Réception au contrôle de légalité le 14 janvier 2022
Référence technique : 017-221700016-20220114-18787-DE-1-1

MODIFICATION DE LA CHARTE DE L'UTILISATEUR PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL ET DU SYSTÈME D'INFORMATION

Première commission : Finances et Administration Générale, Evaluation des Politiques Publiques et Solidarité Territoriale

COMMISSION PERMANENTE du 14 janvier 2022

DELIBERATION N° 2022-01-14-1

La Commission Permanente du Département réunie à la Maison de la Charente-Maritime de La Rochelle, le 14 janvier 2022 à 14h30, sous la présidence de Mme Sylvie MARCILLY, Présidente du Département,

Agissant par délégation de l'Assemblée Départementale (délibération du 1er juillet 2021),

Considérant l'application du Règlement Général de Protection des Données depuis le 25 mai 2018,

Considérant le cadre général de la protection des données à caractère personnel et du système d'information départemental détaillant le cadre organisationnel, juridique et méthodologique de la protection de l'information en vigueur depuis 2017,

Considérant que la charte de l'utilisateur présentant les droits et devoirs consécutifs aux responsabilités de la collectivité et de l'ensemble des utilisateurs du système d'information départemental pour l'exercice de leurs missions quelle que soit leur qualité fait partie intégrante de ce cadre général,

Considérant que par délibération du 19 janvier 2018 de la Commission Permanente a approuvé ladite charte,

Considérant qu'elle doit faire l'objet d'une revue régulière et intégrer l'ensemble des mesures et évolutions techniques,

Considérant que cette charte a été présentée au Comité Technique le 6 décembre 2021,

DECIDE d'approuver la nouvelle charte d'utilisation relative à la protection des données à caractère personnel et du système d'information du Département de la Charente-Maritime, jointe en annexe et de la rendre opposable à toute personne traitant des données à caractère personnel dans le cadre de ses missions pour le Département et à tout utilisateur du système d'information à compter du 17 janvier 2022.

Adopté à l'unanimité

Pour extrait conforme,
P/La Présidente du Département,
Le premier Vice-Président,
Loïc GIRARD

Charte de l'Utilisateur : protection des données à caractère personnel et du système d'information

TABLE DES MATIERES

Pour information, tous les termes suivis d'un * font l'objet d'une définition en fin de charte

1 - PREAMBULE

Le Département de la Charente-Maritime apporte la plus grande importance :

- à la confidentialité et à la sécurité de l'ensemble des informations et des données personnelles (des usagers et des agents) collectées et traitées dans le cadre de ses missions de service public qui participe au patrimoine informationnel de la collectivité..
- à la protection des moyens informatiques, réseaux, télécom (fixes et mobiles) et reprographiques, de traitement et de stockage de l'information et à l'usage qui en est fait au sein de ses services.
- au respect des obligations légales en matière de protection des données à caractère personnel et de sécurité des systèmes d'information.
- Au respect des obligations réglementaires d'archivage

La protection du patrimoine informationnel et la sécurisation maitrisée du système d'information sont deux éléments clés de la performance du Département.

L'objectif de la présente Charte est de conduire chacun à être acteur des usages et de la protection des informations, des ressources informatiques et de télécommunication utilisées dans la collectivité.

1.1 - OBJET

La Charte présente les droits et les devoirs consécutifs aux responsabilités de la collectivité et des utilisateurs, dans le cadre de la protection des données et de l'usage du système d'information du Département.

- Elle apporte conseils et rappelle des principes qui s'appliquent à tous.
- Elle définit les conditions générales d'utilisation du système d'information au sein du Département conformément au cadre légal et réglementaire.
- Elle vise également à informer les utilisateurs des enregistrements ou contrôles éventuels mis en place.

L'ensemble de ces règles permet de renforcer la protection du Système d'Information*, de maintenir un environnement de travail professionnel efficace et sécurisé afin de protéger les informations du Département, tout en garantissant l'équilibre des intérêts de chacun.

1.2 - PERIMETRE D'APPLICATION

Cette charte est partie intégrante du référentiel documentaire relatif à la gouvernance de la donnée. Son application est complétée d'une part par des guides de bonnes pratiques, guide d'utilisation spécifiques aux matériels ou aux applications liés au Système d'Information du Département et d'autre part par des procédures et fiches réflexes liées à la protection des données à caractère personnel et à la sécurité des systèmes d'information, accessibles depuis YATOO et les sites SharePoint « DG – Protection des données » et « Aide en Ligne ».

Le respect des règles archivistiques et de la législation sur la gestion des archives publiques est pris en compte dans le cadre de cette charte.

L'ensemble de ces règles s'appliquent à tout utilisateur du Système d'Information* du Département de la Charente-Maritime pour l'exercice de ses activités départementales quelle que soit sa position (agent permanent, agent temporaire, stagiaire, apprenti, représentant des organisations syndicales, élus, sous-traitant, …).

Le périmètre d'application est valable autant pour les données numériques que pour les données et informations contenues dans les documents papiers.

2 - ORGANISATION INTERNE RELATIVE A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL ET A LA SECURITE DES SYSTEMES D'INFORMATION

Dans le but de garantir la protection des données et le bon fonctionnement du Système d'Information, le Département de la Charente-Maritime a décidé de mettre en place une organisation en charge de traiter la protection des informations et la sécurité des systèmes informatiques, dans le respect des obligations légales et réglementaires en vigueur.

Cette organisation s'appuie notamment sur la désignation d'un Responsable de la Sécurité du Système d'Information (RSSI*), d'un Délégué à la protection des données (DPD) et de Relais Informatiques et Libertés (RIL*) dans les directions métiers ainsi que sur La Commission d'Homologation de la Protection de l'Information et des Données à Caractère Personnel (arrêté 28/04/2017) présidée par le Directeur Général des Services**.**

La Direction Générale des Services attire l'attention sur le fait que chaque utilisateur agent (cadre ou non cadre), sous-traitant, partenaire ou prestataire intervenant au nom du Département est un acteur essentiel de la protection des informations qu'il traite dans le cadre de ses missions en respectant les règles de cette Charte.

3 - REGLES D'UTILISATION DES DONNEES A CARACTERE PERSONNEL

Dans le cadre de ses missions de service public, le Département collecte et traite des données à caractère personnel (DCP). Ces traitements répondent à des règles et obligations que chaque agent au quotidien doit respecter (8 principes clés) :

1 - Détermination des finalités : Le Département détermine les finalités pour lesquelles il recueille des données

2 - Principe de légalité : Le Département traite ces données dans le respect de la légalité

3 - Limitation de la Collecte Le Département limite la collecte de ces données au strict nécessaire

4 - Information des personnes : Le Département informe l'usager sur la gestion de ses données et sur ses droits

5 - Limitation de la conservation des données : Le Département ne conserve les données à caractère personnel « en base active » que le temps nécessaire au traitement pour lequel elles ont été collectées. Une Durée d'Utilisation Courante (DUC) leur est attribuée. A l'échéance de la DUC, le Département s'engage à respecter le sort final et la durée définie de conservation indiqués par les guides d'archivage et tableaux de gestion (législation et réglementation des archives publiques, finalité

de conservation définitive à des fins de recherches historiques ou statistiques ou finalité de conservation intermédiaire avec destruction à des fins de preuve)

6 - Destinataires des données : Le Département ne transmet ces données qu'à des destinataires habilités

7 - Sécurité des données : Le Département sécurise les données par la mise en œuvre des moyens techniques et organisationnels pour appliquer les principes de sécurité en vigueur, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle

8 - Droits liés au traitement des données : Le Département respecte les droits des usagers et y répond selon les délais légaux

3.1 - COLLECTE DES DONNEES A CARACTERE PERSONNEL

Tout traitement comportant des DCP ne pouvant se faire que dans le cadre d'une finalité définie et déclarée, chaque agent doit veiller à limiter la collecte d'informations strictement nécessaires **à la finalité du traitement concerné**. Cette collecte ne peut se faire à l'insu de l'usager.

Les agents s'engagent à n**e collecter que des données adéquates, pertinentes et non excessives** au regard de la finalité du traitement

L'agent doit **informer l'usager** ou **le bénéficiaire** au moment de la collecte ou lors du 1er échange en cas de collecte. Cette information doit a minima comporter :

- L'identité et coordonnées du Responsable de Traitements
- La finalité du traitement
- La base juridique qui légalise le traitement
- Les catégories de données collectées et leurs sources en cas de collecte indirecte
- Les destinataires des données (internes ou externes)
- La durée de conservation des données
- Les coordonnées du Délégué à la protection des données
- Les droits de l'usager selon la base légale appliquée et les modalités pratiques pour exercer vos droits
- Le droit d'introduire une réclamation auprès de la CNIL

(Un modèle de mention d'information est accessible depuis le site SharePoint dédié à la protection des données ou depuis YATOO)

Lorsque le traitement est fondé sur le consentement de la personne, l'agent s'assure du consentement écrit de l'usager et met en place les mesures pour conserver la trace de celui-ci. *(modèle accessible depuis Yatoo et le site SharePoint « DG – Protection des données et sécurité du SI »).*
Le consentement peut être retiré à tout moment par l'usager au travers d'une procédure aussi simple que celle qui a permis d'obtenir le consentement.

Enfin, l'agent s'engage à ne pas utiliser les données collectées dans un autre but que celui annoncé à l'usager.

3.2 - CREATION DE FICHIERS CONTENANT DES DONNEES D'USAGERS, DE BENEFICIAIRES OU D'AGENTS

La création de fichiers contenant des données à caractère personnel n'est autorisée qu'à la condition de respecter les procédures internes définies par le Département qui prévoient notamment l'obligation de recenser la création de tout nouveau traitement dans le registre départemental des traitements maintenu par la DPD.

L'agent s'engage à :

- Vérifier que le traitement est déclaré dans le registre départemental (Cf Yatoo espace informatique et Libertés) ou à se rapprocher de son Référent Informatique & Libertés (RIL) ou de la DPD en cas de doute ;

  Tout nouveau traitement doit faire, sans délai, l'objet d'une déclaration auprès de la DPD pour instruction et inscription dans le registre départemental.
  Il est de la responsabilité des directions métiers de renseigner la fiche de traitement à partir du modèle mis à disposition dans le site « SharePoint Protection des données et du SI » et de l'adresser à la DPD.
  La consultation de la DPD et du RSSI doit être systématiquement effectuée dès l'initialisation d'un projet impliquant un traitement de données à caractère personnel.

  Toute modification substantielle (nouveau destinataire, changement de technologie, nouvelle collecte de données, évolution du cadre juridique applicable…) d'un traitement déjà recensé doit faire l'objet d'une information systématique auprès de la DPD.

- Limiter l'accès aux fichiers autorisés aux seuls personnels habilités à les utiliser ;

- Ne pas faire de copies multiples des fichiers si cela ne se justifie pas, notamment lors de l'usage de supports amovibles tels que les clés USB ou la transmission de courriels ou lorsque le traitement comporte des données sensibles ou perçues comme sensibles ;

Respecter les durées de conservation (documents papiers et numériques) selon les tableaux de gestion* édictés par les Archives Départementales (cf. YATOO et 5.7 de la présente Charte). Pour en savoir plus se référer au guide pratique publié par la CNIL sur les durées de conservation (Cf Référentiels CNIL dans le site Sharepoint « DG-Protection DCP - Securite SI)

3.3 - USAGE DES ZONES COMMENTAIRES

L'usage des zones commentaires sur les formulaires de collecte, dans les logiciels professionnels, dans les bases de données ou dans les fichiers bureautiques (EXCEL et WORD) est strictement réservé aux informations d'ordre général et en aucun cas ne peut porter atteinte aux droits des personnes concernées.

Les commentaires désobligeants, discriminants, voire injurieux, ou encore faisant apparaitre des données dites « sensibles » telles que des données relatives à la santé, sont proscrits et il convient de n'utiliser que des termes neutres et objectifs.

L'agent s'engage à ne pas mentionner des informations subjectives et/ou non autorisées par la législation dans les zones de commentaires disponibles dans les formulaires et/ou les fichiers Excel sans en informer l'usager et sans lui avoir demandé son accord au préalable.

3.4 - TRAITEMENT DE DONNEES SENSIBLES OU PERÇUES COMME SENSIBLES

La réglementation et les directives de la CNIL* imposent un traitement spécifique des données sensibles (Opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, données de santé, origine raciales ou ethniques, infractions, condamnations, mesures de sécurité) et des données perçues comme sensibles (numéro de sécurité sociale (NIR), appréciation sur les difficultés sociales, données biométriques, données bancaires).

Chaque agent traitant ce type de données doit veiller à :

- Ne traiter ces données que dans le cadre des obligations légales en vigueur et en respectant les procédures déclaratives auprès de la DPD.

- Limiter strictement le traitement des données relatives aux condamnations pénales et aux infractions : les documents relatifs aux condamnations pénales et aux infractions ne peuvent en aucun cas faire l'objet d'un traitement interne à la collectivité autre que celui déclaré lors de la collecte. Seules la conservation de ces pièces selon la politique d'archivage en vigueur et la transmission de ces documents à des destinataires dès lors qu'un cadre légal le justifie, sont autorisées.

- Ne pas utiliser le numéro de Sécurité sociale (NIR) comme identifiant unique.
  Cet identifiant ne peut être utilisé que dans la mesure où un cadre légal l'autorise.

- Limiter l'accès aux données (papiers et numériques) concernant les difficultés sociales des usagers aux seuls agents habilités : Seuls les professionnels de l'action sociale sont habilités à collecter et à traiter des données sur les difficultés sociales des usagers.

- S'assurer que la protection des données (papier ou numérique) est bien assurée (notamment lors de leur stockage et de leur transfert) et à alerter la DPD en cas de violation sur ces données*

L'agent s'engage à ne pas transmettre des fichiers contenant des données sur des usagers sans activer les mécanismes de sécurité prévus par le Département. Le RSSI (Responsable de la Sécurité du SI) du Département peut apporter des précisions sur les modalités techniques à appliquer pour un transfert sécurisé.

Tout transfert non sécurisé de fichiers contenant des données personnelles à des destinataires externes au Département doit être justifié et validé par le RSSI, par la DPD ou par la hiérarchie de l'agent.

3.5 - RESPECT DES DROITS DES USAGERS ET DES AGENTS

Le cadre légal en vigueur donne des droits aux usagers et aux agents concernant l'usage et les traitements qui sont réalisés par le Département sur leurs données à caractère personnel. Ils peuvent ainsi exercer leur droit d'accès, de rectification, de suppression de leurs données et s'opposer à des traitements pour des raisons légitimes. (dans le respect de la législation et du code du patrimoine)

L'agent s'engage à prendre en compte toutes les demandes exprimées par les usagers et à les traiter en appliquant les procédures en vigueur au sein du Département et dans le respect de la législation sur les archives publiques et des exceptions liées aux données conservées à des fins de recherches historiques ou statistiques. **L'agent est tenu d'informer sans délai la DPD et le RIL de toute demande exprimée conformément à la procédure de droit d'accès** (Cf Procédure dans le site SharePoint GG-Protection des DCP et du SI – Espace Public – Référentiel documentaire – Procédures)

4 - DROIT A L'IMAGE

L'agent peut être amené, dans le cadre de ses missions professionnelles, à réaliser des photographies, des vidéos, des enregistrements. Cependant la législation française interdit l'utilisation de l'image ou l'enregistrement vidéo et sonore d'une personne ou d'un groupe sans son consentement explicite et écrit.

Sans ce consentement, ce qui a été réalisé par l'agent ne doit en aucun cas permettre d'identifier (directement ou indirectement) des personnes physiques (plaque immatriculation, personne de dos avec un tatouage, enregistrement vidéo…) ou des lieux privés.

Il est donc IMPERATIF d'éviter de photographier des personnes seules ou en groupe, de photographier des plaques d'immatriculation ou encore des habitations reconnaissables. Si toutefois, il est impossible d'obtenir une photo ou vidéo sans la présence d'éléments d'identification, ceux-ci devront être OBLIGATOIREMENT floutés ou masqués.

Cette mesure ne s'applique pas dans le cadre d'une manifestation publique.

Par ailleurs, toute prise de vue effectuée dans le cadre des activités de la collectivité ou dans ses locaux ne peut être utilisée à des fins personnelles et leur diffusion à l'extérieur est interdite sans l'autorisation écrite de la Direction Générale des Services pour les agents et du cabinet du Président pour les élus.

Pour plus de renseignements concernant le droit à l'image, contacter la DCSII.

5 - REGLES D'UTILISATION DU SYSTEME D'INFORMATION

5.1 - IDENTIFICATION, AUTHENTIFICATION ET HABILITATION

5.1.1 - IDENTIFICATION ET AUTHENTIFICATION PAR LE MOT DE PASSE

Tout nouvel arrivant se voit attribuer un identifiant et un mot de passe qui lui sont strictement personnels et confidentiels. Le mot de passe :

- authentifie la véracité d'une identité. Il ne peut en aucune manière être cédé à un tiers sans engager la responsabilité du titulaire.
- ne doit pas être communiqué (ni l'identifiant) à un remplaçant, un prestataire, un collègue, un stagiaire…
- doit respecter les règles de sécurité en vigueur élaborées par le RSSI (cf. Politique des mots de passe disponible sur le site SharePoint « Protection des données et SSI »).

Pour des raisons de sécurité, il est fortement recommandé de :

- ne pas utiliser pour son compte professionnel un mot de passe déjà utilisé pour un compte personnel ;
- s'assurer que son mot de passe n'est pas accessible à autrui (post it, étiquette sous clavier…).
- utiliser le gestionnaire de mots de passe « KeePass » disponible au sein de la collectivité. *Pour en savoir plus, consulter le tutoriel disponible sur le site SharePoint « Aide en Ligne ».*

5.1.2 - L'HABILITATION, UNE AUTORISATION STRICTEMENT PERSONNELLE

L'utilisateur n'a accès qu'aux seules informations et ressources dont il a besoin dans le cadre de ses missions.

En cas de changement de fonction, les habilitations sont modifiées pour répondre aux nouvelles missions de l'utilisateur en fonction des informations transmises par la DRH ou par la direction métier.

Pour information, cette autorisation est suspendue dès que les missions de l'utilisateur prennent fin même temporairement.

5.2 - UTILISATION DES EQUIPEMENTS PROFESSIONNELS

L'utilisateur doit

- Prendre soin du matériel mis à sa disposition ;
- Fermer les applications métiers en cas de non utilisation ;
- Veiller à ne pas exposer les informations confidentielles ou sensibles (fax, imprimante, photocopieur…) ;
- Installer sur ses équipements professionnels uniquement les logiciels disponibles dans son « centre logiciel ». Pour des besoins spécifiques, une demande devra nécessairement être réalisée sous SerenIT.

L'utilisateur ne doit pas

- Tenter d'usurper une identité ;
- Cacher son identité ;
- Mettre hors circuit un dispositif de sécurité ;
- Tenter d'installer un logiciel d'attaque ;
- Détourner de sa finalité un outil mis à sa disposition par le Département ;
- Modifier les paramètres de sécurité mis en place par la Direction du Système d'Information (DSI) sur l'ensemble de ses équipements professionnels.

5.2.1 - UTILISATION DU POSTE DE TRAVAIL

L'utilisateur doit

- Verrouiller son ordinateur avec l'option reprise par mot de passe même pour une absence de courte durée

(Appuyer simultanément sur les touches  du clavier + L)

- Éteindre l'ordinateur et l'écran le soir ;

Le saviez-vous ?
Un ordinateur en veille continue à consommer entre 20 et 40% de son énergie.
Pensez à éteindre vos appareils avec leurs boutons

L'utilisateur ne doit pas

- Rendre impossible l'analyse de son poste de travail par la DSI (« chiffrement » de ses données sans autorisation du Département).
- Sauvegarder ni stocker leurs documents professionnels sur le lecteur C:/ de son poste de travail *(Le C:/ désigne un espace de stockage propre à chaque poste de travail : il n'est donc pas possible pour la DSI de récupérer des documents situés sur cet espace en cas de perte de ceux-ci.)*

Pour information, la DSI ne sauvegarde pas de données sur le lecteur C:/ du poste de travail.

En cas de suppression d'un document professionnel :

- Sur G:/ (bureauti) : la DSI ne procédera à la restauration du fichier que sur demande effectuée sur SerenIT.
- Depuis un outil collaboratif (cf 5.6 de la présente Charte), l'utilisateur est autonome dans la récupération de ce document via l'utilisation de la « corbeille » présente sur chacun de ces outils. (cf. site SharePoint « Aide en Ligne »).

5.2.2 - UTILISATION DES TABLETTES, SMARTPHONES ET SUPPORTS AMOVIBLES

Tout équipement nomade (tablette, smartphone, PC portable) est chiffré avant remise à l'utilisateur pour éviter toute fuite d'information en cas de perte ou de vol du matériel.

L'utilisateur doit

- Utiliser les équipements de protection fournis avec l'équipement nomade ;
- Changer le code de verrouillage du Smartphone et de la tablette dès la réception du matériel ;
- Lorsqu'il quitte sa mission, remettre son matériel nomade à la DSI ou à son RI ;
- Verrouiller son smartphone et sa tablette après utilisation ;

L'utilisateur ne doit pas

- Donner son téléphone ou sa tablette à un autre agent du Département sans en avoir informé la hiérarchie et la DSI ;
- Prêter à un tiers (ex : famille, amis…) son smartphone ou sa tablette ;
- Utiliser un schéma (= dessin qui consiste à relier des points) comme option de déverrouillage sur son smartphone ou sa tablette ;
- Utiliser la carte SIM professionnelle dans un appareil n'appartenant pas à la flotte mobile du Département. En cas de besoin particulier la DSI peut étudier et fournir une solution adaptée.

Pour en savoir plus sur l'utilisation des smartphones et des tablettes, consulter le site SharePoint « Aide en Ligne ».

L'utilisation de matériels USB (clé, Smartphone, disque dur, appareil photo…) appelle à la plus grande vigilance (ex : ne pas brancher une clef USB d'origine inconnue). En effet, elle peut être une cause importante de contamination virale ou de perte de données.

L'utilisateur doit passer au contrôle de l'antivirus tous les supports amovibles strictement nécessaires à sa mission (clé USB – CD/DVD – disque dur externe…) (Cf procédure dans YATOO / site SharePoint « Aide en Ligne »).

5.3 - UTILISATION DES EQUIPEMENTS PERSONNELS SUR LE RESEAU INTERNE DU DEPARTEMENT

Il n'est pas autorisé de connecter un matériel personnel sur le Système d'Information interne de la Collectivité sans en avoir l'autorisation formelle du RSSI.

En cas de besoin particulier, et afin de limiter des risques, contacter le RSSI pour étudier les mesures à mettre en place.

5.4 - INTERNET : REGLES D'UTILISATION ET NAVIGATION SECURISEE

5.4.1 - REGLES D'UTILISATION D'INTERNET

Un accès internet est mis à disposition de chaque utilisateur du Système d'Information du Département.

Les utilisateurs doivent être informés que la plupart des sites internet conservent des traces des accès effectués. Ces sites identifient précisément l'identité numérique* du visiteur, ainsi que celle du Département.

En conséquence, les règles ci-dessous doivent strictement être respectées par l'utilisateur :

L'utilisateur doit

- Demander l'autorisation préalable à sa hiérarchie pour toute publication à caractère professionnel sur un site internet, un blog, un forum, un réseau social ;
- Demander l'autorisation à sa hiérarchie pour tout abonnement payant à un site Web ;
- Avoir l'autorisation de sa direction pour apporter sa contribution sur le site institutionnel charente-maritime.fr et effectuer une demande de création de compte de contribution auprès du service web à la DCSII ;

L'utilisateur ne doit pas

- Communiquer son compte de contribution au site institutionnel à un tiers (collègue, stagiaire, apprenti, ou prestataire) ;
- Naviguer sur des sites ou s'exprimer sur des réseaux sociaux, des blogs, des forums portant atteinte à la dignité humaine (pédophile - pornographique, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine, à la violence à l'égard d'une personne ou d'un groupe de personnes en raison de leur origine ou de leur appartenance ou non à une ethnie, une race ou une religion déterminée) ;
- Télécharger et exploiter, tout ou partie, des données numériques soumises aux droits d'auteurs ou à la loi des copyrights sans autorisation et sans mention des crédits en cas de publication :
- S'exprimer sur les blogs, forums ou les réseaux sociaux au nom de la collectivité sans habilitation. Les pages Twitter et Facebook du Département sont gérées par la Direction de la Communication, des Stratégies Innovantes et de l'International ;
- Créer des sites web personnels en utilisant les ressources informatiques* du Département ;
- Publier des informations à caractère personnel sans déclaration préalable au Délégué à la Protection des Données (DPD) de la Collectivité.

La Direction des Systèmes d'Information peut bloquer à tout moment et sans avertissement préalable l'accès aux sites dont le contenu est illégal, offensant ou perturbant le fonctionnement normal du Système d'Information.

En cas de nécessité de service, l'utilisateur peut demander à rendre accessible un site (demande SerenIT).

5.4.2 - NAVIGATION SECURISEE SUR INTERNET

L'utilisateur doit vérifier :

- Si la navigation sur le site est sécurisée :
    - Présence du sigle « HTTPS » au début de l'URL sur la barre d'adresse du navigateur ;
    - Présence d'un cadenas vert et/ou fermé à gauche de l'URL de la barre d'adresse du navigateur.

- L'URL des liens avant de cliquer dessus : en passant la souris sur un lien sans cliquer dessus, l'URL de ce lien apparait en bas de page du navigateur et permet de vérifier la page sur laquelle l'utilisateur sera redirigé ;

Il est recommandé dès que possible, de repasser par un moteur de recherche connu (ex : Google) pour se connecter à un service en ligne.

Pour en savoir plus, visionner l'épisode de la mini-série saison 2 « C'est pas sorcier de surfer en tout sécurité » ou consulter le site SharePoint « Aide en Ligne ».

5.5 - UTILISATION DE LA MESSAGERIE ELECTRONIQUE PROFESSIONNELLE

5.5.1 - PRINCIPES DE RESPONSABILITE ET DE CONFIDENTIALITE

Tout utilisateur de la collectivité dispose d'une boîte aux lettres professionnelle attribuée personnellement lors de sa prise de fonction.

Chaque utilisateur est responsable de l'utilisation de sa boîte aux lettres.

Tout courrier électronique engageant la collectivité doit respecter les règles formelles de validation en vigueur.

L'utilisateur se doit de respecter les principes de politesse et de respect lorsqu'il échange par mail (cf. Le site SharePoint "Aide en Ligne").

L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

Le saviez-vous ?
Les serveurs présents sur la planète entière (et qui servent en partie à stocker vos emails) consomment en moyenne 200 000 milliards de Watt/heure chaque année dans le monde. C'est presque la moitié de la consommation annuelle de la France !

Cependant la messagerie professionnelle n'est pas un lieu de stockage des documents. L'utilisateur doit régulièrement procéder à la suppression des messages n'étant pas nécessaires au suivi d'un dossier (ex : mails d'informations, demandes de rendez-vous…).

Pour les messages nécessaires au suivi d'un dossier et devant être conservés, se rapprocher de la fiche outils accessible depuis YATOO et sur le site SharePoint « Aide en Ligne ».

Tout mail envoyé à une adresse mail extérieure au Département comportant des données présentant un risque pour la vie privée des personnes ou pour la collectivité, doit être protégé par le biais du chiffrement proposé dans la messagerie. *Pour en savoir plus sur le fonctionnement du chiffrement des messages, se référer au tutoriel « Chiffrer les messages » disponible sur le site Sharepoint « Aide en Ligne » du Département.*

Il est également de la responsabilité de chaque utilisateur de signaler tout mail douteux selon les dispositions prévues au point 7.3 de cette Charte Utilisateur.

Les règles d'utilisation à titre privé de la messagerie sont quant à elles détaillées dans la partie 5.8 de la présente Charte.

5.5.2 - Utilisation des boîtes fonctionnelles

Une adresse électronique fonctionnelle, à usage strictement professionnel, peut être mise en place, pour un utilisateur ou un groupe d'utilisateurs pour les besoins du Département (Boîte aux lettres générique).

Pour créer une boîte fonctionnelle, l'utilisateur doit se référer au tutoriel disponible sur le site SharePoint « Aide en Ligne » du Département.

Le gestionnaire et les personnes habilitées à accéder à cette boîte sont responsables de son utilisation.

Pour des raisons de continuité de service, il est préconisé de diffuser l'adresse générique (liée à la mission) plutôt que celle d'un utilisateur.

5.5.3 - Utilisation et gestion des listes de diffusion*

Les directions métier sont autonomes pour créer leur liste de diffusion sous validation de la DSI.

Pour créer une liste de diffusion, l'utilisateur doit se référer au tutoriel disponible sur le site SharePoint « Aide en Ligne » du Département.

Celle-ci est gérée et mise à jour par le responsable métier défini par la direction à l'origine de la demande.

La liste de diffusion LD-CG-AGENTS doit être utilisée **uniquement à des fins professionnelles**. Toute autre forme de communication (don d'animaux, place de cinéma, de concert, billet de train, prosélytisme religieux ou politique…) est strictement interdite.

Pour éviter la fonction « répondre à tous », **il est obligatoire d'utiliser le champ CCI (copie cachée) de la messagerie lors de l'utilisation de la liste de diffusion LD-CG-AGENTS.**

5.5.4 - Envoi de mails multiples

Le saviez-vous ?

Un envoi d'un email avec une pièce jointe de 1 Mo envoyé à 10 personnes consomme l'équivalent en énergie d'une ampoule (économique) restée allumée pendant 6 à 7 heures !

En cas d'envoi à plusieurs personnes dont au moins 1 destinataire est externe à la collectivité, il est recommandé d'utiliser le champ CCI (copie cachée).

Le champ CCI permet de respecter la vie privée de vos contacts (diffusion non voulue des adresses e-mail).

Par exemple, si tous les noms des destinataires sont affichés, A va récupérer l'adresse de B alors que B ne le souhaitait pas. Ou pire, si D est un spammeur, il recevra toutes les adresses de vos contacts, et n'hésitera pas à s'en resservir.

En résumé, cela permet de respecter l'anonymat de ses correspondants et d'éviter d'exposer une partie de son carnet d'adresses aux malwares (virus, spams, chaînes de mails, ...).

La messagerie n'est pas l'outil préconisé par le Département pour l'envoi de documents/pièce-jointes à un grand nombre de destinataires (plus particulièrement en interne). Pour cela, se référer au point 5.6.4 de la présente Charte.

5.6 - UTILISATION DES OUTILS COLLABORATIFS

Le Département met à disposition - au travers de la suite Microsoft 365 - toutes les fonctionnalités des outils collaboratifs prévus à cet effet, dont les règles d'usages sont décrites dans les points suivants de la présente Charte.

L'utilisateur n'est pas autorisé à déposer des documents et/ou informations sur un outil de messagerie ou collaboratif autres que ceux installés et validés par la DSI (exemples d'outils non-autorisés par défaut : dropbox, gmail, googledrive, wetransfer, zoom …).

L'utilisateur est autorisé à utiliser ces outils dans le cas de la récupération d'un document transmis par un tiers (ex : prestataire, sous-traitant, bureau d'étude…)

5.6.1 – LA VISIOCONFERENCE – LES REUNIONS TEAMS

Un agent du Département n'est pas autorisé à réaliser un enregistrement vidéo et/ou audio d'une réunion Teams sans avoir le consentement éclairé de l'ensemble des participants à cette réunion.

Lors du déclenchement de l'enregistrement, il doit indiquer les finalités de cet enregistrement, sa durée de conservation et demander aux personnes leur accord.

Toute réunion ou conversation dans laquelle il serait échangées des informations personnelles relatives à la situation d'un usager, d'un bénéficiaire ou d'un agent, ne pourra pas être enregistrée sauf cas exceptionnels.

Pour en savoir plus sur l'enregistrement de ces réunions, se référer au site SharePoint « Aide en Ligne » partie « Outils Collaboratifs ».

5.6.2 - LA MESSAGERIE INSTANTANEE PROFESSIONNELLE – LES CONVERSATIONS TEAMS

L'utilisation de la messagerie instantanée professionnelle est destinée aux échanges informels et en temps réel ne nécessitant pas la conservation d'une trace écrite pérenne des échanges réalisés. Pour conserver une trace écrite d'un échange, il est conseillé d'utiliser la messagerie professionnelle classique (cf. 5.5 de la Charte).

Afin d'éviter la multiplication des documents de travail, la messagerie instantanée professionnelle n'est pas l'outil préconisé par le Département pour échanger des documents.

L'utilisateur n'est pas autorisé à installer des applications dans Teams sauf s'il a obtenu la validation de la DSI.

Recommandations d'usage :

- L'utilisateur doit gérer son statut de connexion (ex : « ne pas déranger », « en réunion » : ces statuts permettent d'informer l'ensemble des agents et éviter ainsi la sur-sollicitation).
- L'utilisateur doit respecter le statut des autres utilisateurs de cet outil (exemple : si le statut d'un utilisateur est en rouge sur « ne pas déranger » ou « en réunion »).

Pour en savoir plus sur la gestion des statuts, se référer au site SharePoint « Aide en Ligne » partie « Outils Collaboratifs ».

5.6.3 - UN ESPACE DE STOCKAGE INDIVIDUEL ET DE PARTAGE UNITAIRE - ONEDRIVE

L'outil collaboratif OneDrive est désigné comme un espace de stockage individuel et de partage unitaire de documents.

L'utilisateur est informé que OneDrive est l'outil préconisé pour le partage de documents volumineux (en interne et vers l'externe).

Lors d'un partage de documents vers l'externe, l'utilisateur doit vérifier qu'il a mis en place toutes les mesures de sécurité nécessaires (mot de passe, date d'expiration…) avant le partage de ces documents.

Chaque utilisateur est invité à vérifier régulièrement les personnes et/ou listes de personnes ayant accès aux documents présents sur son espace OneDrive.

Des règles spécifiques s'appliquent sur cet outil lors du départ d'un agent de la collectivité (cf 5.10 de la présente Charte).

5.6.4 - CREATION D'ESPACES COLLABORATIFS (SHAREPOINT) ET CREATION D'EQUIPES (TEAMS)

Une équipe Teams est principalement destinée à la gestion d'un projet et au travail collaboratif au sein d'un service qui s'appuiera sur l'agrégation de plusieurs briques logicielles (conversation et réunion de groupe via le client Teams, coédition de fichiers grâce à SharePoint, échanges d'idées avec Whiteboard, partage de tâches via ToDo, etc.).

La création d'un espace (ou site) SharePoint est principalement destinée au dépôt de documents de travail collaboratifs. Il s'agit de l'outil préconisé pour le partage d'un grand nombre de fichiers à destination de plusieurs personnes.

La création des espaces collaboratifs (SharePoint) et des équipes (Teams) est sous la responsabilité unique de la DSI. Toute demande est réalisée par la création d'un ticket SerenIT.

L'utilisation et les habilitations de ces espaces et équipes relèvent exclusivement de la responsabilité du gestionnaire de site ou du propriétaire d'équipe au sein des directions métier.
La DSI ne sera pas tenue responsable des habilitations trop permissives.

Le propriétaire d'une équipe Teams doit :

- Pour la gestion d'un projet :
  - Gérer les listes de personnes ayant un accès aux documents, aux informations et aux différents canaux de discussions de l'équipe ;
  - Suivre ces accès de façon continue (ex : suppression des permission obsolètes…). Une revue d'habilitation lui sera adressée de façon régulière ;
  - Récupérer en fin de projet les documents produits et utilisés durant le projet et les stocker dans un espace pérenne (ex : un site SharePoint du Service). Une équipe Teams n'a pas vocation à conserver des documents d'un projet à la fin de celui-ci ;
  - Assurer la continuité de service en cas de départ (cf. 5.10 « Départ de la collectivité » de la présente Charte.) ;
  - Demander la suppression de l'équipe Teams à la DSI une fois le projet terminé et les données récupérées.

- Pour le travail collaboratif au sein d'un service :
  - Eviter la multiplication des documents au sein d'un service. L'utilisateur doit privilégier le dépôt de documents sur un site SharePoint (ex : site du Service de l'agent), puis partager un lien vers ce dépôt.

Un gestionnaire de site SharePoint doit :
- Gérer les listes de personnes ayant un accès aux documents déposés sur le site ;
- Suivre ces accès de façon continue (ex : suppression des permission obsolètes…). Une revue d'habilitation lui sera adressée de façon régulière ;
- Assurer la continuité de service en cas de départ (cf. 5.10 « Départ de la collectivité » de la présente Charte.) ;
- Vérifier le sort final des données stockées dans un site avant sa suppression.

Pour en savoir plus sur l'ensemble des règles d'utilisation de ces outils, l'agent est invité à se rapprocher de son Référent Informatique ou du site SharePoint « Aide en ligne » du Département partie « Outils Collaboratifs ».

5.7 - GESTION DU CYCLE DE VIE DES DOCUMENTS ET DES DONNEES

Le cycle de vie du document/ des données correspond aux différentes étapes de l'existence de dossiers, de documents ou de données, depuis la production de l'information (création ou réception) jusqu'à son élimination ou sa conservation définitive.

5.7.1 – CREATION D'UN DOCUMENT : NOMMAGE, CLASSEMENT ET GESTION DES ACCES

Lors de la création d'un document, l'utilisateur doit :

- Nommer son fichier de façon à ce qu'il soit facilement identifiable (cf. « Fiche conseil plan de nommage » disponible sur YATOO)
- Gérer les accès à son document en décidant de l'endroit où le document sera enregistré en vérifiant les points suivants :
    - qui va avoir besoin d'accéder au document (consultation)
    - qui va intervenir sur le document (modification…)
- Vérifier que le document peut être facilement retrouvé par les utilisateurs concernés
    - Un document doit être classé au bon endroit et être associé à la bonne métadonnée*, afin d'être facilement accessible à toute personne habilitée.

Pour en savoir plus, se référer à la fiche pratique « Plan de classement » disponible sur YATOO.

5.7.2 - ARCHIVAGE OU SUPPRESSION DES DONNEES

La conservation de données des usagers ou des agents est soumise à des obligations légales qui imposent une suppression visée et contrôlée par les Archives départementales ou un archivage de celles-ci dans les délais prévus par la loi ou par les règles d'archivage (cf. Législation sur les archives publiques et RGPD).

L'agent doit appliquer les durées légales de conservation des données des administrés qu'il est amené à traiter (cf.tableau de gestion des archives « Yatoo- Outils métiers – Guides d'archivage/TG dans Yatoo). Il doit également respecter les procédures en vigueur au Département relatives à l'archivage (cf. bordereau de versement) ou à la suppression des données (cf. bordereau d'élimination contrôlé et visé par le Directeur des Archives départementales)

Lorsque les données ne sont pas soumises à une obligation de versement aux archives départementales, l'agent s'engage à les supprimer dès lors qu'elles ne sont plus utiles dans le cadre du traitement, qu'elles soient sous une forme numérique ou papier en respectant strictement les procédures en vigueur au Département (Bordereau d'élimination visé par les Archives départementales et la direction métier).

Lorsque des documents isolés contenant des informations personnelles sur des usagers ou des agents doivent être détruits (imprimés par erreur et/ou en double), l'agent s'engage à utiliser les moyens et les procédures du Département prévus pour une destruction sécurisée (notamment par l'utilisation des broyeurs de proximité et/ou poubelles sécurisées pour les documents contenant des données sensibles ou perçues comme sensibles).

5.8 - UTILISATION A TITRE PRIVE DES OUTILS PROFESSIONNELS

L'utilisation à titre privé des outils professionnels mis à disposition par le Département est tolérée si modérée*, loyale, non lucrative et conforme aux lois et aux règles du Département sous réserve que cela ne nuise pas à la performance du Département et à l'accomplissement des missions de service public. Les règles du Département – suivant les outils utilisés – sont les suivantes :

Messagerie :

- L'utilisateur ne doit pas utiliser son adresse professionnelle pour s'inscrire sur des listes de diffusion ou des réseaux non liés à son activité professionnelle ;
- Il doit distinguer l'usage professionnel et l'usage privé par la création de profils distincts dans le cas des sites nécessitant une inscription en ligne.
- Il est interdit d'utiliser le carnet d'adresses du Département pour passer des annonces privées.
- Lors de l'envoi d'un mail à titre privé, l'utilisateur devra veiller à supprimer toute mention relative au Département de la Charente-Maritime (notamment en n'apposant pas sa signature professionnelle) et toute information qui pourrait laisser suggérer que le message est rédigé dans le cadre de ses fonctions.

- **Pour être reconnu comme privé, tout message devra contenir a minima 1 des 2 points ci-dessous :**
    - Avoir la mention « PRIVE » en 1er dans son objet ;
    - Etre classé dans un répertoire nommé PRIVE (et non au nom de l'utilisateur) (cf. la fiche pratique dans Yatoo ou le site SharePoint « Aide en ligne ») ;
    - **En l'absence de ces précautions, le message sera considéré comme professionnel.**
- Concernant la messagerie professionnelle instantanée : il n'est techniquement pas possible d'identifier un message comme étant privé dans l'outil de messagerie instantanée professionnelle Teams. Il est donc préconisé d'utiliser cet outil à des fins strictement professionnelles ;

Stockage sur le matériel professionnel et l'espace individuel OneDrive :

Dans le cadre d'une utilisation privée, chaque utilisateur doit conserver ses informations privées dans un dossier nommé PRIVE. Aucune donnée professionnelle ne devra être stockée dans un répertoire PRIVE.

Conformément à la loi en vigueur, le simple fait de classer les documents dans un espace nommé « mes documents » ou identifié par des initiales de l'utilisateur ne constitue pas un dossier privé et son contenu sera traité comme professionnel.

Utilisation de la téléphonie :

Le Département met à disposition des utilisateurs des ressources informatiques et téléphoniques ainsi que des moyens de télécommunication pour assumer leurs missions professionnelles.

L'usage à titre personnel de ces outils est elle aussi tolérée. Cependant l'utilisateur doit particulièrement faire attention à ne pas saturer la mémoire du téléphone portable avec des applications personnelles (La mémoire disponible sur un téléphone portable est largement inférieure à celle disponible sur un ordinateur).

5.9 - REGLES SPECIFIQUES AU NOMADISME NUMERIQUE

Par outil nomade (ou mobile), on entend tout support numérique permettant de travailler en dehors de son bureau (ordinateur portable, Smartphone…).

Ces matériels sont mis à disposition par la DSI pour répondre aux missions de l'utilisateur, mais leur utilisation est de la responsabilité de l'utilisateur habilité *(cf. guide de bonnes pratiques des outils mobiles).*

5.9.1 – SPECIFICITE DU TELETRAVAIL

Le télétravail est un statut spécifique du nomadisme numérique et suit un protocole particulier. Afin d'appréhender l'ensemble des règles liées au télétravail, l'utilisateur doit se référer au Protocole sur le dispositif pour le télétravail des agents départementaux disponible sur YATOO.

5.9.2 - UTILISATION DES EQUIPEMENTS PROFESSIONNELS EN SITUATION DE NOMADISME

Un utilisateur en situation de nomadisme numérique et en possession de matériel informatique professionnel doit uniquement utiliser ce matériel pour l'exercice de ses fonctions.

L'ensemble du matériel professionnel fourni par la Collectivité est nativement chiffré ce qui permet d'améliorer la sécurité des données qu'il contient.

5.9.3 - UTILISATION DES EQUIPEMENTS PERSONNELS EN SITUATION DE NOMADISME

L'utilisateur n'est pas autorisé à utiliser des équipements personnels pour accéder à des outils professionnels (ex : messagerie professionnelle). En cas de besoin particulier, le RSSI doit obligatoirement être sollicité.

En cas de non-respect de cette interdiction, l'utilisateur engage sa responsabilité qui pourra entraîner des sanctions disciplinaires le cas échéant.

Cette interdiction ne concerne pas les assistants familiaux. Dans le cadre de cette exception, le Département ne saurait être tenu responsable en cas de dommage survenu sur un équipement privé dans le cadre d'une utilisation professionnelle.

Il est de la responsabilité de l'assistant familial de mettre en place les dispositifs de sécurité de base sur son équipement privé *(par exemple, antivirus à jour sur le micro-ordinateur privé)* et de respecter les consignes de sécurité mises en œuvre par le Département.

5.9.4 - SECURITE DES CONNEXIONS EN SITUATION DE NOMADISME

Pour toute utilisation d'une application métier non disponible directement depuis internet, l'utilisateur doit obligatoirement se connecter au SI du Département via l'utilisation d'un VPN afin d'établir une connexion sécurisée.

Un VPN ne peut être installé que sur du matériel professionnel fourni par la DSI.

Afin de sécuriser l'utilisation d'un VPN, un utilisateur doit obligatoirement utiliser une Authentification Multi-Facteur (ou MFA)*.

Pour en savoir sur les procédures liées à la demande d'un VPN, cf. site SharePoint « Aide en Ligne ».

5.9.5 - PROTECTION DES DONNEES EN SITUATION DE NOMADISME

- Pour limiter le risque de vol : Éviter de laisser le matériel professionnel visible (véhicule, locaux ouverts sans surveillance…) ;
- Ne pas confier le matériel professionnel à un tiers (famille – amis …) ;
- Pour limiter le risque d'accès illicite à des données confidentielles :
    - Eviter de travailler sur des données confidentielles dans les lieux publics (train, avion, séminaire, hall d'hôtel…)
    - Éviter d'échanger des données confidentielles sur un réseau WIFI public (Le Département ne maîtrisant pas la sécurité de ces réseaux) ou par SMS ;
    - Penser à verrouiller les sessions de votre matériel nomade (Appuyer simultanément sur les touches du clavier  +L).

5.10 – ABSENCE TEMPORAIRE ET DEPART DE LA COLLECTIVITE

Messagerie :

En l'absence de l'utilisateur et afin d'assurer la continuité de service, le directeur de l'agent peut être amené à accéder aux courriers professionnels arrivés ou stockés dans la messagerie de l'agent dans le respect d'une procédure formelle validée par la Direction Générale des Services.

Afin de traiter tous les cas d'absence, 3 procédures ont été mises en place (cf dans Yatoo) :

1. Absence planifiée (vacances, formations, congé parental, missions…) ;
2. Absence non planifiée (arrêt maladie, accident…) ;
3. Départ d'un utilisateur de la collectivité (fin de contrat, départ en retraite, démission, décès …).

Dans le cas où l'utilisateur quitte la collectivité (départ à la retraite, mutation, démission, ...) il doit procéder avant son départ à la suppression de tous les mails privés qui sont dans sa boite de messagerie. En aucun cas, l'utilisateur ne doit détruire les mails ou les données professionnelles nécessitant le suivi d'un dossier et devant être conservés.

Pour assurer la continuité des services après son départ, l'utilisateur devra informer les usagers avec qui il est en relation, de l'identité de son remplaçant et remettre à son chef de service ou son remplaçant les mails professionnels en sa possession.

L'utilisateur est informé que des procédures spécifiques relatives à l'accès aux mails professionnels après son départ (planifié ou non planifié) sont prévues par la Direction Générale des Services afin de permettre la continuité du service public dans le respect du secret de correspondance et de la vie privée.

Outils collaboratifs :

OneDrive :

Lorsqu'un agent quitte la collectivité, l'intégralité de son espace OneDrive est mise à disposition de son supérieur hiérarchique N+1 pendant une durée de 30 jours, puis à l'issue de ce délai, cet espace sera automatiquement supprimé.

Par conséquent, l'agent doit veiller à supprimer de cet espace tous les documents qu'il aurait stockés dans un répertoire « Privé » ou « Personnel ». En cas d'oubli de l'agent, l'espace privé sera mis à disposition du supérieur hiérarchique.

SharePoint / Teams :

Avant son départ, un gestionnaire d'un site collaboratif SharePoint et/ou propriétaire d'une équipe Teams doit transmettre ses droits à une autre personne du service rattaché au site collaboratif et/ou à l'équipe Teams. (*se référer à la procédure disponible sur le site SharePoint « Aide en Ligne » du Département*).

Avant son départ de la collectivité, chaque utilisateur du SI doit suivre les règles suivantes :

- ne pas détruire de données professionnelles en dehors des dispositions prévues au point 5.7.2 de la présente Charte ;
- mettre en ordre et classer ses dossiers
- prendre attache auprès du « référent archives » du service pour débuter l'archivage des dossier/données en lien avec les Archives départementales
- ramener à la DSI l'ensemble de son matériel professionnel nomade (smartphones, tablettes, supports amovibles…) ;
- remettre au service Développement du Numérique la clef de signature électronique attribuée s'il en possède une. Celle-ci sera révoquée à l'issue de son départ ;

6 - PROTECTION DES DOCUMENTS ET DES DOSSIERS PAPIERS

Chaque agent s'engage à ranger les documents et les dossiers sensibles notamment ceux des usagers dans des espaces protégés (armoires ou bureau fermés à clés…) dès qu'il est absent afin que des personnes non habilitées *(collègues autres services, usagers, prestataires, intervenants externes…)* ne puissent y accéder.

Les documents et dossiers des usagers ne doivent pas sortir des locaux du Département à moins que cela ne soit strictement nécessaire à la mission *(ex : visites à domicile, réunions à l'extérieur…)* et validé par la hiérarchie. En situation de mobilité, l'utilisateur doit privilégier les outils numériques et/ou collaboratifs.

Lorsque l'agent est amené à emporter des documents contenant des informations sur des usagers, il s'engage à prendre toutes les mesures nécessaires pour éviter qu'ils ne soient perdus ou volés (ne pas laisser les documents sans surveillance, dans sa voiture, ne pas autoriser la lecture des documents par des personnes non habilitées, …).

Cette disposition ne s'applique pas dans le cadre du télétravail qui interdit la sortie des dossiers papiers contenant des données à caractère personnel.

Enfin, l'agent veille à ne pas laisser des documents contenant des informations sensibles notamment ceux contenant des données à caractère personnel sur les copieurs multifonctions ou dans des espaces de réunions ou d'accès au public.

7 - DEVOIRS D'ALERTE ET DE REMONTEE D'INCIDENTS

7.1 - ALERTE EN CAS D'INCIDENT SUR LES DONNEES DES USAGERS ET DES AGENTS

Pour rappel, une violation de données personnelles est avérée dès que l'agent constate que les fichiers ou les documents (papiers ou numériques) contenant des informations sur des usagers ou des agents sont consultés illicitement, corrompus ou perdus *(détruits, volés ou perdus)*.

L'agent s'engage à alerter sans délai sa hiérarchie et la DPD du Département à l'adresse suivante : **violation.donnees@charente-maritime.fr**

Dès que la DPD aura pris connaissance de l'incident, une analyse avec l'agent et sa hiérarchie permettra de notifier la violation à la CNIL le cas échéant et informer les personnes concernées en cas d'impact important sur leur vie privée (cf procédures « Protection des Données » disponibles sur le site « DG – Protections des DCP et du SI »).

Pour rappel, voici quelques exemples de violation de données les plus courantes :

- Le piratage des systèmes d'informations (cf.7.2)
- Des données transmises à un mauvais destinataire (erreur de mail ou de courrier)
- Un équipement perdu ou volé (clé usb – smartphone – pc portable – tablette – dossiers papier – mallette …)
- Publication involontaire de données sur internet
- Impressions laissées par erreur sur un photocopieur
- Dépôt des documents dans un espace bureauti ou Sharepoint dans un espace où des agents non habilités peuvent accéder aux données

7.2 - ALERTE EN CAS D'EVENEMENT DOUTEUX / INCIDENT DE SECURITE

Chaque agent du Département est un acteur de la sécurité du Système d'Information de la collectivité. En ce sens, chaque utilisateur se doit de signaler selon la procédure en vigueur :

- Toute anomalie ou dysfonctionnement de son poste de travail ;
- Tout accès à une information ou à une ressource qui ne correspond pas à ses missions *(notamment lors des changements de missions) via un ticket SerenIT.*
- La perte ou le vol du matériel mis à disposition (dans les locaux ou en dehors des locaux) via un ticket SerenIT;
- Toute suspicion d'accès non autorisé à des données ou des informations professionnelles ;
- Signaler les mails douteux (tentative d'hameçonnage) qu'il reçoit. Ex : liens suspicieux vers des sites non connus, orthographe décousue dans un mail… *(écrire à l'adresse cybersecurite@charente-maritime.fr);*
- Signaler chaque suspicion de cyberattaque. Ex : Fichiers illisibles/extensions de fichiers étranges (.encrypted .ccc .crypt), poste informatique bloqué, affichage à l'écran d'un message en anglais… (se référer à la fiche réflexe « en cas de cyberattaque »).

8 - LES TRACES ET LES CONTROLES DE LA BONNE UTILISATION DU SYSTEME D'INFORMATION

Dans le respect des principes de transparence et de proportionnalité et à des fins de sécurité, et de protection des intérêts de la collectivité, le Département est en droit d'analyser, de limiter et de contrôler l'utilisation du Système d'Information.

Ces contrôles sont réalisés dans le respect :

- De la législation applicable, notamment la règlementation relative aux Données à Caractère Personnel ;
- Du droit à la vie privée de l'utilisateur et du secret des correspondances ;
- Des règles et procédures internes applicables en matière de sécurité.

Le Département peut mettre en place des systèmes de filtrage et de contrôle pour contrôler tout accès aux applications, tout message électronique entrant ou sortant (contrôle antiviral, contrôle anti-spam, contrôle de la taille, liste des destinataires, …) et également pour bloquer, les messages, échanges informatiques ou les accès à des sites non autorisés.

Ces systèmes enregistrent les différentes traces d'activité, à des fins de sécurité.

Les dispositifs de sécurité informatique du Département permettent, conformément à la réglementation en vigueur, une conservation, pendant une durée limitée et proportionnée à la finalité, des informations suivantes :

- La liste des services auxquels l'utilisateur a eu accès sur l'internet ;
- La liste des accès/connexion ou tentative d'accès/connexion aux applications du Système d'Information (identification du compte, date, heure, liste des comptes habilités à accéder aux ressources et historique de celle-ci, …) ;

L'utilisateur ne devra en aucun cas empêcher ou gêner le fonctionnement normal de ces moyens de traçabilité et de contrôle.

Ces dispositifs sont nécessaires pour :

- La protection des agents dans le cas où une levée de doute est nécessaire concernant un usage illicite par un tiers ;
- La protection des intérêts du Département de la Charente-Maritime auxquels sont attachés un caractère de confidentialité ainsi que la lutte contre les pratiques contraires ;
- La prévention et la répression de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui, ainsi que la répression de ces faits ;
- La sécurité et/ou le bon fonctionnement technique des systèmes informatiques ainsi que la protection physique des installations ;
- La maintenance corrective, curative ou évolutive ;
- Le respect de la bonne foi des principes et règles d'utilisation des ressources des systèmes d'information, tels que définis par la présente charte ;

- La réalisation de statistiques.

Au sein de la collectivité, Il y a 2 types de contrôle :

8.1 - CONTROLE COLLECTIF :

À des fins statistiques, ce contrôle anonyme et non individualisé ne vise pas le contenu des informations consultées mais uniquement les flux des sites Internet consultés, la fréquence, le volume des courriers de la messagerie.

8.2 - CONTROLE INDIVIDUALISE :

En cas de doute sur le respect des bonnes pratiques lors d'un échange par messagerie ou sur un fichier noté privé, seul le Directeur général des services peut mandater un contrôle. L'utilisateur en est toujours informé au préalable et peut demander, avant le contrôle, à être assisté d'un représentant syndical ou de toute autre personne de son choix.

Les résultats obtenus lors du contrôle sont transmis exclusivement au Directeur Général des Services.

Ce dernier prendra les décisions qui s'imposent au regard de ces résultats notamment pour répondre aux requêtes des autorités judiciaires ou pour engager des sanctions adaptées aux circonstances.

Le contrôle individualisé concernant la sphère privée peut se faire sans prévenir l'utilisateur dans le cas où ce dernier ne peut être joint et si le Département se trouve dans une situation d'exceptionnelle gravité. L'utilisateur sera informé dès que possible.

Les fichiers de journalisation des connexions Internet sont conservés 1 an.

8.3 – CONTROLE ET GESTION DES TIERS UTILISATEURS

Un tiers (consultant, sous-traitant, ...) qui souhaite se connecter au réseau du Département doit préalablement signer un contrat avec la direction métier concernée en lien formalisé avec la DSI.

Ce contrat inclut des clauses définissant les termes et conditions d'un tel accès.

Il est de la responsabilité des Directions métier de s'assurer que le contrat est signé et respecté.

9 - INFORMATION DES UTILISATEURS SUR LA GESTION DU SYSTEME D'INFORMATION

Le Système d'Information du Département et ses ressources sont administrés par la Direction des Systèmes d'Information (DSI).

La DSI, le RSSI et la DPD peuvent conseiller et assister tout utilisateur qui le souhaite, en cas de difficultés d'application de la présente charte.

9.1 - LES BONNES PRATIQUES DU RESPONSABLE FONCTIONNEL*(RF) DU RESPONSABLE D'APPLICATION* (RA) ET DE L'ADMINISTRATEUR TECHNIQUE (AT)

- Le Responsable Fonctionnel administre l'application et assure le suivi des incidents « fonctionnels » ;

- Le Responsable d'Application veille au bon fonctionnement des applications de son portefeuille applicatif ;
- L'Administrateur Technique veille au bon fonctionnement et à la sécurité des réseaux, postes de travail, des serveurs.

De par leurs missions et leurs droits étendus, ils peuvent techniquement avoir accès à l'ensemble des données informatiques produites par les utilisateurs.

Ils sont tenus au secret professionnel particulier lié à leur fonction et au devoir de remontée d'incident.

Ils doivent informer immédiatement le Responsable de la Sécurité des Systèmes d'Information (RSSI) et le Délégué à la Protection des Données (DPD) de toute tentative d'intrusion ou d'attaque sur le Système d'Information ou de tout comportement délictuel ou non conforme aux règles de la présente charte.

L'administrateur technique ne peut en aucun cas réaliser un contrôle sur un mail ou fichier notifié privé de sa propre initiative. Seul le DGS peut diligenter ce type de contrôle.

9.2 - UTILISATION DES LOGICIELS DE PRISE DE MAIN A DISTANCE INTERNE

Ces outils permettent d'accéder à distance sur un poste de travail connecté au réseau du Département.

Cette prise de main ne peut se faire qu'après accord de l'utilisateur qui devra rester présent devant son ordinateur tout le temps de la connexion.

Pendant toute la durée de la prise de main, un message reste affiché sur l'écran de l'utilisateur.

Dès que la prise de main est interrompue, le message disparaît indiquant à l'utilisateur la fin du contrôle à distance.

Seuls les personnels habilités de la DSI, les administrateurs techniques, les Responsables Fonctionnels Métier et les Référents Informatiques au sein des directions sont habilités à utiliser ces outils.

10 - ENTREE EN VIGUEUR

La présente charte remplace la version précédente éditée en 2018.

Elle a fait l'objet d'un avis favorable en Comité Technique (CT) en date du 6/12/2021

Elle a fait l'objet d'une approbation par la Commission Permanente en date du 14/01/2022 et de ce fait est opposable à l'ensemble des utilisateurs du Système d'Information de la collectivité à partir du 17/01/2022.

Elle est diffusée à l'ensemble des utilisateurs de la collectivité.

Elle est consultable sur YATOO et sur SharePoint sur le site DG protection DCP-SI.

Elle pourra être modifiée en particulier pour prendre en compte les évolutions des politiques de sécurité, de la réglementation et des progrès technologiques.

L'utilisateur s'engage à prendre connaissance et à appliquer l'ensemble des dispositions de la présente charte.

Elle est systématiquement remise à tout nouvel arrivant dans le livret d'accueil.

Les principales dispositions légales applicables sont consultables sur YATOO.

11 - SANCTIONS

L'usurpation d'identité ou la tentative d'usurpation d'identité, en vue d'accéder aux ressources informatiques*, est passible de sanctions.

Tout utilisateur ne respectant pas les règles et obligations définies dans cette charte est passible de sanctions disciplinaires ou contractuelles et s'expose selon la gravité des infractions à des poursuites pénales ou civiles conformément aux dispositions légales en vigueur.

12 - DEFINITIONS

A

Authentification : consiste à vérifier que l'entité correspond à l'identité qui cherche à se connecter, c'est-à-dire le lien entre l'identité et la preuve de l'identité.
La forme d'authentification la plus répandue est celle de l'identifiant/mot de passe.

Authentification Multi-Facteur : authentification faisant intervenir au moins deux facteurs. Généralement le premier facteur repose sur quelque chose que l'utilisateur sait (le mot de passe), et le second facteur repose sur quelque chose que l'utilisateur possède (carte à puce, téléphone portable...). Plus le nombre de facteurs est élevé, plus l'authentification est considérée comme fiable.

Administrateur technique : toute personne à laquelle est confiée la responsabilité de serveurs informatique, bases de données, réseaux, équipements de téléphonie, d'applications,..). Cet agent possède des droits étendus et par conséquent pourra être amené à avoir accès aux informations des autres utilisateurs (confidentielles ou non)

Administrateur système *: Agent de la DSI en charge des serveurs, des bases de données et de leur sécurité*

Administrateur réseau *: Agent de la DSI en charge des réseaux et des infrastructures réseaux et téléphoniques et de leur sécurité*

C

Commission d'Homologation de la Protection de l'Information et des Données à Caractère Personnel (2017) : Présidée par le Directeur Général des Services, elle homologue le système d'information, notamment pour tout système appelé téléservice (possibilité donnée par l'administration aux usagers d'effectuer des démarches en lignes : demande de subvention, abonnement en ligne…) et valide les risques résiduels pour tous les traitements de données à caractère personnel présentant un risque pour la vie privée des usagers et des agents.

Elle atteste aux utilisateurs que le système d'information du Département est protégé conformément aux objectifs de sécurité fixés.

Consentement de la personne concernée : Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement

CNIL : Commission Nationale Informatique et Libertés – Autorité de contrôle nationale pour toute les questions relevant de la protection des données à caractère personnel.

D

Donnée à caractère personnel (DCP) : information qui permet d'identifier de manière directe ou indirecte une personne physique : Un nom, une photographie, un matricule, le numéro de sécurité sociale, un RIB, un enregistrement audio ou vidéo…

Délégué à la Protection des données Personnelles (DPD/DPO) : agent du Département, désigné par la Présidente du Département de la Charente-Maritime, il est le « Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme. Ses principales missions sont **d'informer et de conseiller** le responsable de traitement ou le sous-traitant, ainsi que leurs employés ; **de contrôler le respect du règlement** et du droit national en matière de protection des données ; **de conseiller l'organisme** sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ; **de coopérer avec l'autorité de contrôle** et d'être le point de contact de celle-ci

Durée d'utilité courante (DUC) : « base active » : cette étape concerne l'utilisation courante des données personnelles par les services chargés de la mise en œuvre de leur traitement. Concrètement, cela correspond aux dossiers utilisés quotidiennement par les métiers. Les données sont accessibles, dans l'environnement de travail immédiat, par tous ceux qui sont en charge du traitement des affaires courantes.

Durée d'utilité administrative (DUA) : Durée légale ou pratique pendant laquelle un document est susceptible d'être utilisé par le service producteur ou son successeur, au terme de laquelle est appliquée la décision concernant son traitement final (élimination ou conservation à des fins historiques). Le document ne peut être détruit pendant cette période qui constitue sa durée minimale de conservation. C'est l'archivage intermédiaire : les données personnelles ne sont plus utilisées pour atteindre l'objectif fixé (« dossiers clos ») mais présentent encore un intérêt administratif pour l'organisme (par exemple : gestion d'un éventuel contentieux, etc.) ou doivent être conservées pour répondre à une obligation légale (par exemple : les données de facturation doivent être conservées dix ans en application du code de commerce, même si la personne concernée n'est plus cliente). Les données peuvent alors être consultées de manière ponctuelle et motivée par des personnes spécifiquement habilitées.

F

Fichier de Données à Caractère Personnel : Tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ;

I

Identité numérique : Ensemble des informations que l'on trouve sur internet concernant un individu. Cette identité se compose à mesure que la personne surfe et communique avec des ressources et des individus sur le Web, laissant ainsi diverses traces plus ou moins visibles, profondes, et indélébiles.

H

Habilitation : L'utilisateur authentifié n'est pas systématiquement autorisé à accéder à une ressource, il doit y être habilité.
Un administrateur détermine celui qui a le droit ou non à utiliser une ressource.

L

Liste de diffusion : Liste regroupant plusieurs contacts qui permet à l'expéditeur d'envoyer un mail à tous les destinataires de la liste.

Métadonnée : Donnée servant à définir ou à décrire une autre donnée quelque soit son support (date de création – durée de conservation – thématique – classification selon la sensibilité …)

	Nomadisme Numérique : Le nomadisme numérique désigne toute forme d'utilisation des technologies de l'information permettant à un utilisateur d'accéder au SI de son entité d'appartenance ou d'emploi, depuis des lieux distants, ces lieux n'étant pas maîtrisés par l'entité. (source ANSSI)
P	**Patrimoine informationnel** : Ensemble des informations propriété du Département ou qui lui sont confiées quel que soit le support (oral, papier, numérique) permettant à la collectivité de réaliser ses missions
R	**Relais Informatique et Libertés (RIL) (création en 2015) :** doit s'assurer que l'ensemble des traitements dont il a la responsabilité est conforme et porté au registre de la DPD. C'est le directeur métier qui assume cette mission. **Réseau social** : s'applique en particulier au domaine de l'Internet. Il désigne alors un site web qui, dans un domaine quelconque, fédère des individus et facilite leurs échanges d'informations, d'images… **Responsable d'application** (RA): Agent (DSI, DCSII ou SG/OCE) en charge du maintien en condition opérationnelle des applications (MAJ applications, correctifs, évolution, suivi des bases de données…) appartenant à son portefeuille applicatif. Il travaille en étroite collaboration avec le Responsable Fonctionnel. **Responsable Fonctionnel (RF)**: Agent appartenant à la Direction Métier référente/application. Il a en charge l'administration fonctionnelle de l'application. Il accède à l'ensemble des données (confidentielles ou non) et les gère au travers de l'application (pas d'accès direct aux serveurs et aux bases de données). Il travaille en étroite collaboration avec le responsable d'application. **Responsable de la Sécurité des Systèmes d'Information (RSSI) :** Placé sous la responsabilité du Directeur des Systèmes d'Information (DSI), le RSSI veille à la mise en œuvre de la sécurité des systèmes d'information conformément à la réglementation en vigueur. A ce titre, il définit, anime et coordonne l'ensemble des tâches de maîtrise d'œuvre de la sécurité du système d'information. **Ressources informatiques :** Ensembles de moyens informatiques matériels et logiciels mis à disposition d'un utilisateur pour accomplir ses missions : Poste de *travail : Micro-ordinateurs et leurs périphériques (scanner, imprimantes, téléphones…) ; Serveurs ; Outils de mobilité : Tout matériel numérique permettant de travailler en dehors de son bureau :(PC portables, tablettes, smartphones, GPS, appareil photo …) ; Applications métiers (IODAS, ASTRE, GFD, AUTOCAD …) ; Systèmes d'exploitation et logiciels bureautiques (Word, Excel, PowerPoint…) ; Réseaux informatiques* …
S	**Système d'information** : Ensemble de ressources matérielles, logicielles, procédurales, organisationnelles et humaines visant à acquérir, gérer, structurer, stocker, diffuser des informations ou des données sous des formes diverses. **Support amovible** : mémoire de masse conçue pour être connectées et utilisée sans avoir besoin de redémarrer l'ordinateur (Clé USB, Disque dur externe, appareil photo, tablettes, smartphone, Carte mémoire pour tablette, Cigarette électronique, …)

T	**<u>Technologies de l'Information et de la Communication (TIC)</u> :** Moyens d'échanges d'informations et de communications (web, messagerie, etc.) mis à disposition par le Département à partir de serveurs locaux ou à distance constituant les services internet. **<u>Traitement de données à caractère personnel</u>** : Toute opération ou ensemble d'opérations effectuée(s) ou non à l'aide de procédés automatisés, et appliquée(s) à des données à caractère personnel, telle(s) que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que la limitation du traitement, l'effacement ou la destruction ; Tableau de gestion (ou guide d'archivage) : Tableau recensant les documents et les données produits par un service, reflétant son organisation et servant à gérer ses archives courantes et intermédiaires et à procéder à l'archivage de ses archives historiques. Il fixe pour chaque type de documents le délai d'utilité administrative* , délai de versement au service d'archives compétent pour les recevoir, traitement final et modalités de tri à lui appliquer. Ce tableau est réglementaire car il est signé par le directeur du service et le directeur des Archives départementales.
U	**<u>Utilisateur du système d'information</u> :** Toute personne quel que soit son statut *(agent permanent, agent temporaire, stagiaire, apprenti),* autorisée à accéder aux outils informatiques et aux moyens de télécommunication et à les utiliser pour assurer sa mission. **<u>Usage modéré à titre privé</u>** : est l'utilisation ne gênant pas les ressources professionnelles et n'affectant pas les missions confiées à l'agent
V	**<u>Violation de données à caractère personnel</u>** : Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »
W	**<u>WIFI public</u> :** En déplacement, pouvoir connecter son ordinateur, son smartphone ou sa tablette sur un réseau WIFI gratuit est très pratique d'autant que l'on en trouve de plus en plus (aéroport, bus, restaurant, hôtel, magasin, bar…). Néanmoins, par définition ces zones d'accès sans fil ouvertes ne sont pas du tout sécurisées et représentent un risque important pour toutes les informations envoyées voir même pour l'ordinateur ou la tablette utilisée.