4

Le Directeur Général est chargé de la publication des règles de conduite en matière de protection des données à caractère personnel et de l'exécution de la présente décision, qui sera publiée au journal officiel de la République de Côte d'Ivoire et sur le site internet de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire.

Fait à Abidjan le 03 Septembre 2014

Le Président



Dr Lémassou FOFANA

OFFICIER DE L'ORDRE NATIONAL

ARTCI
AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

CONSEIL DE REGULATION

REGLES DE CONDUITE RELATIVES AU TRAITEMENT ET A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Conseil de Régulation : 31 Av Nogués, Imble Braodway 2ème étage 17 BP 110 Abj 17 Tél: +225 20 34 43 04 - Fax: +225 20 34 43 02
Siège Direction Générale : Marcory Anoumabo, 18 BP 2203 Abj 18 Tél: +20 34 43 73 / 74 - Fax: +225 20 34 43 75
www.artci.ci

SOMMAIRE

AVANT PROPOS

L'émergence et le développement d'une économie numérique en Côte d'Ivoire a conduit le Gouvernement Ivoirien à mettre en œuvre un cadre juridique intégrant les préoccupations liées à la cybercriminalité, aux transactions électroniques et à la protection des données à caractère personnel (DCP).

En 2012, l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication a été adoptée, suivie en 2013, des lois sur les transactions électroniques, la protection des données à caractère personnel et la lutte contre la cybercriminalité.

La Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel en son article 46 désigne l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) en tant que Autorité de protection des données à caractère personnel. A ce titre, elle est chargée de nombreuses missions dont **l'élaboration de règles de conduite relatives au traitement et à la protection des données à caractère personnel**.

Le présent guide est destiné aux acteurs de la protection des données à caractère personnel, aux personnes dont les informations font l'objet de traitements, aux responsables de traitements (personnes assurant le traitement des données), et aux parties prenantes dans la création ou l'amélioration de traitement des données à caractère personnel, notamment:

- 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 à la protection des DCP, qui doivent accompagner les MOA dans le domaine de la protection des DCP et jouer un rôle d'interface avec l'Autorité de protection ;

- 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 la loi sur les données à caractère personnel.

Le présent guide ne se limite pas aux considérations techniques des systèmes informatiques. Il s'applique également aux systèmes d'information dans leur globalité : systèmes informatiques, personnes, documents papiers, organisation, locaux, etc.

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.

CHAPITRE 1 : LES ELEMENTS A PROTEGER

1.1. Minimiser les données à caractère personnel

- Vérifier que les données à caractère personnel sont adéquates, pertinentes et non excessives au regard de la finalité poursuivie, et ne pas les collecter dans le cas contraire ;

- Vérifier que les données à caractère personnel 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, sauf dans les cas d'exceptions prévus à l'article 21 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

- Empêcher de collecter davantage de données à caractère personnel. Seuls les champs relatifs aux données à caractère personnel 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 données à caractère personnel aux personnes ayant le besoin d'en disposer dans le cadre de leur activité ;

- Effacer de manière sécurisée les données à caractère personnel qui ne sont plus utiles ou qu'une personne demande de supprimer, sur le système en opération et sur les sauvegardes le cas échéant. Veuillez à

utiliser des outils spécialisés et respectant les normes internationales en la matière.

1.2. Gérer les durées de conservation des données à caractère personnel

- Respecter les temps de conservation des données à caractère personnel qui ont été définis par l'Autorité de protection. Vérifier que le traitement permet de détecter la fin de la durée de conservation (le traitement intègre la date à laquelle chaque donnée à caractère personnel enregistrée doit être supprimée) ;

- Vérifier que le traitement permet de supprimer les données à caractère personnel 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. Evaluer les risques avant tout effacement des données à caractère personnel ; ainsi, face à des risques faibles, une simple suppression peut suffire, et face à des risques élevés l'utilisation des outils d'effacement sécurisés est convenable ;

- Une fois que la durée de conservation des données à caractère personnel est atteinte, les supprimer sans délai. Développer une fonctionnalité automatisée qui efface les données à caractère personnel dont la durée de conservation est atteinte.

1.3. Informer les personnes concernées

- Vérifier que le traitement ne fait pas l'objet d'une exception ou de conditions particulières mentionnées dans la loi relative à la protection des données à caractère personnel ;

- 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 données à caractère personnel et des moyens pratiques choisis. (formuler l'information dans un langage compréhensible du point de vue d'une personne non formée aux TIC ou d'Internet) ;

- S'assurer que les personnes concernées auront été informées au plus tard au moment où seront collectées leurs données ;

- S'assurer que la collecte ne puisse pas être effectuée sans en informer les personnes concernées. (déterminer des solutions alternatives au cas où les moyens pratiques choisis ne seraient plus opérationnels) ;

- Si possible, prévoir un moyen apportant la preuve que la personne concernée a été informée avant la collecte des données. (par exemple, placer l'information sur un panneau que tous les employés ont forcément vu, faire signer un émargement ou un document, faire une notification – fenêtre pop-up – sur le site internet...).

1.3.1. Spécificités pour les salariés d'un organisme

- 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.

1.3.2. Spécificités pour une collecte de données à caractère personnel via un site Internet

- Faire figurer une information à destination des internautes directement ou facilement accessible. 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 données à caractère personnel par téléphone

- Délivrer un message automatique avant que la conservation soit engagée, précisant notamment les droits des personnes, et le cas échéant, les finalités de l'enregistrement de la conservation (formation, enquête sur la qualité du service rendu etc.), en leur offrant la possibilité de s'opposer à l'enregistrement (pour motif légitime) ;

- Mettre en place des moyens permettant l'authentification de l'appelant (par une information connue seulement de l'organisme et de la personne concernée).

1.3.4. Spécificités pour une collecte de données à caractère personnel via un formulaire

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

- 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 auxquels 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 ;

- 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.

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

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

1.4. Obtenir le consentement des personnes concernées

- Vérifier si le traitement ne repose pas sur une autre base légale que le consentement (intérêt légitime, sauvegarde de la vie, obligation légale) ;

- 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. (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 ;

- 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.

1.4.1. Spécificités pour les données relevant des articles 21 de la loi relative à la protection des données à caractère personnel.

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

1.4.2. Spécificités pour la collecte de données à caractère personnel via un site Internet

Prévoir un formulaire avec des cases à cocher et qui ne sont pas cochées par défaut.

1.4.3. Spécificités pour la collecte de données à caractère personnel via des cookies

- 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.

1.4.4. Spécificités pour la géolocalisation via un smartphone

- Permettre à l'usager de refuser qu'une application puisse le géolocaliser de manière systématique ;

- Permettre à l'usager de sélectionner quelle application peut utiliser la géolocalisation ;

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

1.4.5. Spécificités pour l'utilisation de techniques de publicité ciblée

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.

1.4.6. Spécificités pour des recherches sur des prélèvements biologiques identifiants

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.

1.5. Permettre l'exercice du droit d'opposition

- Vérifier que le traitement ne fait pas l'objet d'une exception mentionnée à l'article 14 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel (obligation légale, mission d'intérêt public, sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée ...) 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 être exercé le plus rapidement possible, sans jamais excéder un (01) mois, dans une forme similaire à celle du traitement (voie postale, voie électronique). Les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais ;

- S'assurer que le droit d'opposition pourra toujours s'exercer et que les données à caractère personnel collectées et traitées permettent effectivement l'exercice du droit d'opposition ;

- 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'une pièce d'identité (carte nationale d'identité, permis de conduire, passeport biométrique) 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 (pièce d'identité scannée) ;

- S'assurer que le motif légitime des personnes exerçant leur droit d'opposition est fourni et apprécié (sauf dans les cas de prospection et des traitements portant sur des données génétiques, médicales et sur la recherche scientifique, 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.

1.5.1. Spécificités pour un traitement par formulaire

- Créer un formulaire, facilement accessible, avec des cases à décocher ou prévoir la possibilité de se désinscrire d'un service (suppression de compte).

1.5.2. Spécificités pour un traitement par courrier électronique

- 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.

1.6. Permettre l'exercice du droit d'accès

- Vérifier que le traitement ne fait pas l'objet d'une exception mentionnée dans l'article 14 de la loi relative à la protection des données à caractère personnel (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'Etat, 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 un (01) mois pour des données, dans une autre forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches ne doivent pas leur occasionner de frais excédant le coût de la reproduction ;

- S'assurer que le droit d'accès pourra toujours s'exercer ;

- 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'une pièce d'identité (qui ne devrait pas être conservé sauf en cas de besoin de conservation d'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 sont accompagnées d'un titre d'identité numérisé (carte nationale d'identité, permis de conduire, passeport biométrique)qui ne devrait pas être conservée sauf en cas de besoin de conservation d'une preuve ;

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

1.6.1. Spécificités pour l'accès aux dossiers médicaux

- Communiquer les informations au plus tard dans les huit (8) jours suivant la demande et dans les deux (2) mois si les informations remontent à plus de trois (3) ans (à compter de la date à laquelle l'information médicale a été constituée) ;

- Permettre l'exercice du droit d'accès par les représentants légaux, pour les mineurs ou le curateur pour les majeurs incapables.

1.7. Permettre l'exercice du droit de rectification

- Vérifier que le traitement ne fait pas l'objet d'une exception mentionnée à l'article 14 de la loi relative à la protection des données à caractère personnel (Sûreté de l'Etat, défense ou sécurité publique) ;

- Des moyens pratiques doivent 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 un (01) mois, dans une forme similaire à celle du traitement (voie postale/ou voie électronique). Les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais ;

- le droit de rectification doit pouvoir toujours s'exercé ;

- l'identité des demandeurs doit être vérifiée ;

- la véracité des rectifications demandées doit être vérifiée ;

- une confirmation doit être fournie aux demandeurs ;

- les tiers à qui des données auraient été transmises doivent être informés des rectifications faites.

17.1. Spécificités pour la publicité en ligne

Prévoir un accès par la personne aux centres d'intérêts 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.

1.8. Cloisonner les données à caractère personnel

- prévoir un accès des personnes aux seules données dont elles ont besoin ;
- Séparer logiquement les données utiles à chaque processus ;
- Vérifier de manière régulière que les données à caractère personnel sont bien cloisonnées, et que des destinataires ou des interconnexions n'ont pas été ajoutés.

1.9. Chiffrer les données à caractère personnel

- Déterminer ce qui doit être chiffré ;
- Choisir le type de chiffrement (symétrique ou asymétrique) selon le contexte et les risques identifiés ;
- Recourir à des solutions de chiffrement basées sur des algorithmes publics réputés forts ;
- Mettre en place des mesures pour garantir la disponibilité, l'intégrité et la confidentialité des éléments permettant de récupérer des secrets perdus.

1.9.1. Spécificités pour un chiffrement symétrique (ou conventionnel)

- N'employer une clé que pour un seul usage ;
- Choisir un mécanisme reconnu par les organisations compétentes et qui dispose d'une preuve de sécurité ;
- Formaliser la manière dont les clés vont être gérées.

1.9.2. Spécificités pour un chiffrement asymétrique (ou à clé publique)

- N'employer une bi-clé pour un seul usage (l'emploi d'une même clé à plus d'un usage, par exemple pour assurer l'authenticité avec un mécanisme de signature) ;

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

- Générer les clés conformément aux meilleures pratiques ISO 27001 ;

- Mettre en place des mécanismes de vérification des certificats électroniques ;

- 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.

1.9.3. Spécificités pour le chiffrement de matériels

- Chiffrer les données au niveau matériel (surface du disque dur) ou au niveau du système d'exploitation (chiffrement d'une partition) ;

- Privilégier les dispositifs ne stockant pas les clés sur le matériel à chiffrer.

1.9.4. Spécificités pour le chiffrement de bases de données

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 bases de données.

1.9.5. Spécificités pour le chiffrement de partitions ou de conteneurs

- Chiffrer les données au niveau du système d'exploitation (chiffrement d'une partition ou d'un conteneur).

1.9.6. Spécificités pour le chiffrement de fichiers isolés

Chiffrer les fichiers stockés ou les pièces à joindre à des courriers électroniques.

1.9.7. Spécificités pour le chiffrement de courriers électroniques

Chiffrer les messages électroniques.

1.9.8. Spécificités pour le chiffrement d'un canal de communication

Chiffrer le canal de communication entre un serveur authentifié et un client distant.

1.10. Rendre anonyme les données à caractère personnel

- Déterminer ce qui doit être rendu anonyme selon le contexte, la forme de stockage des données à caractère personnel (champs d'une base de données) et les risques identifiés ;

- Rendre anonyme de sorte à ce que qui que ce soit ne puisse retrouver les données originales, ce qui doit l'être, selon la forme des données à rendre anonyme (base de données) et les risques identifiés ;

- Choisir les outils (suppression partielle, chiffrement, hachage, hachage à clé) qui satisfont le mieux possible les besoins fonctionnels, lorsque ce qui doit être rendu anonyme ne peut l'être de manière irréversible.

1.10.1. Spécificités pour les bases de données

- Rendre anonyme de manière irréversible les données à caractère personnel qui peuvent l'être ;

- Si ce n'est pas possible, déterminer les solutions qui satisfont le mieux possible les besoins fonctionnels ;

- Utiliser uniquement des données à caractère personnel rendues anonymes ou des données fictives pour les phases de développement et de test.

1.10.2. Spécificités pour les documents électroniques textuels

- Vérifier manuellement les textes rendus anonymes à l'aide du dispositif choisi afin de corriger les éventuelles anomalies et d'améliorer le paramétrage du dispositif.

CHAPITRE 2 : AGIR SUR LES IMPACTS

2.1. Sauvegarder les données à caractère personnel

- Effectuer une sauvegarde des données à caractère personnel, qu'elles soient sous forme papier ou électronique, de manière régulière, selon les besoins de disponibilité et d'intégrité des métiers ;

- Mettre en œuvre des mécanismes de chiffrement du canal de transmission des données dans le cas où la sauvegarde est automatisée par le réseau ;

- Protéger les données à caractère personnel sauvegardées au même niveau de sécurité qu'en exploitation ;

- Tester les sauvegardes de manière régulière ;

- Tester l'intégrité des données à caractère personnel sauvegardées si les besoins des métiers le nécessitent ;

- 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.

2.2. Protéger les archives des données à caractère personnel

- Vérifier que les processus de gestion des archives sont définis ;
- Vérifier que les rôles en matière d'archivage sont identifiés ;
- 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 ;
- Déterminer les moyens de protection de la confidentialité des données à caractère personnel archivées selon les risques identifiés ;
- Vérifier que les autorités d'archivage (responsable de la conservation) disposent d'une politique d'archivage ;
- Vérifier qu'il existe une déclaration des pratiques d'archivage ;

2.3. Contrôler l'intégrité des données à caractère personnel

- 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 ;
- Définir le moment auquel la fonction est appliquée et celui où le contrôle doit être effectué selon le déroulement du processus métier.

2.3.1. Spécificités pour une fonction de hachage

Utiliser un mécanisme reconnu par les organisations compétentes.

2.3.2. Spécificités pour un code d'authentification de message

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

2.3.3. Spécificités pour une fonction de signature électronique

- N'employer une bi-clé que pour un seul usage ;
- Recourir à des solutions de signatures basées sur des algorithmes publics réputés forts ;
- Choisir un mécanisme reconnu par les organisations compétentes et qui dispose d'une preuve de sécurité ;
- Générer les clés conformément aux meilleures pratiques ISO 27001 ;
- Mettre en place des mécanismes de vérification des certificats électroniques ;
- 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.

2.4. Tracer l'activité sur le système informatique

- Mettre en place une architecture de journalisation permettant de conserver une trace des événements de sécurité et du moment où ils ont eu lieu ;

- 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 ;

- Respecter les exigences de la loi relative à la protection des données à caractère personnel si les événements journalisés comprennent des données à caractère personnel ;

- 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 (06), hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques.

2.4.1. Spécificités pour un poste client

- 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 ;

- 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

- 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 ;

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

2.4.3. Spécificités pour un équipement réseau

- 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 pour les routeurs.

2.4.4. Spécificités pour un serveur

- 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 ;

- 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.

2.5. Gérer les violations de données à caractère personnel

- Définir les rôles et responsabilités des parties prenantes, ainsi que les procédures de remontées d'informations et de réaction, en cas de violation de données à caractère personnel ;

- Etablir un annuaire des personnes en charges de gérer les violations de données à caractère personnel ;

- Elaborer un plan de réaction en cas de violation de données à caractère personnel pour chaque risque élevé, le tenir à jour et le tester périodiquement (par exemple tous les 2 ans) ;

- Permettre de qualifier les violations de données à caractère personnel selon leur impact sur les libertés et la vie privée des personnes concernées ;

- Traiter les événements selon leur qualification (événement : le consigner et avertir le Correspondant à la protection, incident : le résoudre et si possible notifier les personnes concernées par la violation, sinistre : déclencher le lancement d'une analyse approfondie, crise : déclencher un plan de gestion préalablement établi) ;

- Tenir à jour un inventaire des violations de données à caractère personnel ;

- Etudier la possibilité d'améliorer les mesures de sécurité en fonction des violations de données à caractère personnel qui ont eu lieu.

CHAPITRE 3 : AGIR SUR LES SOURCES DE RISQUES

3.1. S'éloigner des sources de risques

- Placer les produits dangereux (inflammables, combustibles, corrosifs, explosifs, aérosols) dans des lieux de stockage appropriés et éloignés de ceux où sont traitées les données à caractère personnel ;

- Eviter les zones géographiques dangereuses (zones inondables, proximité d'aéroports, zones d'industries chimiques) ;

- Ne pas stocker les données dans un Etat étranger sauf s'il existe des garanties permettant d'assurer un niveau suffisant de protection de la vie privée, des libertés et droits fondamentaux. Il est sans ignorer que le responsable du traitement reste responsable de la sécurité des données à caractère personnel stockées et doit s'assurer du niveau de sécurité du stockage.

3.2. Marquer les documents contenant les données à caractère personnel

- Porter une mention visible et explicite sur chaque page des documents papier ou électroniques qui contiennent des données à caractère sensibles ;

- Porter une mention visible et explicite dans les applications métiers permettant d'accéder à des données à caractère personnel.

3.3. Gérer les personnes internes qui ont un accès légitime

- Déterminer les rôles et responsabilités en matière de protection des données à caractère personnel ;

- Déterminer les conséquences prévues pour les personnes ayant un accès légitime aux données à caractère personnel 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 données à caractère personnel ;

- Obtenir l'engagement des personnes ayant un accès légitime aux données à caractère personnel à respecter les mesures déterminées (faire signer un engagement de confidentialité ou prévoir dans les contrats de travail une clause de confidentialité spécifique aux données à caractère personnel) ;

- Sensibiliser les personnes ayant un accès légitime aux données à caractère personnel 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 ;

- Former convenablement les personnes ayant un accès légitime aux données à caractère personnel 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 ;

- Déterminer la procédure à appliquer systématiquement au départ ou au changement d'affectation d'une personne ayant un accès légitime aux données à caractère personnel.

3.4. Gérer les droits de traitement des utilisateurs sur les données à caractère personnel

- Gérer les profils d'utilisateurs en séparant les tâches et les domaines de responsabilité, afin de limiter l'accès aux données à caractère personnel aux seuls utilisateurs habilités, en appliquant les principes du besoin d'en connaître et du moindre droit de traitement ;

- Identifier toute personne ayant un accès légitime aux données à caractère personnel (employés, contractants et autres tiers) par un identifiant unique ;

- Limiter l'accès aux outils et interfaces d'administration aux personnes habilitées ;

- Limiter l'utilisation des comptes permettant de disposer de droits de traitement 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 ;

- Chaque compte doit avoir un mot de passe propre ;

- Journaliser les informations liées à l'utilisation des droits de traitement ;

- Editer une revue annuelle des droits de traitement afin d'identifier et de supprimer les comptes non utilisés ;

- 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.

3.5. Authentifier les personnes désirant accéder aux données à caractère personnel

- Choisir un moyen d'authentification pour les ouvertures de session, adapté au contexte, au niveau des risques et à la robustesse attendue ;

- 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 ;

- 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) ;

- Authentifier le poste de travail auprès du système d'information distant (serveurs) à l'aide de mécanismes cryptographiques.

3.5.1. Spécificités pour une authentification par certificat électronique

- N'employer une clé que pour un seul usage ;
- Recourir à des solutions d'authentification basées sur des algorithmes publics réputés forts ;
- Choisir un mécanisme reconnu par les organisations compétentes et qui dispose d'une preuve de sécurité ;
- Générer les clés conformément aux meilleurs pratiques ISO 27001 ;
- Mettre en place des mécanismes de vérification des certificats électroniques ;
- 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.

3.6. Gérer les authentifiants

- 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 ;
- 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 ;
- 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, et le contraindre à le modifier lors de sa première connexion et lorsqu'un nouveau mot de passe lui est fourni (en cas d'oubli) ;

- Stocker les informations d'authentification (mots de passe d'accès aux systèmes d'information, clés privées liées aux certificats électroniques) de façon à être accessibles uniquement par des utilisateurs autorisés ;

- Placer les authentifiants permettant l'administration des ressources des systèmes informatiques sous séquestre et les tenir à jour ;

- 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, de mots de passe à usage unique ;

- 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 d'administrateur).

3.7. Gérer les tiers qui ont un accès légitime aux données à caractère personnel

- Identifier tous les tiers qui ont ou pourraient avoir un accès légitime aux données à caractère personnel ;

- 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 ;

- Déterminer les responsabilités respectives en fonction des risques liés à ces données à caractère personnel ;

- Apprécier précisément les risques spécifiques que les accès aux données à caractère personnel 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 ;

- Formaliser les règles que les personnes doivent respecter durant tout le cycle de vie de la relation liée au traitement ou aux données à caractère personnel, selon la catégorie de personnes et les actions qu'elles vont réaliser ;

- Déterminer une procédure à suivre pour les requêtes de tiers autorisés.

3.7.1. Spécificités pour une sous-traitance

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

- 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...) ;

- 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.

3.7.2. Spécificités pour une externalisation

- Etudier 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 à l'externalisation de tout ou partie du système d'information.

3.7.3. Spécificités pour un hébergement mutualisé

- Etudier 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) ;

- Contractualiser les règles de suivi de la ressource co-herbégée ;

- Contractualiser les règles de gestion des attaques informatiques ;

- Contractualiser les règles de gestion des incidents ;

- Contractualiser les règles de réversibilité.

3.7.4. Spécificités pour une maintenance

- Chiffrer ou effacer les données à caractère personnel de manière sécurisée avant l'envoi en maintenance externe de toute ressource informatique (serveur, poste client, équipement réseau) ;

- Si les données à caractère personnel ne peuvent être chiffrées ou effacées dans leur totalité (panne d'un disque dur, dysfonctionnement) et qu'elles ne sont pas sensibles, faire signer un engagement de confidentialité au fournisseur de service de maintenance, ou bien faire des réparations sur place en présence d'un membre du service en charge de l'informatique ;

- Dans le cas de données à caractère personnel sensibles, 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.

3.7.5. Spécificités pour une télémaintenance

- 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 (SSH ou équivalent) ;

- 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 les réseaux interurbains (WAN) nationaux.

3.8. Lutter contre les codes malveillants

- Installer un antivirus sur les serveurs et postes de travail et le configurer ;

- Tenir les logiciels antivirus à jour ;

- 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.

3.9. Contrôler l'accès physique des personnes

- Distinguer les zones des bâtiments selon les risques ;

- Tenir à jour une liste des personnes (visiteurs, employés, employés habilités, stagiaires, prestataires) autorisées à pénétrer dans chaque zone ;

- Choisir des moyens d'authentification des collaborateurs proportionnels aux risques selon chaque zone ;

- 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 ;

- Conserver une trace des accès après en avoir informé les personnes concernées ;

- Faire accompagner les visiteurs, en dehors des zones accessibles au public par un agent de l'organisme ;

- Protéger les zones plus sensibles de manière proportionnelle aux risques ;

- Installer un dispositif permettant d'être alerté en cas d'effraction ;

- Se protéger contre les sources de risques non humaines :

    - Mettre en place des moyens de prévention, détection et protection contre l'incendie,

    - Mettre en place des moyens de surveillance de la température,

    - Mettre en place des moyens de surveillance et de secours de l'alimentation électrique,

    - Mettre en place des moyens de prévention des dégâts des eaux,

    - 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 chaque année.

CHAPITRE 4 : AGIR SUR LES SUPPORTS

4.1. Réduire les vulnérabilités des logiciels

- Tenir les systèmes et applications à jour (versions, correctifs de sécurité) ou quand cela est impossible, isoler la machine et porter une attention particulière aux journaux ;

- Documenter les configurations et les mettre à jour à chaque changement notable ;

- Limiter les possibilités de détournements d'usages ;

- Protéger les accès ;

- Activer les mesures de protection offertes par le système et les applications ;

- Rechercher les vulnérabilités exploitables, notamment sur les serveurs les plus critiques ;

- Protéger l'intégrité, la disponibilité et si besoin la confidentialité des logiciels et des codes sources des applications développées en interne ;

- Contrôler l'intégrité du système à l'aide de contrôleurs d'intégrité (qui vérifient l'intégrité de fichiers choisis.

4.1.1. Spécificités pour les postes de travail

- Interdire le partage de répertoires ou de données localement sur les postes de travail ;
- Stocker les données des utilisateurs sur un espace réseau sauvegardé et non sur les postes de travail ;
- Interdire l'exécution des applications téléchargées ne provenant pas de sources sûres.

4.1.2. Spécificités pour les téléphones mobiles/smartphones

- Configurer les téléphones avant d'être livrés aux utilisateurs ;
- Informer les utilisateurs sur l'usage du téléphone, des applications, des services fournis et des règles de sécurité à respecter ;
- Sécuriser le serveur ;
- Sécuriser la fin de vie de l'appareil.

4.1.3. Spécificités pour les acquisitions de logiciels

- Vérifier que les développeurs et les mainteneurs (maintenanciers) disposent de ressources suffisantes pour maîtriser leurs actions ;
- Privilégier les applications interopérables et ergonomiques ;
- Effectuer les développements informatiques dans un environnement informatique distinct de celui de la 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 (exemple : 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 ;

- Interdire l'utilisation de données à caractère personnel réelles avant la mise en opération, et les rendre anonymes si nécessaire.

4.1.4. Spécificités pour les bases de données

- 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 ;
- Prévoir des mesures particulières pour les bases de données sensibles.

4.1.5. Spécificités pour les navigateurs Internet

- Sécuriser la configuration du navigateur Internet (la configuration doit inclure la protection des informations nominatives stockées par le navigateur : mots de passe, certificats, formulaires) ;

- Déployer le navigateur dont la configuration a été sécurisées 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.

4.2. Réduire les vulnérabilités des matériels

- Tenir à jour un inventaire des ressources informatiques utilisées ;

- Cloisonner les ressources de l'organisme en cas de partage de locaux ;

- Empêcher l'accès à des données à caractère personnel sur des ressources informatiques mises au rebut ;

- 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 ;

- Protéger l'accès aux matériels sensibles ;

- Limiter les possibilités de modification des matériels.

4.2.1. Spécificités pour les postes de travail

- 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

- Chiffrer les données à caractère personnel stockées sur les postes nomades

- Limiter le stockage de données à caractère personnel sur les postes nomades au strict nécessaire, et éventuellement l'interdire lors de déplacement à l'étranger ;

- Assurer la disponibilité des données à caractère personnel stockées sur les postes nomades (les copier dès que possible sur un autre poste, sur un serveur...) ;

- Purger les données à caractère personnel 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.

4.2.3. Spécificités pour les supports amovibles

- Limiter l'usage des supports amovibles à ceux fournis par le service en charge de l'informatique ;

- Interdire l'utilisation des clés USB à connexion sans fil (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 données à caractère personnel stockées sur un support amovible ;

- Restituer les supports amovibles défectueux ou plus utiles au service en charge de l'informatique ;

- Détruire de manière sécurisée les supports de données à caractère personnel qui sont inutiles.

4.2.4. Spécificités pour les imprimantes et copieurs multifonctions

- Changer les mots de passe « constructeur » par défaut ;
- Désactiver les interfaces réseau inutiles ;
- Désactiver ou supprimer les services inutiles ;
- Chiffrer les données sur le disque dur lorsque cette fonction est disponible ;
- Limiter l'envoi de documents numérisés aux adresses de messagerie internes et dans certains cas limiter l'envoi de documents numérisés à une seule adresse de messagerie ;
- Dans le cas d'une maintenance par un tiers, prévoir les mesures destinées à empêcher l'accès aux données à caractère personnel ;
- 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 ;
- Empêcher l'accès à des données à caractère personnel stockées sur des imprimantes ou copieurs multifonctions mis au rebut.

4.3. Réduire les vulnérabilités des canaux informatiques

- Maintenir à jour une cartographie détaillée du réseau et s'assurer que les mesures prévues sont bien appliquées à chacun d'entre eux ;

- Assurer la disponibilité des canaux informatiques ;

- Segmenter le réseau en sous-réseaux logiques étanches selon les services censés y être déployés ;

- Interdire toute communication directe entre des postes internes et l'extérieur ;

- N'utiliser que les flux explicitement autorisés, c'est-à-dire limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées, à l'aide d'un pare-feu ;

- Surveiller l'activité réseau après en avoir informé les personnes concernées ;

- Prévoir un plan de réponse en cas d'intrusion majeure contenant les mesures organisationnelles et techniques pour délimiter et circonscrire la compromission (faire : une cartographie du réseau, une liste des personnels en mesure d'intervenir sur les systèmes, les 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 (utiliser l'adresse MAC afin de détecter et d'empêcher la connexion d'un dispositif non répertorié) ;

- Sécuriser les flux d'administration et restreindre, voire interdire l'accès physique et logique aux ports (ports physiques) de diagnostic et de configuration à distance ;

- Interdire le raccordement d'équipements informatiques non maîtrisés ;

- Transmettre les secrets garantissant la confidentialité de données à caractère personnel (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 (envoyer un mot de passe par mail et communiquer le mot de passe par téléphone ou *sms*...).

4.3.1. Spécificités pour les connexions aux équipements actifs du réseau

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

4.3.2. Spécificités pour les outils de prise de main à distance

- 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 de main à distance ;

- Sécuriser le flux d'authentification sécurisé (aucun mot de passe en clair) ;

- Obliger à faire accepter la prise de main à distance par l'utilisateur de manière explicite par une action sur le poste de travail (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

- Mettre en place une solution d'authentification forte des utilisateurs accédant à distance au système d'information interne (quand cela est possible) ;

- Chiffrer les communications entre le poste nomade et le système d'information interne ;

- 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.

4.3.4. Spécificités pour les interfaces sans fil (wifi, bluetooth, infrarouge, 3G...)

- Interdire les communications non sécurisées dans le cas de connexions à l'aide d'interfaces sans fil ;

- 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.

4.3.5. Spécificités pour le Wifi

- 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.

4.3.6. Spécificités pour le bluetooth

- 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.

4.3.7. Spécificités pour l'infrarouge

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+...)

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

4.3.9. Spécificités pour la navigation sur Internet

- Utiliser le protocole SSL (HTTPS) pour assurer l'authentification des serveurs et la confidentialité des communications.

4.3.10. Spécificités pour le transfert de fichiers

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

4.3.11. Spécificités pour le fax

- 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

- 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 (perte de disponibilité de l'accès au réseau inter-urbain). Ne les activer que lors de leur utilisation et désactiver leur éventuelle interface sans fil (wifi).

4.3.13. Spécificités pour la messagerie électronique

- Chiffrer les pièces jointes contenant des données à caractère personnel ;

- Sensibiliser les utilisateurs au fait qu'ils doivent éviter d'ouvrir des courriers électroniques d'origine inconnue, surtout les pièces jointes à

risque (extensions .pif,.com, .bat .exe, .vbs, .ink...) 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.

4.3.14. Spécificités pour les messageries instantanées

- Sensibiliser les utilisateurs au fait qu'ils doivent faire attention à ce qu'ils écrivent, éviter de donner de vraies données à caractère personnel 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 nécessaire, sensibiliser les utilisateurs aux risques et bonnes pratiques à adopter (les utilisateurs ne doivent installer que des logiciels téléchargés depuis le site de l'éditeur).

4.4. Réduire les vulnérabilités des personnes

- Vérifier que les personnes ayant accès aux données à caractère personnel et au traitement sont aptes à exercer leur fonction ;

- S'assurer que les conditions de travail des personnes ayant accès aux données à caractère personnel et au traitement sont satisfaisantes ;

- Sensibiliser les personnes ayant accès aux données à caractère personnel et au traitement aux risques liés à l'exploitation de leurs vulnérabilités.

4.5. Réduire les vulnérabilités des documents papier

- Choisir des supports papier et des procédés d'impression appropriés aux conditions de conservation ;

- Récupérer les documents imprimés contenant des données à caractère personnel immédiatement après leur impression ;

- Limiter la diffusion des documents papier contenant des données à caractère personnel qu'aux personnes ayant le besoin d'en disposer dans le cadre de leur activité ;

- Stocker les documents papier contenant des données à caractère personnel dans un meuble sécurisé ;

- Détruire les documents papier contenant des données à caractère personnel qui ne sont plus utiles (à l'aide d'un broyeur approprié).

4.6. Réduire les vulnérabilités des canaux papier

Limiter la circulation (au sein de l'entreprise, transport en véhicule, envoi par la poste) des canaux papier de sorte qu'ils ne soient pas exploités pour porter atteinte aux données à caractère personnel.

- N'envoyer que les documents papier contenant des données à caractère personnel nécessaires au traitement ;

- Garder une trace précise de la transmission des documents papier contenant des données à caractère personnel ;

- Choisir un canal de transmission adapté aux risques et à la fréquence de transmission (recours à une entreprise spécialisée, emploi des ressources de l'entreprise : chauffeurs, véhicules) ;

- Améliorer la confiance envers le transporteur de documents papier contenant des données à caractère personnel ;

- Protéger les documents papier contenant des données à caractère personnel (apposer une marque «*Confidentiel* » sur les enveloppes). Si les risques sont importants, il peut être utile de conserver une copie des documents transmis...

CHAPITRE 5 : AU NIVEAU DE L'ORGANISME

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

Disposer d'une organisation apte à diriger et contrôler la protection des données à caractère personnel au sein de l'entreprise.

- Faire désigner par le responsable des traitements une personne en charge de l'assister et lui accorder les moyens nécessaires à l'exercice de sa mission (désignation d'un correspondant à la protection) ;

- Définir les rôles, responsabilités et interactions entre toutes les parties prenantes dans le domaine ;

- Créer un comité de suivi, composé du responsable du traitement, du correspondant à la protection et des parties intéressées. Ils doivent se réunir de manière régulière pour fixer les objectifs à atteindre et faire un bilan sur l'ensemble des traitements de l'entreprise.

5.2. Gérer les risques sur la vie privée

- Réaliser une cartographie des risques sur l'ensemble des traitements de l'organisme ;

- Ajuster la cartographie à chaque évolution majeure et de manière périodique.

5.3. Gérer la politique de protection de la vie privée

- Formaliser les éléments importants relatifs au domaine des données à caractère personnel au sein d'une base documentaire qui constitue la politique de protection des données à caractère personnel, dans une forme aux différents contenus (risques, grands principes à respecter, objectifs à

atteindre, les règles à appliquer...) et aux différentes cibles de communication (usagers, service en charge de l'informatique, décideurs...) ;

- Faire connaître la politique de protection des données à caractère personnel aux personnes qui doivent l'appliquer ;

- Permettre aux personnes qui doivent appliquer cette politique 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 en conséquence ;

- Etablir un plan d'action pluriannuel et suivre sa mise en œuvre ;

- Prévoir les dérogations aux règles de la politique de protection des données à caractère personnel ;

- Prévoir de prendre en compte les difficultés rencontrées dans l'application de la politique de protection des données à caractère personnel ;

- Vérifier la conformité aux règles de la politique de protection des données à caractère personnel et la mise en œuvre du plan d'action de manière régulière ;

- Réviser la politique de protection des données à caractère personnel de manière régulière.

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

Prendre en compte la protection des données à caractère personnel dans tout nouveau traitement.

- Privilégier le recours à des référentiels éprouvés et reconnus (recourir de préférence à des normes internationales, des guides publiés par des institutions telles que la Commission Nationale de l'Informatique et des Libertés (CNIL) et l'Agence Nationale de la Sécurité des Systèmes d'Informations (l'ANSSI) ;

- Effectuer les formalités auprès de l'Autorité de protection avant le lancement d'un nouveau traitement.

5.5. Superviser la protection de la vie privée

Disposer d'une vision globale et à jour de l'état de protection des données à caractère personnel et de la conformité à loi relative à la protection des données à caractère personnel.

- Effectuer régulièrement des contrôles des traitements de données à caractère personnel afin de vérifier leur conformité à la loi ainsi que l'effectivité et l'adéquation des mesures prévues ;

- Fixer des objectifs dans le domaine de la protection des données personnelles et des indicateurs permettant de vérifier l'atteinte de ces objectifs ;

- Faire un bilan protection des données à caractère personnel de manière régulière.