Covaldem 11

Collecte et Valorisation
des Déchets Ménagers de l'Aude

Charte informatique

Utilisation des moyens de communication et des systèmes informatiques

Révision n°2

Avis du comité technique en date du 28/11/2022

Délibération n° 2022_41 du 12/12/2022

REÇU EN PREFECTURE
le 15/12/2022
Application agréée E-legalite.com
09_DE-011-200036101-20221212-CS2022_41-D

Table des matières

Préambule 3
Définitions 3
Champ d'application 5
Personnes visées par la présente charte 5
Règles générales d'utilisation 5
Droits et devoirs des utilisateurs 5
Droits et devoirs de la Collectivité 6
Sanctions 6
Évolution 7
Opposabilité de la présente charte 7
~~Les postes informatiques~~ Moyens informatiques et de communication électronique concernés 7
Sécurité 8
Utilisation des Systèmes d'Information et des outils de communication 8
Accès 8
La messagerie électronique : 9
Internet 10
Les médias sociaux 10
La téléphonie 11
~~Service dans le nuage~~ Le cloud 12
Le travail à distance 12
~~Musique et vidéo en ligne~~ 12
Contrôle – Traçabilité – Conservation 13
Références réglementaires et législatives 13
Obligations de transparence et de concertations 13
Les textes législatifs 14
Le droit disciplinaire 14
Le code pénal 15
La réglementation européenne 15

REÇU EN PREFECTURE
le 15/12/2022
Application agréée E-legalite.com
99_DE-011-200036101-20221212-CS2022_41-D

Préambule

Le Covaldem11 met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique, ainsi que des équipements informatiques fixes et mobiles.

Les agents, dans l'exercice de leurs fonctions, sont conduits à accéder et à utiliser lesdits équipements informatiques, ainsi que les systèmes d'information et de communication mis à leur disposition.

L'utilisation du système d'information et de communication doit être effectuée exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte.

Par ailleurs, des tiers au Covaldem11 (élus, prestataires…) peuvent également avoir accès aux équipements informatiques et aux systèmes d'information et de communication du Covaldem11.

Or, l'utilisation d'équipements informatiques (matériels et logiciels), de réseaux de communication et du système d'information fait peser un risque pour le Covaldem11 concernant le fonctionnement, la sécurité et l'intégrité de son système d'information et de communication, mais également concernant les données (à caractère personnel ou non, sensibles ou non) qui sont traitées dans le cadre de l'activité du Covaldem11.

Aussi, dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information et des équipements informatiques, la présente charte pose les règles relatives à l'utilisation de ces ressources.

Cette charte a pour objectifs :

- De sensibiliser les utilisateurs aux risques liés à la sécurité informatique en matière de libertés et de vie privée, notamment à travers les traitements de données à caractère personnel qu'ils peuvent être amenés à effectuer ;
- D'informer les utilisateurs sur :
  - Les usages permis des moyens informatiques mis à leurs dispositions ;
  - Les règles de sécurité en vigueur ;
  - Les mesures de contrôle prises par le Covaldem11 ;
  - Les sanctions éventuellement encourues par les utilisateurs ;
- De formaliser les règles générales de sécurité que les utilisateurs s'engagent à respecter, en contrepartie de la mise à disposition des systèmes d'information et des équipements informatiques, et ainsi de déterminer les droits et devoirs des utilisateurs.

Ces règles s'inscrivent dans une démarche responsable afin de protéger d'une part le patrimoine informationnel et l'image de marque de la collectivité, et d'autre part les libertés et la vie privée des personnes concernées que sont les agents du Covaldem11 et les tiers en lien avec les Covaldem11 (élus, prestataires…).

Le Systèmes d'Information (SI) ou le Responsable du pôle Finances Informatique (RFI), la Direction Générale (DG) et le délégué à la protection des données personnelles (DPO - Data Protection Officer) se tiennent à la disposition des utilisateurs qui souhaiteraient disposer d'informations ou de conseils complémentaires relatifs à l'usage des systèmes d'information et des équipements informatiques.

Définitions

REÇU EN PREFECTURE
le 15/12/2022
Application agréée E-legalite.com
038_DE-011-200039181-20221212-022022_41-0

- **Collectivité** : La personne morale Covaldem11 qui fournit les ressources informatiques, téléphoniques, informationnelles, numériques et technologiques et les met à disposition du personnel.

- **Système d'Information** : Ensemble de tous les éléments qui contribuent au traitement et à la circulation de l'information dans la collectivité (base de données, logiciels d'application, procédures…) et du système informatique (serveur, périphériques, imprimantes, copieurs multifonction, système d'exploitation…).

- **Utilisateurs** : les personnes utilisant le Système d'information ~~de la collectivité~~ du Covaldem11.

- ~~**Poste de travail**~~ **Equipements informatiques**: Ensemble des équipements matériels, logiciels et services mis à la disposition des Utilisateurs pour leur permettre d'assurer leurs missions et d'accéder aux moyens de communication électronique.

- **Moyens de communication électronique** : Outils et services mis à la disposition des utilisateurs du Système d'Information pour communiquer. Il s'agit des outils et services de messagerie électronique, des outils et services d'accès aux réseaux informatiques internes et externes, des outils et services de téléphonie.

- **Règlement Général sur la Protection des Données (RGPD)** : encadre le traitement des données personnelles sur le territoire de l'Union européenne.

- **Data Protection Officer (DPO)** : Personne désignée par le Président de la collectivité, qui a pour mission de veiller à la bonne application au sein de la collectivité de la loi européenne du 25 mai 2018 relative au RGPD.

- **Responsable informatique (RSI)** : Désigne la personne en charge de l'organisation et du management des outils et services informatiques et numériques, support du Système d'Information de la collectivité. Il est le garant du maintien en condition opérationnelle du Système d'Information.

- **Responsable de la Sécurité du Système d'Information** : Désigne la personne en charge de l'organisation et du management de la sécurité du Système d'Information.

REÇU EN PREFECTURE
le 15/12/2022
Application agréée E-legalite.com
93_DE-011-200036101-20221212-052022_41-D

Champ d'application

Personnes visées par la présente charte

Les dispositions de la présente charte s'appliquent à toute personne autorisée à accéder aux ressources informatiques, informationnelles, numériques et technologiques et à utiliser les moyens de communication électronique du Covaldem11 :

- Les agents et les élus
- Les stagiaires
- Les intérimaires
- Les intervenants extérieurs, prestataires
- Les visiteurs occasionnels

Règles générales d'utilisation

Les agents doivent adopter un comportement responsable s'interdisant par exemple toute tentative d'accès à des données ou à des sites qui leur seraient interdits.

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques, ainsi que du contenu de ce qu'il affiche, télécharge ou envoie et s'engage à ne pas effectuer d'opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement du réseau informatique de la collectivité. Il doit en permanence garder à l'esprit que c'est sous le nom de la collectivité qu'il se présente sur Internet et doit se porter garant de l'image de l'institution.

Au même titre que pour le courrier ou le téléphone, chacun est responsable des messages envoyés ou reçus, et doit utiliser la messagerie dans le respect de la hiérarchie, des missions et fonctions qui lui sont dévolues et des règles élémentaires de courtoisie et de bienséance.

Du fait du traitement de données personnelles, le Covaldem11 s'engage, dans le cadre des dispositions légales et réglementaires qui s'imposent à lui et dans le respect du principe édicté par le RGPD, à mettre en œuvre toutes les mesures organisationnelles et techniques utiles afin de préserver la sécurité, l'intégrité et la confidentialité des données, ainsi que la sécurité de son système d'information et de communication, sur le plan technologique et procédural, afin notamment d'empêcher toute modification, tout transfert et toute suppression non-autorisés des données, et toute intrusion non-autorisée dans son système d'information ou son endommagement.

Toutefois, le premier risque reste le risque humain lié aux traitements et aux manipulations des données par les utilisateurs, et par l'utilisation par ces derniers du système d'information et de communication et des outils qui y sont liés.

Par conséquent, la mise en place d'outils de sécurité ne doit pas dispenser les utilisateurs de signaler toute tentative d'intrusion extérieure, de falsification ou de présence de virus au RSI.

Tout utilisateur a la charge, à son niveau, de contribuer à la sécurité des moyens mis à sa disposition et du réseau auquel il a accès, principalement en évitant l'intrusion de virus susceptibles d'endommager le Système d'Information de la collectivité.

Droits et devoirs des utilisateurs

Toute personne ~~(agent ou élu)~~ travaillant dans la collectivité, dispose d'un droit d'accès au Système d'Information.

REÇU EN PREFECTURE
le 15/12/2022
Application agréée E-legalite.com
99_DE-111-200036101-20221212-092022_41-0

Ce droit est strictement personnel et incessible.

Les ressources informatiques mises à disposition constituent un outil de travail nécessaire.

Chaque utilisateur doit adopter une attitude responsable et respecter les règles définies sur l'utilisation des ressources, notamment :

- Respecter l'intégrité et la confidentialité des données.
- Ne pas perturber la disponibilité du système d'information
- Ne pas stocker ou transmettre d'information portant atteinte à la dignité humaine ou vie privée
- Ne pas marquer les données exploitées d'annotations pouvant porter atteinte à la dignité humaine ou vie privée
- Respecter les droits de propriété intellectuelle
- Ne pas introduire de ressources extérieures matérielles et/ou logicielles qui pourraient porter atteinte à la sécurité
- Respecter les contraintes liées à la maintenance du système d'information
- Ne pas masquer son identité ou usurper celle d'un autre

L'usage de ces outils de communication ne modifie en rien les obligations de validation et d'information vis-à-vis de la hiérarchie. La continuité du service étant une priorité, l'utilisateur s'interdit, cependant, d'appliquer des mesures de sécurité non validées par la Direction Générale et qui auraient pour conséquence de rendre inaccessibles des informations intéressant le bon fonctionnement de la collectivité.

Les droits d'accès peuvent être modifiés ou retirés à tout moment, selon les besoins du service et prennent fin lors de la cessation de l'activité professionnelle.

Droits et devoirs de la Collectivité

La collectivité doit veiller à la disponibilité et à l'intégrité du système d'information.

En ce sens, elle s'engage à :

- Mettre à disposition les ressources informatiques matérielles et logicielles nécessaires aux missions des utilisateurs
- Mettre en place des programmes de formations adaptés et nécessaires aux utilisateurs
- Informer les utilisateurs des diverses contraintes d'exploitation du système
- Effectuer les mises à jour nécessaires des matériels et des logiciels composant le système
- Respecter la confidentialité des « données utilisateurs » auxquelles elle pourrait être amenée à accéder
- Définir les règles d'usage de son système et veiller à leur application

Sanctions

La loi, les textes réglementaires et la présente charte informatique définissent les droits et obligations des personnes utilisant les ressources informatiques. Tout utilisateur du système d'information de la collectivité n'ayant pas respecté la loi pourra être poursuivi pénalement.

En cas de non-respect des règles définies par la présente charte, le Président de la Collectivité pourra par mesure conservatoire, sans préjudice des poursuites civiles ou pénales et des procédures disciplinaires pouvant être engagées à l'encontre de l'utilisateur, prendre toute mesure utile à la

REÇU EN PREFECTURE
le 15/12/2022
Application agréée E-legalite.com
99_DE-011-200035101-20221212-CS2022_41-0

préservation de ses intérêts et des intérêts des personnels, usagers, partenaires publics et privés, ou tiers, notamment :

- Limiter les usages du système d'information
- Interdire tout accès au système d'information de la collectivité
- Procéder à toute mesure d'investigation sur les ressources informatiques matérielles et immatérielles mises à disposition par la collectivité ainsi que dans les échanges avec l'extérieur

La collectivité est également tenue par la loi de signaler aux services concernés compétents toute violation des lois constatée.

Toute infraction aux règles internes décrites dans le document peut entraîner des sanctions disciplinaires.

Évolution

Avant son entrée en vigueur, la présente charte a été soumise à l'avis du Comité Technique ~~Paritaire~~ en date du 28/11/2022.
Elle pourra être complétée ou modifiée par l'autorité territoriale, l'avis du Comité Technique Paritaire sera à nouveau demandé.

Opposabilité de la présente charte

La présente charte est portée à la connaissance des utilisateurs par tous moyens jugés adéquats par le Covaldem11.
Constitue notamment un moyen adéquat et suffisant l'un des moyens suivants : mise à disposition dans I:\Infos pour Tous, annexe signée aux conventions de stage pour les stagiaires externes, transmission individuelle via la messagerie électronique pour les utilisateurs.

~~Les postes informatiques~~ Moyens informatiques et de communication électronique concernés

~~Cette présente partie a pour objectif d'établir les règles d'utilisation des postes.~~

~~Un ensemble « matériel – système d'exploitation – logiciels » est mis à disposition de chaque utilisateur :~~

- ~~MATÉRIEL : Unité centrale, écran, clavier, souris, …~~
- ~~SYSTEME d'EXPLOITATION : Windows (Seven, 8, 10)~~
- ~~LOGICIELS : Pack bureautique (Office), logiciels de communication, logiciels de gestion, applications spécifiques, …~~

La présente charte concerne l'ensemble des moyens informatiques et de communication électronique qui sont mis à la disposition des utilisateurs à des fins professionnelles exclusivement.

Les systèmes d'information et de communication du Covaldem11 sont notamment constitués des éléments suivants :

- Ordinateurs portables ou fixes

REÇU EN PREFECTURE
le 15/12/2022
Application agréée E-legalite.com
99_DE-011-200036101-20221212-CC2022_41-0

- Périphériques (écran, clavier, souris, clés USB)
- Réseaux informatiques (serveurs, routeurs, connecteurs, bornes WIFI)
- Copieurs multifonctions
- Téléphones (fixes, portables et smartphones)
- Tablettes
- Logiciels
- Fichiers informatiques et bases de données
- Espaces de stockage individuel
- Messagerie
- Connexions internet

Les matériels et logiciels sont mis à disposition par le ~~Responsable informatique~~ RSI en fonction des besoins et impératifs des missions. Ils demeurent la propriété de la collectivité. L'utilisateur est et demeure responsable des matériels et logiciels qui lui sont confiés, il doit en prendre soin. Ils sont restitués selon les procédures en vigueur en cas de mobilité interne ou avant le départ définitif.

Les espaces de stockage (disques locaux, disques partagés, boîte de messagerie, espaces collaboratifs, etc.) auront préalablement été sauvegardés, transmis à la hiérarchie. Pour les données à caractère privé, elles auront été supprimées.

Le matériel est fragile, il faut en prendre soin. Les supports amovibles (clé USB, ~~cd rom,~~ disque dur externe…) provenant de l'extérieur doivent être soumis à un contrôle antivirus préalable.

Sécurité

Tout téléchargement ou toute installation logicielle est à la charge de la personne compétente désignée par l'autorité territoriale et totalement proscrit pour le reste des utilisateurs.

L'utilisateur est tenu de n'utiliser de périphérique de stockage externe qu'avec extrême précaution et prudence et après s'être assuré que le support est exempt de virus.

En cas d'absence du bureau, l'utilisateur doit VERROUILLER son poste informatique à l'aide de la combinaison :

puis cliquer sur « Verrouiller l'ordinateur » (ou à l'aide de la combinaison de touches

). A la fin de la journée de travail le poste informatique doit être impérativement éteint dans sa totalité.

L'utilisateur doit signaler tout dysfonctionnement ou anomalie au service ou référent informatique selon la procédure définie par la collectivité.

Utilisation des Systèmes d'Information et des outils de communication

Accès

REÇU EN PREFECTURE
le 15/12/2022
Application agréée E-legalite.com
93_DE-011-200036101-20221212-052022_41-D

L'accès à certains éléments du système d'information (comme la messagerie électronique, les sessions sur les postes de travail ou certaines applications) est protégé par des paramètres de connexion (identifiant, mot de passe). Chaque utilisateur reçoit un droit d'accès individuel.

Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'accès des utilisateurs. Ils ne doivent être communiqués à personne, ni responsable hiérarchique, ni informatique. Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles.

Lorsqu'ils sont choisis par l'utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement. Des consignes de sécurité sont élaborées par le RSI.

L'utilisateur s'engage à respecter les considérations d'efficacité d'un mot de passe, laquelle dépend du nombre de caractères alphanumériques (un minimum de 8 caractères contenant au moins 1 majuscule, 1 minuscule, 1 chiffre et 1 caractère spécial), de son originalité, de son renouvellement régulier par l'utilisateur (tous les 6 mois). Un logiciel « coffre-fort » de mot de passe (KeePass) est installé sur l'ensemble des ordinateurs des utilisateurs permettant de disposer de mots de passe sécurisés et différents pour chacun des accès dont il dispose. Il convient de sauvegarder cette base de données dans le lecteur P:\, étant personnel à chacun.

Chaque utilisateur doit s'identifier personnellement et ne peut utiliser l'identité d'autrui.

Ce droit d'accès cesse automatiquement lors d'un départ (l'utilisateur quittant la collectivité) et peut être modifié lors d'un changement d'affectation (changement de poste) ou s'il est constaté que l'utilisateur a enfreint l'une des obligations imposées par la présente charte.

La messagerie électronique :

~~Cette présente partie a pour objectif d'établir les règles d'utilisation de la messagerie électronique.~~

L'utilisation de la messagerie est réservée à des fins professionnelles. Néanmoins il est toléré en dehors des heures de travail un usage modéré de celle-ci pour des besoins personnels et ponctuels.

L'utilisateur est tenu de consulter sa messagerie électronique au moins une fois par jour, hors période d'absence. Il doit accorder la même importance aux messages électroniques qu'aux courriers postaux et se doit de les traiter.

L'utilisateur veillera à ne pas ouvrir les messages électroniques dont la provenance ou le sujet paraissent suspects.

Tout courrier électronique est réputé professionnel et est donc susceptible d'être ouvert par l'autorité territoriale ou le référent informatique (sur demande de l'autorité territoriale). Les courriers à caractère privé et personnel doivent expressément porter la mention « personnel » ou « privé » dans leur objet ou alors se situer dans un dossier de classification portant le nom « personnel » ou « privé ». Ces derniers ne pourront être ouverts que par l'autorité territoriale sur des raisons exceptionnelles de manquement avéré à la loi ou de droit à des tiers.

L'utilisateur soigne la qualité des informations envoyées à l'extérieur et s'engage à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et image de chacun.

Chaque courrier électronique sera signé automatiquement par le serveur de messagerie, et contiendra les informations relatives à l'expéditeur (nom, fonction, numéro de téléphone).

REÇU EN PREFECTURE
le 15/12/2022
Application agréée E-legalite.com
99_DE-011-200030191-20221212-052022_41-0

L'utilisateur doit éviter de surcharger le réseau d'informations inutiles. Les messages importants sont à conserver et/ou archiver, les autres à supprimer. Le dossier « Éléments supprimés » doit être vidé périodiquement.

En cas d'absence prévisible, l'utilisateur devra mettre en place un message automatique d'absence indiquant sa date de retour prévue. Il peut exister la possibilité qu'un agent gère les messages pendant l'absence de l'utilisateur.

La signature électronique est présumée fiable jusqu'à preuve du contraire. Son utilisation est limitée aux personnes autorisées et doit respecter la procédure définie par la collectivité.

Une équivalence juridique est établie entre le courrier électronique et le courrier sur support papier. Ils doivent, en conséquence être traités dans les mêmes délais.

Seront considérés comme fautifs ou abusifs les comportements suivants :

- L'échange de messages à caractère xénophobe, raciste, négationniste, pornographique, contribuant à un harcèlement sexuel ou moral, de menaces ou d'insultes et, plus généralement, tout message contraire à la réglementation en vigueur et aux bonnes mœurs.
- L'échange d'informations confidentielles au mépris des dispositions internes relatives à la confidentialité des échanges et du secret professionnel.
- La redirection de sa messagerie vers une messagerie externe à la collectivité.

Internet

~~Cette présente partie a pour objectif d'établir les règles d'utilisation d'internet depuis un accès filaire ou en wifi.~~

L'utilisation d'Internet est réservée à des fins professionnelles et/ou syndicales dans le cadre de l'exercice des décharges d'activité et autorisations spéciales d'absence.

Néanmoins il est toléré en dehors des heures de travail un usage modéré de l'accès à Internet et l'utilisation des services de messageries instantanées de type « chat » (skype, messenger~~, icq,~~ …) pour des besoins personnels à condition que la navigation n'entrave pas l'accès professionnel. L'utilisateur s'engage lors de sa navigation à ne pas se rendre sur des sites illégaux ou contraires à la bienséance.

Le téléchargement de tout ou partie de données numériques soumises aux droits d'auteurs ou à la loi du copyright est strictement INTERDIT. De plus le stockage sur le réseau de données à caractère non professionnel téléchargées sur Internet est interdit.

Tout abonnement payant à un site web ou à un service via Internet doit faire l'objet d'une autorisation préalable de l'autorité territoriale.

Pour éviter les abus, l'autorité territoriale peut procéder, à tout moment, au contrôle des connexions entrantes ou sortantes et des sites les plus visités.

Les médias sociaux

Les plateformes de média sociaux incluent les blogs, wikis, communautés internet, forums de discussion, sites de partage de vidéos et applications de réseaux (Facebook, Twitter, Linkedin, Youtube, TikTok, Instagram,...), que ce soit via un ordinateur un smartphone ou une tablette. Compte tenu de l'évolution des offres, cette liste n'est pas exhaustive.

REÇU EN PREFECTURE
le 15/12/2022
Application agréée E-legalite.com
99_DE-011-200030101-20221212-052022_41-D

Il est rappelé à l'utilisateur, qu'à moins d'y être formellement autorisé, il est interdit de publier sur les plateformes de média sociaux toute forme d'information au nom ou faisant référence au Covaldem11.

Dans tous les cas, les quatre grands principes qui s'appliquent à l'utilisation des médias sociaux sont :

- Être responsable
- Respecter la confidentialité
- Être transparent
- Respecter l'auditoire.

Dans le cadre de l'utilisation des médias sociaux, et compte tenu des répercussions que celle-ci peut avoir sur le Covaldem11, il appartient à tous les utilisateurs de ne pas se revendiquer comme appartenant au personnel du Covaldem11 ou comme agissant pour le compte du Covaldem11. L'utilisation des médias sociaux devra également répondre à certaines obligations de sorte qu'il ne soit pas porté atteinte aux intérêts et à la réputation tant du Covaldem11 que de ses collaborateurs, tout en veillant au respect de la liberté d'expression de chacun.

Une utilisation inappropriée des médias sociaux peut en effet entraîner des atteintes à votre vie privée et à celle des autres collaborateurs du Covaldem11, et des dommages à la réputation du Covaldem11 et de ses collaborateurs.

Toute création de blog, de compte Facebook / Twitter de profil Linkedin / Viadéo ou toute contribution aux médias en ligne (Wikipédia, forum internet, mailing list, etc…) à titre personnel, par toute personne utilisant des Ressources Informatiques peut en effet avoir un impact sur le Covaldem11.

Dans ce cadre général, et indépendamment des utilisations spécifiques décrites ci-après, chacun des utilisateurs se doit de respecter les règles élémentaires d'utilisation des médias sociaux suivantes :

- N'oubliez pas que ce que vous mettez en ligne restera. Chacun se doit donc de préserver la réputation du Covaldem11 ainsi que celles de ses collaborateurs.

- Veillez au respect de la vie privée des autres. Ne révélez aucune information personnelle les concernant sans avoir obtenu au préalable leur consentement express.

Il s'agit ici d'alerter les utilisateurs sur le fait qu'ils ne peuvent abuser de leur liberté d'expression quel que soit le sujet, dans les productions/commentaires qu'ils seraient susceptibles de publier sur les médias sociaux/collaboratifs utilisés à titre privé et qui pourraient entacher la réputation du Covaldem11. Exemple : *commentaire sur une page personnelle facebook d'un utilisateur portant préjudice à un autre utilisateur au sujet de son comportement par exemple.*

Dans le cadre de l'utilisation des médias sociaux, il est donc expressément indiqué aux utilisateurs qu'ils doivent éviter les dérives suivantes dans les commentaires qu'ils pourraient faire :

- L'atteinte à la vie privée
- La diffamation et l'injure
- Le dénigrement
- La divulgation à des tiers d'informations confidentielles
- L'incitation à la consommation de substances interdites
- La provocation aux discriminations de toute sorte, aux harcèlements de toute sorte ayant notamment trait à la race, la religion, l'appartenance politique et syndicale, la nationalité, le sexe ; le handicap, ou l'âge, la provocation aux crimes et délits et au suicide.

La téléphonie

~~Cette présente partie a pour objectif d'établir les règles d'utilisation du téléphone.~~

REÇU EN PREFECTURE
le 15/12/2022
Application agréée E-legalite.com
99_DE-011-200060011-20221212-052022_41-0

L'utilisation des téléphones fixes et mobiles est réservée à des fins professionnelles. Néanmoins un usage personnel ponctuel est toléré à condition que cela n'entrave pas l'activité professionnelle.

L'utilisation des téléphones portables personnels doit rester occasionnelle et discrète. L'accès internet par le réseau Wifi de la Collectivité n'est pas autorisé pour les téléphones personnels.

L'autorité territoriale peut procéder au contrôle de l'ensemble des appels émis.

Un agent ou élu qui quitte définitivement la collectivité doit restituer le téléphone portable professionnel.

L'utilisateur doit veiller à soigner sa présentation lors d'un appel pour faciliter son identification et/ou son service.

Par défaut, les communications depuis ou vers l'étranger sont interdites. Il en va de même pour l'utilisation des réseaux de données ~~(3G/4G)~~ (4G/5G) depuis l'étranger.

~~Service dans le nuage~~ Le cloud

~~L'informatique dans le nuage~~ Le cloud est un concept qui consiste à déporter sur des serveurs distants des stockages et des traitements informatiques traditionnellement localisés sur des serveurs locaux ou sur le poste de l'utilisateur.

Les services dans le cloud portent le risque pour la collectivité de la perte de souveraineté, et de la perte du contrôle sur les données qu'elle produit.

Il en résulte que l'utilisateur connecté aux ressources internes de la collectivité n'est pas autorisé à utiliser ces types de services en dehors de ceux explicitement validés par le RSI. Dans ce cadre, l'utilisateur doit veiller à la pertinence des contenus et des destinataires.

Le transfert de fichiers à caractère professionnel vers ces services est soumis aux mêmes règles que les copies de données sur supports externes.

Le travail à distance

Le présent article concerne l'utilisation des systèmes d'information du Covaldem11, de ses ressources, et des moyens de communication par l'utilisateur lorsque celui-ci est situé en-dehors du site physique du Covaldem11.

En premier lieu, il convient de préciser que l'ensemble des dispositions de la présente charte sont applicables aux utilisateurs accédant aux systèmes d'information et de communication de la Collectivité à distance.

Par ailleurs, il est impératif que l'utilisateur informe préalablement le RSI, après avoir eu l'accord de sa hiérarchie, afin que lui soit communiqué les accès nécessaires ainsi que les consignes de sécurité et de confidentialité propres à sa situation.

Tout accès à distance par du matériel informatique personnel est interdit sauf l'accès à Webmail.

Musique ~~et vidéo~~ en ligne

~~L'accès à ces médias en temps réel est un service qui nécessite des ressources de communication conséquentes et risque d'encombrer, d'engorger et de ralentir les accès aux réseaux.~~

~~Il en résulte que l'Utilisateur n'est pas autorisé à utiliser ces modes de communication en dehors de la stricte nécessité de ses fonctions au sein de la Collectivité.~~

L'usage de musique en ligne, notamment, est toléré avec modération et respect d'autrui, et ne doit en aucun cas nuire au bon fonctionnement du service et de la collectivité.

REÇU EN PREFECTURE
Le 15/12/2022
Application agréée E-legalite.com
99_DE-011-200053101-20221212-C52022_41-D

Contrôle – Traçabilité – Conservation

Dans le respect des principes de transparence et de proportionnalité, à des fins de sécurité et de vérification du bon accès et usage des moyens de communication électronique, ainsi que du bon fonctionnement du Système d'Information, des systèmes de filtrage, de contrôle et des dispositifs d'enregistrement des traces d'activités des systèmes peuvent être mis en place par le RSI. Le fonctionnement des systèmes de contrôle, de filtrage et d'enregistrement de trace des activités des systèmes est assuré par le Responsable de la Sécurité du Système d'Information.

Les systèmes de contrôle peuvent être mis en œuvre pour contrôler les messages entrants et sortants et également pour bloquer, notamment sur la base d'une liste de mots clefs, de types de fichiers joints ou de tailles des messages, les échanges informatiques.

Les systèmes de filtrage peuvent être mis en œuvre pour contrôler les flux de communication Internet et également pour bloquer, notamment sur la base de listes de catégories et de mots clefs, l'accès aux contenus externes au réseau du Covaldem11.

Les systèmes de restriction d'usage peuvent être mise en œuvre pour limiter ou interdire certains services accessibles depuis les téléphones fixes et mobiles pour ceux qui en sont dotés.

L'utilisateur est informé que les traces suivantes peuvent être conservées :

- Liste des contenus ou services auxquels l'Utilisateur a eu accès sur le réseau Internet
- Date et heure des connexions ou tentatives de connexion de l'utilisateur sur les systèmes d'accès aux moyens de communication électronique
- Liste des paramètres techniques de gestion des services de messagerie électronique (identification du compte Utilisateur, coordonnées du destinataire, date et heure, etc.)
- Liste des traces de connexion aux applications et aux ressources informatiques

Les traces, messages et documents pourront être conservés pour une durée maximale d'un an, sous réserve du respect des dispositions légales et réglementaires applicables au titre de la prescription.

A des fins statistiques relatives aux connexions et aux contacts réalisés, des contrôles portant sur la volumétrie des connexions à des sites Internet ou de l'utilisation de la messagerie pourront être réalisés par le RSI.

L'Utilisateur est informé que des contrôles individualisés pourront être diligentés par le Responsable de la Sécurité du Système d'Information, sur ordre du Président de la Collectivité, suite à un dysfonctionnement du Système d'Information, d'une alerte de sécurité et également en cas de suspicion d'un usage non conforme des moyens de communication électronique, sous réserve du respect des dispositions applicables au secret des correspondances privées.

Références réglementaires et législatives

Obligations de transparence et de concertations

REÇU EN PREFECTURE
le 15/12/2022
Application agréée E-legalite.com
99_DE-011-200036191-20221212-CS2022_41-D

Décret de 1982 régissant les obligations de consulter le CTP.

Vu le code général de la fonction publique,

Art. L 432-2 du code du travail prévoyant la consultation obligatoire du CTP lorsque l'employeur projette d'introduire dans l'entreprise des moyens qui rendent possible la surveillance des salariés.

Art. L 412-8 du code du travail modifié par l'article 45 de la loi relative à la formation professionnelle tout au long de la vie et au dialogue social, adoptée le 7 avril 2004. La nouvelle rédaction de cet article ne procure aucun droit nouveau en matière de communication syndicale sur les outils électroniques de l'entreprise.

Les textes législatifs

Loi du 06/01/1978 relative à l'informatique, aux fichiers et aux libertés.

Elle a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique.

Loi du 17/07/1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

~~**Loi du 03/07/1985** relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle.~~

~~Elle interdit à l'utilisateur d'un logiciel toute reproduction de celui-ci autre que l'établissement d'une copie de sauvegarde.~~

Loi du 05/01/1988 sur la fraude informatique.

Cette loi, dite de GODEFRAIN, vise à lutter contre la fraude informatique en réprimant :
Les accès frauduleux dans un système d'information

Les atteintes accidentelles ou volontaires au fonctionnement

La falsification des documents informatiques et leur usage illicite

L'association ou l'entente en vue de commettre un de ces délits

~~**Loi du 10/07/1991** relative au secret des correspondances émises par voie des télécommunications~~

Loi du 13/03/2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

Loi du 21/06/2004 pour la confiance dans l'économie numérique.

Elle est destinée à favoriser le développement du commerce par Internet, en clarifiant les règles pour les consommateurs et les prestataires aussi bien techniques que commerciaux.

Le droit disciplinaire

~~**Loi n°84-53 du 26 janvier 1984** (art. 89 et 90) et le décret n° 89-677 du 18 septembre 1989 relatif à la procédure disciplinaire applicable aux fonctionnaires territoriaux.~~

Vu le code général de la fonction publique,

Décret n°92-1194 du 4 novembre 1992 (art. 6) fixant les dispositions communes applicables aux fonctionnaires stagiaires de la Fonction Publique Territoriale.

Décret n°88-45 du 15 février 1988 (art. 36 et 37) relatif aux agents non titulaires.

REÇU EN PREFECTURE
le 15/12/2022
Application agréée E-legalite.com
093_DE-011-200036411-20221212-CS2022_41-D

Décret n°91-298 du 20 mars 1991 (art. 15) relatif aux agents à temps non complet.

Le code pénal

Article 323-1 : Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de ~~30000~~ 60000 euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de ~~45000~~ 100000 euros d'amende.

Article 323-2 : Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de ~~75000~~ 150 000 euros d'amende.

Article 323-3 : Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de ~~75000~~ 150 000 euros d'amende.

Article 323-3-1 : Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-4 : La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-5 : Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

Article 323-6 : Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 323-7 : La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

La réglementation européenne

REÇU EN PREFECTURE
le 15/12/2022
Application agréée E-legalite.com
09_DE-011-200036101-20221212-CS2022_41-0

La règlementation européenne du 25 mai 2018 impose aux organismes d'assurer une protection optimale des données et d'être en mesure de la démontrer.

Elle se décompose en 6 étapes :

1- Désigner un pilote

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

2- Cartographier

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

3- Prioriser

Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

4- Gérer les risques

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (PIA).

5- Organiser

Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire).

6- Documenter

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

Le Président,

Pierre BARDIES

REÇU EN PREFECTURE
le 15/12/2022
Application agréée E-legalite.com
99_DE-011-200036101-20221212-CS2022_41-0