DELIBERATION N° DEL-2024-38

CONSEIL D'ADMINISTRATION DU CENTRE DE GESTION DU GARD Séance du 28 novembre 2024

✧✧✧✧✧✧✧✧✧✧✧✧✧

OBJET : Adoption d'une charte informatique

PJ : 1

ETAIENT PRESENTS :

Fabrice VERDIER, Président, Jacky REY, Jean-Christian REY, Annick CHOPARD, Liliane ALLEMAND, Maryse GIANNACCINI, Fabienne DHUISME, Florence BOUIS, Nasséra LEGAL, Patrick HIGON, Stéphane LIBERI, Marie-Michèle ALVARO

ETAIENT ABSENTS OU EXCUSES :

Frédéric GRAS,Joffrey LEON , Aurélie GENOLHER, Caroline SAUMADE, Rémi NICOLAS, Henri CROS, Pierre MAUMEJEAN, Pascale FORTUNAT-DESCHAMPS, Serge CATHALA, Jean-Yves CHAPELET, Jean-Michel AZEMA, Nicolas CARTAILLER, Olivier MARTIN, Christine LADET, Jean-Bernard GUILHERMET, Philippe RIBOT, Sylvie ARNAL, Sébastien OMBRAS, Gilles TRAULLET, Jean-François DURAND-COUTELLE, Jean DENAT, Joseph PEREZ, Georges DAUTUN, Françoise LAUTREC, Régis BAYLE, Farès ORCET, Catherine LANÇON, Thierry JACOT, Marie-Andrée DRACS, Olivier JOUVE, Jean-Michel PERRET, Mylène CAYZAC PRAME, Olivier JOUVE, Didier DART,

PROCURATIONS :

Didier DART à Patrick HIGON
Jean-Michel AZEMA à Jacky REY
Jean-Yves CHAPELET à Jean-Christian REY
Caroline SAUMADE à Liliane ALLEMAND
Aurélie GENOLHER à Maryse GIANNACCINI
Pierre MAUMEJEAN à Fabrice VERDIER
Rémi NICOLAS à Stéphane LIBERI

Secrétaire de séance :

Maryse GIANNACCINI

✧✧✧✧✧✧✧✧✧✧✧✧✧

Accusé de réception en préfecture
030-283000024-20241128-DEL-2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

Sur rapport n° 2-1 de Monsieur Fabrice Verdier, Président du centre de gestion du Gard,

Entendu le rapporteur, Monsieur Jean-Christian Rey

Vu, le code général de la fonction publique,

Vu, la directive européenne 95/46/CE du 24 octobre 1995, relative à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,

Vu, la loi n° 78-17 modifiée du 06 janvier 1978 relative l'informatique, aux fichiers et aux libertés,

Vu, le règlement général sur la protection des données (RGPD) du 25 mai 2018 fixant les règles à respecter en matière de protection des données personnelles,

Vu l'avis du comité social territorial en date du 21 octobre 2021,

Considérant ce qui suit :

Les orientations stratégiques arrêtés par le centre de gestion visent à maintenir l'intégrité de son système d'information avec la volonté d'être en mesure de garantir un niveau de performance satisfaisant à tous les utilisateurs des ressources informatiques.

Le centre de gestion dispose d'un système d'information et de communication nécessaire à l'exercice de ses missions.

Il permet au personnel de disposer des moyens de communication électronique, ressources informatiques, informationnelles, numériques et technologiques.

L'essor des technologies et de l'innovation a fait évoluer les usages et les modalités de travail en permettant la mise à disposition d'outils informatiques aux agents qui offrent une ouverture vers l'extérieur qui se révèlent être des vecteurs de

Accusé de réception en préfecture
030-283000024-20241128-DEL-2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

modernisation de la collectivité et du service public, si leur utilisation est faite à bon escient et dans le respect des usages et de la législation en vigueur.

A l'inverse, une mauvaise utilisation de ces outils peut engendrer des risques d'atteinte à la confidentialité, à la disponibilité et à l'intégrité de l'information et par conséquent du système d'information. Celle-ci peut avoir des conséquences graves de nature à engager la responsabilité civile et/ou pénale de l'utilisateur ainsi que celle de la collectivité.

Ainsi, il vous est proposé d'approuver une nouvelle charte informatique ayant pour objet d'assurer la bonne utilisation des systèmes d'information dans le respect des lois, de la confidentialité, du respect d'autrui et de l'intérêt du CDG. Elle s'inscrit par ailleurs dans une démarche d'information, de sensibilisation, de responsabilisation des utilisateurs des moyens de communication électronique et du son système d'information du centre de gestion.

Les membres du conseil d'administration décident à l'unanimité des membres présents ;

Article 1 :

➢ d'approuver la charte informatique telle que présentée en annexe.

Article 2 :

➢ de prendre acte de son application à l'ensemble du personnel, tous statuts confondus, ainsi qu'aux élus et à tout prestataire extérieur ayant accès aux données et aux outils informatiques du CDG.

Article 3 :

➢ d'autoriser le président à signer tout acte permettant l'application et l'exécution de la charte informatique.

Article 4 :

La présente délibération peut faire l'objet, dans un délai de deux mois à compter de son entrée en vigueur, d'un recours administratif auprès de Monsieur le Président du centre de gestion du Gard, 183 chemin du Mas Coquillard 30000 Nîmes, ou d'un recours contentieux auprès du tribunal administratif de Nîmes, 16 avenue Feuchères, 30000 Nîmes. Le tribunal administratif peut aussi être saisi par l'application informatique « Télérecours Citoyens » accessible par le site internet www.telerecours.fr pour le recours contentieux.

La secrétaire de séance

Maryse GIANNACCINI

Le Président

Fabrice Verdier

Acte rendu exécutoire compte tenu de :
- La transmission au représentant de l'Etat le : 28-11-2024
- La publication par voie électronique le : 29-11-2024

Accusé de réception en préfecture
030-283000024-20241128-DEL-2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

CENTRE DE GESTION
DE LA FONCTION PUBLIQUE TERRITORIALE
DU GARD

CHARTE INFORMATIQUE

Vu le règlement n°2016/679 du 27 avril 2016 dit « règlement général sur la protection des données » ;

Vu la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

Vu la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles ;

Vu le décret n° 2018-687 du 1er août 2018 portant application de la loi n°2018-493 ;

Vu l'avis du comité social territorial du Centre de Gestion de la Fonction Publique Territoriale du Gard en date du [**date**] ;

PREAMBULE

Le centre de gestion de la fonction publique territorial du Gard (CDG 30) met en œuvre un **système d'information et de communication (SI)** nécessaire à l'exercice de ses compétences, comprenant notamment un réseau informatique et téléphonique.

Les agents, dans le cadre de leurs missions, sont conduits à accéder aux outils informatiques et aux moyens de communications mis à leur disposition et à les utiliser.

Cette charte a pour finalités :

1. de contribuer à la préservation de la sécurité du système d'information de la collectivité/de l'établissement et fait de l'utilisateur un acteur essentiel à la réalisation de cet objectif,
2. de promouvoir une utilisation raisonnée, loyale, responsable et sécurisée du système d'information par les utilisateurs,
3. de faire respecter la réglementation en vigueur en matière de protection des données, et notamment du règlement n°2016/679 dit « règlement général sur la protection des données » du 27 avril 2016,
4. d'informer tout agent de la collectivité/de l'établissement sur ses droits et devoirs en tant qu'utilisateurs, entre autres :
    - ✓ les usages autorisés des moyens informatiques mis à sa disposition ;
    - ✓ les règles de sécurité en vigueur ;
    - ✓ les mesures de contrôle prises par l'employeur ;
    - ✓ les sanctions encourues par l'utilisateur.

Accusé de réception en préfecture
030-283000024-20241128-DEL-2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

CDG 30 CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD

SOMMAIRE

Accusé de réception en préfecture
030-283000024-20241128-DEL-2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

ARTICLE 1 - CHAMP D'APPLICATION :

ARTICLE 1.1 - DEFINITION DU SYSTEME D'INFORMATION ET DE COMMUNICATION (SI) :

La présente charte s'applique en cas d'utilisation du système d'information et de communication du centre de gestion de la fonction publique territoriale du Gard.

Le système d'information et de communication est notamment constitué des moyens informatiques et téléphoniques mis à la disposition par le Centre de Gestion de la Fonction Publique Territoriale du Gard, qu'ils soient fixes ou mobiles, logiciels ou matériels.

Les moyens informatiques comprennent notamment les serveurs, stations de travail, micro-ordinateurs fixes ou portables, tablettes, smartphones ou tout dispositif susceptibles de se connecter au réseau local ou à l'internet du Centre de Gestion de la Fonction Publique Territoriale du Gard, toute unités d'entrée, de sortie (imprimantes, écrans, etc.), de stockage (clés USB, disques externes), ainsi que les moyens de communication (téléphonie, etc.) présents dans l'ensemble des services du Centre de Gestion de la Fonction Publique Territoriale du Gard.

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication le matériel personnel des agents connecté au réseau du Centre de Gestion de la Fonction Publique Territoriale du Gard, ou contenant des informations à caractère professionnel.

ARTICLE 1.2 - UTILISATEURS CONCERNES :

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication du centre de gestion de la fonction publique territoriale du Gard, quel que soit leur statut, qu'ils soient agents de l'établissement, membres des organisations syndicales, agents ou élus des collectivités affiliées ayant un accès extérieur, ou encore salariés d'une société sous-traitante. Les règles énoncées par la présente charte sont également applicables aux utilisateurs occasionnels tels que les invités ou les visiteurs.

Le centre de gestion de la fonction publique territoriale du Gard met à la disposition de chaque organisation syndicale représentative un matériel spécifique et un espace d'information hébergé sur le site. Il est demandé aux organisations syndicales et représentants du personnel les mêmes précautions d'usage que pour l'ensemble des agents du centre de gestion de la fonction publique territoriale du Gard.

Les agents veillent à faire respecter les règles posées par la présente charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication.

ARTICLE 1.3 - RESPONSABLE DU SYSTEME D'INFORMATION ET DE COMMUNICATION :

Le service informatique est responsable du contrôle du bon fonctionnement du système d'information et de communication. Il veille à l'application des règles de la présente charte. Le responsable du système d'information et de communication est assujetti à une obligation de confidentialité sur les informations qu'il est amené à connaître.

L'administration du système d'information et de communication peut rendre nécessaire un examen des fichiers, journaux (connexions, accès distants, etc.), non seulement afin de diagnostiquer et corriger certains problèmes liés au logiciel, mais aussi pour vérifier, suite à un incident, si un utilisateur n'agit pas en violation des règles de déontologie et de la législation. Dans ce dernier cas, le responsable du système d'information et de communication informera la Direction préalablement à toute investigation. Il peut en outre générer et consulter tout journal d'évènements.

Accusé de réception en préfecture
030-283000024-20241126-DEL-2024-36-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

En fonction des moyens à sa disposition, il est notamment tenu :

- De faire respecter les droits et responsabilités des utilisateurs.
- De respecter la confidentialité des fichiers, courriers et sorties imprimées des utilisateurs.
- D'assurer la sécurité et la confidentialité des réseaux en mettant en œuvre les ressources techniques et humaines requises.
- D'informer les utilisateurs, par les moyens appropriés, de toute intervention prévue à l'avance et susceptible de perturber ou interrompre l'utilisation des ressources informatiques.

Le responsable du système d'information et de communication peut, après accord de la Direction, prendre des mesures conservatoires, telles que l'arrêt d'une exécution, la suppression des droits d'accès et de mots de passe, voire la fermeture du réseau au monde extérieur, afin de pallier un incident éventuel de fonctionnement et de sécurité.

Le responsable du système d'information et de communication est autorisé par la Direction à prendre les mesures conservatoires, telles que la coupure des connexions, l'arrêt total du système d'information ou des serveurs, sans son accord préalable si l'urgence le nécessite.

Le responsable du système d'information et de communication se donnera les moyens appropriés pour mettre fin à tout abus. L'utilisateur en sera, dans tous les cas, averti.

ARTICLE 1.4 - MISE EN APPLICATION

1.4.1 - INFORMATION DES AGENTS

La présente charte est affichée publiquement en annexe du règlement intérieur. Elle est communiquée individuellement à chaque agent.

Le responsable du système d'information et de communication est à la disposition des agents pour leur fournir toute information concernant l'utilisation des nouvelles technologies de l'information et de la communication. Il informe les utilisateurs régulièrement sur l'évolution des limites techniques du système d'information et sur les menaces susceptibles de peser sur sa sécurité.

1.4.2 - ÉVOLUTION DE LA CHARTE INFORMATIQUE

La présente charte peut être amenée à évoluer, notamment en raison des évolutions législatives, réglementaires et techniques.

1.4.3 - ENTREE EN VIGUEUR DE LA CHARTE INFORMATIQUE

La présente charte est applicable à compter du [**date**].

Accusé de réception en préfecture
030-283000024-20241128-DEL-2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

ARTICLE 2 - MODALITES D'UTILISATION DE L'OUTIL INFORMATIQUE

ARTICLE 2.1 - UTILISATION DE L'OUTIL INFORMATIQUE

L'utilisation des outils informatiques et des moyens d'information et de communication mis à la disposition des agents doit être exclusivement professionnelle, sauf autorisation préalable de la Direction après consultation du service informatique afin de pallier toute action susceptible de compromettre la sécurité du système. Si une telle autorisation devait être accordée, l'usage personnel qui en résulterait devrait être occasionnel et raisonnable, tant dans la fréquence que dans la durée, conforme à la législation en vigueur et ne pas porter atteinte à la sécurité et à l'intégrité du système d'information, des données professionnelles ou à caractère personnel traitées au sein du centre de gestion de la fonction publique territoriale du Gard, ou encore à l'image de l'établissement, et plus largement à celle de la fonction publique.

ARTICLE 2.2 - CONFIDENTIALITE DES PARAMETRES D'ACCES

L'accès à certains éléments du système d'information est protégé par des paramètres de connexion requérant un identifiant et un mot de passe. Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels.

Ces éléments doivent êtres mémorisés par l'utilisateur et ne pas être conservés par lui, sous quelque forme que ce soit. Est cependant tolérée l'usage de gestionnaires de mots de passe, sous réserve qu'ils aient été installés et paramétrés par le service informatique dans les règles de l'art, conformément aux recommandations de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI). Ils ne doivent pas être transmis à des tiers ou être aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.

Ces paramètres sont déterminés lors de la première utilisation par le responsable du système d'information et de communication selon un certain degré de complexité, conformément aux recommandations de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), et sont communiqués aux agents sous un format apte à en garantir la confidentialité. Il appartient ensuite à l'utilisateur de les modifier de sorte à être le seul à les connaître. Ces paramètres pourront être amenés à être modifiés pour des raisons de sécurité selon un rythme déterminé par le service informatique.

L'utilisateur est responsable de son compte et de son mot de passe, et de l'usage qui en est fait. Il ne doit pas masquer son identité sur le réseau local ou usurper l'identité d'autrui en s'appropriant le mot de passe d'un autre. Il a l'interdiction d'utiliser le compte d'un autre utilisateur ou d'utiliser un compte générique ou encore de laisser l'usage de ses identifiants à autrui.

Pour ce qui concerne le cas particulier des utilisateurs extérieurs (collectivités affiliées, organisation syndicales, etc.) qui ne peuvent avoir de compte attaché à une personne physique, le responsable du compte est respectivement l'autorité territoriale pour la collectivité ou l'établissement public affilié, et le délégué désigné par les organisations syndicales auprès du centre de gestion de la fonction publique territoriale du Gard. Ce responsable doit veiller à ce que l'utilisation de ce compte soit conforme à la présente charte et à la réglementation en vigueur.

Lors du départ définitif d'un utilisateur de l'établissement, ce droit d'accès sera supprimé.

Accusé de réception en préfecture
030-283000024-20241128-DEL-2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

ARTICLE 2.3 - REGLES DE SECURITE ET PROTECTION DES RESSOURCES SOUS LA RESPONSABILITE DE L'UTILISATEUR

L'utilisateur est chargé de signaler au responsable du système d'information et de communication toute violation ou tentative de violation suspectée de son compte informatique et, de manière générale, tout dysfonctionnement.

Il est responsable quant à lui des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence.

En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel. Il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé et à son innocuité. À la fin de son service, l'utilisateur veillera à arrêter son poste de travail informatique.

L'utilisateur doit effectuer des sauvegardes régulières des fichiers dont il dispose sur le matériel mis à sa disposition. Il doit néanmoins s'efforcer de n'occuper que la quantité d'espace disque qui lui est strictement nécessaire dans le cadre de ses missions ou de ses tâches. Il en est de même pour les activités privées tolérées. L'utilisateur veillera à ne stocker qu'un minimum de photos personnelles ou autres fichiers dont l'utilisation est tolérée sous la condition de ne pas outrepasser les limites du raisonnable.

L'utilisateur ne doit pas installer, copier, modifier ou détruire des logiciels sans autorisation. Il doit éviter de copier ou d'installer des fichiers susceptibles de créer des risques de sécurité au sein du centre de gestion de la fonction publique territoriale du Gard. Il doit dans tous les cas en informer le responsable du système d'information et de communication.

L'utilisateur ne devra en aucun cas contourner les restrictions d'utilisation des logiciels, ni développer de programmes pouvant s'auto-dupliquer, s'attacher ou s'attaquer à d'autres programmes (virus informatique).

L'utilisateur ne doit pas accéder, tenter d'accéder ou supprimer des informations si cela ne relève pas des tâches lui incombant. Il veille au respect de la confidentialité des informations en sa possession. Il doit en toutes circonstances veiller au respect de la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables.

Les activités risquant de monopoliser fortement les ressources informatiques (impression de gros documents, calculs importants, utilisation intensive du réseau, etc.) devront être effectuées dans la mesure du possible aux moments qui pénalisent le moins l'ensemble des utilisateurs et après en avoir averti le responsable du système d'information et de communication.

Tout utilisateur du centre de gestion de la fonction publique territoriale du Gard ayant besoin de connecter au réseau filaire ou Wi-Fi un appareil personnel, tel qu'un ordinateur portable ou un smartphone, il doit en avertir le responsable du système d'information et de communication. L'utilisation de cet appareil doit alors respecter les règles de la présente charte comme si l'appareil était une ressource informatique du centre de gestion de la fonction publique territoriale du Gard.

À l'exception des ordinateurs portables mis à la disposition des agents, aucun matériel ni logiciel informatique appartenant au centre de gestion de la fonction publique territoriale du Gard ne peut en être sorti sans autorisation préalable de la Direction.

Lors de son départ définitif de l'établissement, chacun est tenu de restituer les matériels, logiciels et documentations informatiques, qui lui auront été confiés en vue de l'exécution de son travail, et ce, en bon état.

Accusé de réception en préfecture
030-283000024-20241128-DEL-2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

ARTICLE 2.4 – REGLES SPECIFIQUES AUX AGENTS EXERÇANT MOMENTANEMENT LEURS FONCTIONS EN DEHORS DU CENTRE DE GESTION

Les agents peuvent, exceptionnellement, être amenés à exercer leurs fonctions en dehors du centre de gestion de la fonction publique territoriale du Gard, soit du fait de leurs missions itinérantes nécessitant un déplacement justifié par un ordre de mission permanent ou temporaire, soit du fait d'une mise en télétravail au sens du décret n°2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique et la magistrature.

Ces agents sont amenés à appliquer en toutes circonstances les règles de confidentialité et de sécurité prescrites par la présente charte. Ils doivent en toutes circonstances veiller à ne pas laisser quiconque accéder au matériel professionnel, informatique ou non, ainsi qu'aux dossiers et données traités dans le cadre professionnel. Ils doivent garantir par tous les moyens l'intégrité du matériel, des dossiers et données, notamment contre les risques naturels et technologiques, ainsi que contre tout accident domestique de nature à les détériorer ou les détruire.

Lors de l'utilisation de l'outil informatique, notamment en cas d'accès distant aux serveurs du centre de gestion de la fonction publique territoriale du Gard, les agents ont pour obligation de suivre les instructions qui leur auront été données par le responsable du système d'information et de communication afin de garantir l'intégrité du matériel et des données traitées informatiquement.

ARTICLE 2.5 - ACCES A INTERNET

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par le responsable du système d'information et de communication. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

L'utilisateur est informé que les traces de la navigation sont temporairement archivées. En effet, à la demande d'une autorité judiciaire ou administrative, l'administrateur du pare-feu devra fournir les informations de la navigation web.

Le centre de gestion de la fonction publique territoriale du Gard se réserve le droit :

- De contrôler le contenu de toute page Web hébergée sur ses serveurs en vue de s'assurer du respect des conditions d'utilisation des services énoncées par la présente Charte.
- De suspendre l'usage du service d'hébergement des pages Web par un utilisateur en cas de non-respect de la Charte et notamment dans l'hypothèse où l'utilisateur aurait diffusé sur ses pages Web un contenu manifestement illicite.

L'utilisateur s'engage à respecter les règles suivantes :

- L'utilisateur ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par l'administrateur du Système d'Information ou la Direction.
- L'utilisateur ne doit pas utiliser ces services pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur.
- Interdiction de consulter ou télécharger du contenu de sites web à caractère pornographique, pédophile ou tout autre site illicite, contraire aux bonnes mœurs ou susceptible de porter atteinte à l'image de la fonction publique.
- Interdiction de se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède.
- Pour participer à des forums, l'utilisateur doit disposer d'autorisations internes afin de

Accusé de réception en préfecture
030-283000024-20241128-DEL-2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

s'exprimer au nom du centre de gestion de la fonction publique territoriale du Gard. Dans toutes ses communications, l'utilisateur devra faire preuve de la plus grande correction à l'égard de ses interlocuteurs. Il n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice au centre de gestion de la fonction publique territoriale du Gard. De même, il doit s'imposer le respect des lois, notamment celles relatives aux publications à caractère injurieux, raciste, négationniste, pornographique, pédophile, homophobe, diffamatoire ou discriminatoire sur les mœurs ou l'orientation sexuelle ou l'identité de genre. (Loi n° 2012-954 du 6 août 2012 relative au harcèlement sexuel, Loi n° 2017-86 du 27 janvier 2017 relative à l'égalité et à la citoyenneté)

- Les téléchargements de contenu illicite sont interdits (contrefaçon de marque, copie de logiciels commerciaux, etc.).

La consultation de sites web à titre privé est tolérée à titre exceptionnel et à condition que la navigation n'entrave pas l'accès professionnel et qu'elle s'effectue hors du temps de travail de l'utilisateur. La Direction se réserve le droit d'effectuer des contrôles sur les durées de connexion et les sites visités.

ARTICLE 2.6 - MESSAGERIE ELECTRONIQUE

Chaque agent dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique personnelle attribuée par le responsable du système d'information et de communication.

Cette adresse de messagerie électronique personnelle ne doit être utilisée que par l'agent lui-même de la même manière que pour le compte qui permet l'accès au système d'information. L'accès à la boite e-mail personnelle est réservé à l'agent et seule une autorité judiciaire peut, le cas échéant, en réclamer l'accès.

De plus, selon les missions assurées par l'agent, celui-ci dispose d'un ou de plusieurs accès aux adresses électroniques des services auxquels il est affecté. Les règles d'utilisation de ces adresses électroniques professionnelles sont les mêmes que pour les adresses personnelles. Le principe de moindre privilège s'applique de la même façon que pour le reste des données du système d'information.

Les messages électroniques reçus font l'objet d'un contrôle antiviral et d'un filtrage des courriels indésirables. Les agents sont invités à signaler tout dysfonctionnement constaté dans le dispositif de filtrage.

L'envoi de messages électroniques obéit aux mêmes règles que l'envoi de correspondances postales. Les messages électroniques ont la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. L'utilisateur doit donc prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager sa responsabilité civile ou pénale ou celle du Centre de Gestion de la Fonction Publique Territoriale du Gard.

Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non-sollicités. Il doit également dissimuler les destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

En cas d'envoi à une liste de diffusion, il est impératif de vérifier la liste des abonnés à celle-ci.

La vigilance des utilisateurs doit redoubler en présence d'informations à caractère personnel et/ou confidentiel. Les messages doivent dans ce cas être chiffrés, conformément aux recommandations de l'ANSSI.

Accusé de réception en préfecture
030-283000024-20241128-DEL-2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

Le risque de retard, de non remise et de suppression automatique des messages électroniques doit être pris en considération pour l'envoi de correspondances importantes. Les messages importants doivent être envoyés avec un accusé de réception et être, le cas échéant, doublés par des envois postaux.

Afin de ne pas surcharger les serveurs de messagerie, il est attendu de chaque utilisateur, une gestion des messages (suppression, archivage, effacement périodique) et de la taille des pièces jointes envoyées.

L'utilisateur doit veiller au respect des lois et règlements. Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, injurieux, contrefaisants ou, d'une manière plus générale, contrevenants aux dispositions statutaires relatives aux droits et obligations du fonctionnaire.

L'utilisateur devra faire preuve de vigilance afin de ne pas suivre les liens piégés dans les messages de type « *phishing* ». Les fichiers rattachés ayant une extension de type « .exe » ne devront jamais être ouverts. Les messages suspects (objet douteux, émetteur inconnu, adresse mail étrange, pièce jointe suspecte, etc.) ne devront pas être ouverts non plus. Tout fichier semblant suspect devra être supprimé. En cas de doute, l'utilisateur est invité à prendre immédiatement conseil auprès du responsable du système d'information et de communication.

ARTICLE 3 - CONDITIONS D'ADMINISTRATION DU SYSTEME D'INFORMATION

Pour des nécessités de maintenance et de gestion, l'utilisation des ressources matérielles ou logicielles, les échanges via le réseau, ainsi que les rapports des télécommunications peuvent être analysés et contrôlés dans le respect de la législation applicable, et notamment de la loi Informatique et Libertés.

L'utilisateur est informé que pour effectuer la maintenance corrective, curative ou évolutive, le responsable du système d'information et de communication dispose de la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition. Il a potentiellement la possibilité d'accéder, à des fins de contrôle ou de maintenance, et après en avoir informé au préalable l'utilisateur, à l'ensemble des fichiers stockés sur les postes utilisateurs, sur les serveurs, et de manière générale à tout contenu créé par un agent sur l'infrastructure informatique du centre de gestion de la fonction publique territoriale du Gard. Des moyens de chiffrement sont toutefois à la disposition des utilisateurs pour permettre le stockage d'informations à caractère confidentiel.

Le centre de gestion de la fonction publique territoriale du Gard se réserve, dans ce cadre, le droit de recueillir et de conserver les informations nécessaires à la bonne marche du système. Il se réserve la possibilité de procéder à un contrôle des sites visités afin d'éviter l'accès par les utilisateurs à des sites illicites.

Le centre de gestion de la fonction publique territoriale du Gard met en place un pare-feu destiné à vérifier et filtrer tout le trafic sortant. Il vérifie et filtre également le trafic entrant. Il consigne toutes les traces de l'activité qui transite par lui : s'agissant de la navigation sur internet (sites visités, heures des visites, éléments téléchargés et leur nature) ou s'agissant des messages envoyés et reçus (expéditeur, destinataire, nature et nom des éventuelles pièces jointes).

Le responsable du système d'information et de communication respecte la confidentialité des données et des traces auxquelles il est amené à accéder dans l'exercice de ses fonctions, mais peut être amené à les utiliser pour mettre en évidence certaines infractions commises par les utilisateurs ou dysfonctionnements du système.

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde des informations et un dispositif miroir destiné à doubler le système en cas de défaillance. Cependant, il est rappelé que la suppression par un utilisateur d'un fichier de son espace disque n'est pas absolue et qu'il en reste

Accusé de réception en préfecture
030-283000024-20241128-DEL-2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

éventuellement une copie, soit sur le dispositif de miroir du serveur de sauvegarde, soit sur le dispositif de sauvegarde. Les sauvegardes sont effectuées suivant un calendrier établis par le responsable du Système d'Information et de Communication et disponible auprès de lui.

Les sauvegardes de données ne s'appliquent pas aux organisations syndicales qui ne disposent pas d'un accès au système de stockage interne mutualisé du centre de gestion de la fonction publique territoriale du Gard. Les sauvegardes de leurs données sont à la charge de ces mêmes organisations. Seuls les flux entrants et sortants seront contrôlés pour des raisons de sécurité.

Afin de respecter les obligations légales et réglementaires, et notamment les obligations en matière de durée de conservation des données, le centre de gestion de la fonction publique territoriale du Gard s'est doté d'outils d'historisation et de filtrage de contenu. Sont ainsi susceptibles d'être stockés pendant une durée conforme aux obligations légales et réglementaires :

- Concernant les connexions Internet :
  - ✓ Le nom de l'utilisateur
  - ✓ L'adresse IP source
  - ✓ Le site visité (IP destination + URL)
  - ✓ La date et l'heure
  - ✓ La catégorie du site visité
- Concernant la messagerie électronique, le responsable du système d'information et de communication est en mesure de consulter :
  - ✓ Les quotas des Boites à Lettres
  - ✓ La date de la dernière connexion
- Il peut également être amené à demander au fournisseur de la messagerie :
  - ✓ La fréquence et la taille des messages électroniques
  - ✓ Le volume des messages échangés, de façon globale et par l'utilisateur
  - ✓ Le format des pièces jointes
- Concernant les communications téléphoniques passées ou reçues sur les postes fixes ou mobiles du centre de gestion de la fonction publique territoriale du Gard :
  - ✓ Le numéro appelant
  - ✓ Le numéro appelé
  - ✓ La date, l'heure et la durée de l'appel

La consultation de ces historiques (navigation Internet, messagerie, téléphonie) est strictement limitée au responsable du système d'information et de communication ainsi qu'à la Direction du centre de gestion de la fonction publique territoriale du Gard.

ARTICLE 4 - PROTECTION DES DONNEES A CARACTERE PERSONNEL

ARTICLE 4.1 - CONFIDENTIALITE DES DONNEES

Le règlement n°2016/679 dit « règlement général sur la protection des données » du 27 avril 2016 définit les conditions dans lesquelles des traitements de données personnelles peuvent être opérés. Il institue au profit des personnes concernées par les traitements de données des droits que la présente charte invite à respecter, tant à l'égard des utilisateurs que des tiers.

Accusé de réception en préfecture
030-243000024-20241128-DEL2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

Les agents sont soumis à une obligation de discrétion qui leur impose d'assurer la confidentialité des données qu'ils détiennent.

Un comportement exemplaire est exigé dans toute communication orale ou écrite, téléphonique ou électronique, que ce soit lors d'échanges professionnels ou au cours de discussions relevant de la sphère privée.

ARTICLE 4.2 - ACCES AUX DONNEES PAR LES AGENTS

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, ainsi que ceux publics ou partagés (principe de moindre privilège).

Il est ainsi interdit de prendre connaissance des informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées. Cette règle s'applique en particulier aux données couvertes par le secret professionnel, ainsi qu'aux conversations de type courrier électronique dont l'utilisateur n'est ni directement destinataire, ni en copie.

L'utilisateur doit assurer la confidentialité des données qu'il détient. En particulier, il ne doit pas diffuser à des tiers, au moyen d'une messagerie non sécurisée, des informations nominatives et/ou confidentielle.

Les documents bureautiques produits doivent être stockés sur des serveurs de fichiers. Ces espaces sont à usage professionnel uniquement. Le stockage de données privées sur des disques réseau est interdit.

Les médias de stockage amovibles (clefs USB, CD, disques durs, etc.) présentent des risques très forts vis-à-vis de la sécurité : risques importants de contamination par des programmes malveillants ou risque de perte de données. Leur usage doit donc être fait avec une très grande vigilance. Le centre de gestion de la fonction publique territoriale du Gard se réserve le droit de limiter voire d'empêcher l'utilisation de ces médias en bloquant les ports de connexion des outils informatiques.

L'utilisateur s'engage à récupérer sur les matériels d'impression les documents sensibles envoyés, reçus, imprimés ou photocopiés.

Les données concernant l'utilisateur (sites consultés, messages échangés, etc.) peuvent être enregistrées par des tiers, analysées et utilisées à des fins notamment commerciale. Il est donc recommandé à chaque utilisateur de ne pas fournir son adresse électronique professionnelle, ni aucune coordonnée professionnelle sur internet, si ce n'est strictement nécessaire à la conduite de son activité professionnelle.

Article 4.3 - Responsable de traitements et délégué à la protection des données

Le Président du centre de gestion de la fonction publique territoriale du Gard est responsable des traitements de données à caractère personnel. Le responsable de traitements veille au sein du centre de gestion de la fonction publique territoriale du Gard à la bonne application des règles issues du règlement général sur la protection des données.

Un délégué à la protection des données a été désigné afin de piloter la bonne application de ces règles.

Accusé de réception en préfecture
030-283000024-20241128-DEL-2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

ARTICLE 5 - REPONSES AUX DEMANDES D'USAGE DES DROITS DES PERSONNES CONCERNEES PAR LES TRAITEMENTS DE DONNEES

ARTICLE 5.1 - DROITS DES PERSONNES CONCERNEES PAR LES TRAITEMENTS DE DONNEES

Les personnes concernées par les traitements de données personnelles, quels qu'ils soient, disposent de droits leur permettant de garder la maîtrise des informations les concernant. Ainsi, toute personne peut :

- Accéder à l'ensemble des informations la concernant ;
- Connaître l'origine de ces informations :
- En obtenir une copie ;
- Exiger que ses données soient rectifiées, complétées, mises à jour ou, selon les cas, supprimées.

ARTICLE 5.2 - DROIT A L'INFORMATION DES PERSONNES CONCERNEES PAR LES TRAITEMENTS DE DONNEES

Les agents ont l'obligation d'informer toute personne du recueil de ses données à caractère personnel, de ses droits ainsi que des moyens par lesquels cette personne pourra user de ses droits sur ces données.

ARTICLE 5.3 - DEMANDES D'USAGE DES DROITS DES PERSONNES

Les personnes concernées par les traitements de données à caractère personnel peuvent faire usage de leurs droits sur simple demande, soit par écrit, soit en personne.

Les agents recevant une telle demande ont pour obligation de contrôler par tous moyens de l'identité du demandeur.

ARTICLE 5.4 - INSTRUCTION DES DEMANDES D'USAGE DES DROITS DES PERSONNES

Les agents recevant une demande d'usage des droits des personnes concernées par un traitement de données ont pour obligation de transmettre cette demande au service chargé de la mise en œuvre du traitement.

Ce service aura alors pour obligation de répondre à cette demande dans un délai maximum d'un mois à compter de la date de présentation de la demande.

À défaut de pouvoir identifier le service chargé de la mise en œuvre du traitement, les agents peuvent transmettre la demande d'usage des droits de la personne concernée par le traitement au délégué à la protection des données qui sera alors chargé de procéder à son instruction dans les mêmes délais et selon la même procédure.

La réponse devra se faire de manière compréhensible. Toute abréviation, sigle ou code devra faire l'objet de précisions, notamment aux moyens d'un lexique ou d'une notice explicative.

ARTICLE 5.5 - REFUS DE LA DEMANDE D'USAGE DES DROITS DES PERSONNES

La demande pourra être refusée pour des motifs légitimes, notamment le respect d'une obligation légale. Peuvent également être refusées les demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique.

Publié le, réceptionné préfecture
030-283000024-20241128-DEL-2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

Tout refus devra alors faire l'objet d'une justification. Le demandeur devra être également informé des voies et délais de recours permettant de contester cette décision.

Si le centre de gestion de la fonction publique territoriale du Gard ne dispose d'aucune donnée sur la personne qui exerce son droit d'accès, une réponse précisant ce fait devra être apportée dans le délai d'un mois.

ARTICLE 5.6 - REPONSES AUX DEMANDES D'USAGE DES DROITS DES PERSONNES

Toute demande et toute réponse devront faire l'objet d'une traçabilité. Tout service instruisant une telle demande ou procédant à une telle réponse devra procéder à son inscription dans le registre des demandes d'usage des droits sur les données à caractère personnel.

Ce registre est tenu et mis à jour par le responsable de traitement du centre de gestion de la fonction publique territoriale du Gard avec l'assistance du délégué à la protection des données.

ARTICLE 6 - VIOLATIONS DE DONNEES A CARACTERE PERSONNEL

ARTICLE 6.1 - CONSTATATION DES VIOLATIONS DE DONNEES

Toute 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 manière, ou l'accès non autorisé à de telles données constitue une violation de données à caractère personnel.

Tout agent amené à constater une telle violation de données a l'obligation d'en informer immédiatement le délégué à la protection des données.

ARTICLE 6.2 - DOCUMENTATION DE LA VIOLATION DE DONNEE

Conjointement avec le délégué à la protection des données, l'agent devra, dans un délai maximum de 48 heures :

- Déterminer la nature de la violation ;
- Déterminer la catégorie et le nombre approximatif de personnes concernées par les données faisant l'objet de la violation ;
- Déterminer la catégorie et le nombre approximatif de données concernées ;
- Décrire les conséquences probables de la violation de données ;
- Déterminer et décrire les mesures prises pour atténuer les effets de la violation et éviter que celle-ci ne se reproduise.

L'ensemble de ces éléments devront faire l'objet d'une traçabilité et d'une inscription dans le registre des violations de données.

Ce registre est tenu et mis à jour par le délégué à la protection des données.

ARTICLE 6.3 - NOTIFICATION DES VIOLATIONS DE DONNEES AUPRES DE LA CNIL

Toute violation de données susceptible de porter atteinte à la vie privée des personnes concernées par les données touchées par la violation doit faire l'objet d'une notification auprès de la CNIL aux moyens d'une plate-forme sécurisée sur son site internet (www.cnil.fr).

Accusé de réception en préfecture
030-283000024-20241128-DEL-2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024

Cette notification devra être réalisée conjointement avec le délégué à la protection des données dans un délai maximal de 72 heures suivant la violation de données ou, à défaut, dans un délai maximal de 72 heures suivant la constatation de la violation de données.

En cas d'impossibilité de réunir toutes les informations susmentionnées dans un tel délai, une notification initiale devra être déposée dans ledit délai, suivie d'une notification complémentaire dès que l'ensemble des éléments seront réunis.

Toute notification effectuée hors délais devra être justifiée.

ARTICLE 6.4 - NOTIFICATION DES VIOLATIONS DE DONNEES AUPRES DES PERSONNES CONCERNEES

Toute violation de données susceptible de porter une atteinte excessivement élevée à la vie privée des personnes concernées par les données touchées par la violation devra, en outre de la notification mentionnée à l'article 6.3, faire l'objet d'une notification auprès des personnes concernées.

La notification devra *a minima* contenir et exposer, en des termes clairs et précis, la nature de la violation, les conséquences probables de la violation, les coordonnées du délégué à la protection des données et les mesures prises pour remédier à la violation et en limiter les conséquences.

La notification devra être complétée, si nécessaire, de recommandations à destination des personnes pour atténuer les effets négatifs potentiels de la violation et leur permettre de prendre les précautions qui s'imposent, tel qu'un changement de mot de passe ou la vérification de l'intégrité des données de leur compte utilisateur.

Cette notification devra être réalisée en collaboration avec le délégué à la protection des données dans les meilleurs délais.

Article 6.5 - Traçabilité des notifications de violations de données

La notification de la violation de données auprès de la CNIL et, le cas échéant, la notification aux personnes concernées devront faire l'objet d'une traçabilité et être inscrites dans le registre des violations de données.

ARTICLE 7 - RESPONSABILITE ET SANCTIONS

L'utilisateur est responsable de son utilisation des outils d'information et de communication mis à sa disposition. Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager sa responsabilité et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

Accusé de réception en préfecture
030-283000024-20241128-DEL-2024-38-DE
Date de télétransmission : 28/11/2024
Date de réception préfecture : 28/11/2024