Charte d'Utilisation des Services et Matériel Informatiques

335 Allée du Général GIRARD - La Citadelle- Quartier des 3 parallèles – 62000 ARRAS
contact@lafibrenumerique5962.fr - Tél 03 74 04 59 62

Envoyé en préfecture le 27/06/2025
Reçu en préfecture le 27/06/2025
Publié le
ID : 059-200039386-20250625-2025_12-DE

Préambule

Les activités du Syndicat Mixte La Fibre Numérique 59 62 s'appuient fortement sur les ressources informatiques mises à disposition par le syndicat

Le Système d'Information (SI) du syndicat est un outil indispensable pour l'ensemble des agents.

La performance et la sécurité reposent sur le respect d'un certain nombre de règles et de bonnes pratiques.

Une prise de conscience individuelle et collective des enjeux de la sécurité du SI est indispensable, tant pour l'institution que pour l'utilisateur, notamment en ce qui concerne la responsabilité civile et pénale.

Cette Charte se veut pragmatique et pédagogique. Elle doit susciter pour chaque utilisateur du SI des réflexes d'autorégulation favorisant une utilisation sûre et performante des services informatisés offerts aux agents du Syndicat.

La présente charte a pour but de définir les règles de sécurité et de bons usages des SI du Syndicat. Il s'agit de fournir à tous, un document de référence formalisant les règles de sécurité et les comportements attendus des utilisateurs.

Compte tenu de la nécessité pour le Syndicat de se protéger contre toute activité illégale, abusive ou préjudiciable au bon fonctionnement de ses services, la présente charte fixe également les modalités de contrôle et de surveillance de l'utilisation des matériels et ressources informatiques, les durées de conservation et conditions de stockage afférant à ces contrôles, dans le respect des obligations réglementaires (droit à la vie privée, secret des correspondances, Règlement Général sur la Protection des Données, etc.).

Table des matières

Envoyé en préfecture le 27/06/2025
Reçu en préfecture le 27/06/2025
Publié le
ID : 059-200039386-20250625-2025_12-DE

I – CHAMP D'APPLICATION

Article 1 - Utilisateurs concernés

La présente charte s'applique et est opposable à l'ensemble des utilisateurs des systèmes d'information.

Est considéré comme utilisateur toute personne physique formellement autorisée à accéder au SI du Syndicat, quel que soit son statut (Titulaire, contractuel en CDI, en CDD, stagiaire, étudiant).

La présente charte s'applique à l'ensemble des fonctions du Syndicat

Article 2 – Moyens informatiques concernés

Les moyens informatiques visés par la présente charte sont notamment constitués des ressources et outils suivants : ordinateurs (fixes, portables, …), terminaux mobiles (tablettes, smartphones, …), périphériques (imprimantes, multifonctions …), réseaux informatiques (filaire ou sans-fil), logiciels, fichiers, données et bases de données, serveurs et équipements réseaux, systèmes de messagerie, visioconférence et Internet.

II – REGLES GENERALES D'USAGE DES MOYENS INFORMATIQUES

Article 3 –Règles d'usage communes à tous les moyens informatiques

L'utilisation des moyens informatiques quels qu'ils soient est soumise au respect des règles précisées ci-dessous.

Article 3.1 Utilisation professionnelle des moyens informatiques

L'utilisation des moyens informatiques est réservée à des fins professionnelles.

L'utilisation de la messagerie et d'internet à des fins personnelles doit être raisonnable, demeurer exceptionnelle et ne pas affecter la sécurité des systèmes d'information, le fonctionnement du réseau de communication interne (téléchargements notamment), l'image du Syndicat ou la productivité.

Article 3.2 Utilisation prudente des moyens informatiques

Le matériel mis à disposition des utilisateurs est la propriété exclusive du Syndicat. Le matériel et les accessoires (sacoche, périphérique, souris, cordon, …) sont mis à disposition des utilisateurs à titre individuel et répertoriés comme tels. L'utilisateur se doit de maintenir le matériel ainsi confié en bon état et alerter le service informatique de toute difficulté d'utilisation. Le matériel ne doit pas faire l'objet d'échanges ou de prêts y compris à un autre agent du Syndicat. Il appartient également à l'utilisateur de veiller sur son matériel et notamment de prendre les mesures de précaution élémentaires contre le vol, en particulier des ordinateurs portables et terminaux mobiles.

Il est strictement interdit d'installer des périphériques (scanner, webcam, imprimante…), et logiciels (jeux, outils, …) personnels afin d'éviter tout dysfonctionnement. Un audit du parc peut être effectué pour déceler la présence de matériels ou logiciels non autorisés/requis par la mission des agents. En cas de détection de tels périphériques ou logiciels, ceux-ci seront désactivés ou désinstallés sans préavis par le service informatique.

Seuls les ordinateurs et équipements mobiles fournis ou agréés par le Syndicat peuvent être connectés au réseau informatique.

Le réseau wifi est accessible en zone couverte par tout agent disposant d'un ordinateur portable ou d'un téléphone portable du syndicat.

Le service informatique met en place et maintien des solutions de sécurité (antivirus, antispam, filtrage de flux, etc.) permettant de limiter les risques liés à la sécurité des systèmes d'information.

Cependant, l'évolution des menaces (hameçonnage, rançongiciel, etc.) nécessite une vigilance accrue de la part des utilisateurs qui, malgré les précautions prises, pourraient introduire à leur insu des virus ou provoquer d'autres incidents de sécurité (ex : perte ou fuite de données).

En cas d'incident, d'anomalie ou de doute, l'agent doit stopper toute manipulation ou transaction et prévenir immédiatement le service informatique.

Article 3.3 Confidentialité et propriété des données

Quel que soit le matériel ou la ressource informatique utilisée (réseau, internet, messagerie, …), l'utilisateur se doit de veiller au respect de la confidentialité des données en sa possession ou des données dont il peut avoir connaissance à l'occasion de l'exercice de sa mission ou par erreur, en particulier des données couvertes par le secret professionnel ou le droit à la vie privée et signaler au service informatique toute donnée de cette nature figurant sur une ressource non prévue à cet effet.

Les moyens mis à la disposition de l'utilisateur doivent être mis en œuvre dans une finalité professionnelle et leur utilisation doit rester conforme aux besoins du service et aux intérêts du Syndicat.

Tout utilisateur peut être amené à avoir connaissance ou à manipuler des informations plus ou moins sensibles sur le plan de la confidentialité. Il est de son devoir de ne pas diffuser à l'extérieur du Syndicat les informations qui pourraient nuire au fonctionnement ou à l'image de l'institution ou porter préjudice à une personne.

Les informations sont accessibles aux professionnels dans la mesure où elles sont nécessaires à l'exercice de leur fonction qui lui sont affectés ou dans le cadre de remplacement.

Pour rappel, corollaire du droit des personnes, le devoir de discrétion implique de :

- ne pas rechercher ou consigner d'informations au-delà de ce qui est nécessaire pour la mission à accomplir ;

- ne pas divulguer à des tiers des informations de nature confidentielle apprises du fait de l'exercice de sa fonction, ou ne le faire qu'avec l'accord de la personne concernée

- veiller à tout propos qui serait susceptible de porter atteinte à l'image, à la dignité, à la réputation, à l'honneur, à la tranquillité ou à la sécurité de la personne concernée ;

- veiller à la confidentialité du cadre dans lequel se déroulent les échanges ;

- sécuriser l'accès à la conservation des données, qu'il s'agisse d'écrits ou de fichiers informatisés ;

-informer la personne de leur existence, lui permettre d'y accéder et d'exercer son droit de rectification, de formulation d'un avis contradictoire, voire de suppression pour les fichiers informatisés.

L'ensemble des informations, données, documents, fichiers, logiciels (cette liste n'est pas exhaustive), que l'utilisateur produit dans le cadre de son activité professionnelle sont de la propriété du Syndicat.

L'utilisateur s'interdit donc de faire de ces données une utilisation autre que celle pour laquelle elles sont destinées. Il lui est donc interdit de les utiliser à des fins personnelles, que ce soit dans un cadre purement privé, ou dans le cadre d'une autre activité professionnelle, salariée ou non. Cette interdiction vaut tant pendant le temps où l'utilisateur est employé par le Syndicat, qu'après son départ du Syndicat pour quelque cause que ce soit.

Article 3.4 Premier accès au réseau et nouveaux besoins

Tout nouvel utilisateur est créé dans l'annuaire informatique du Syndicat, ce qui lui permet de disposer d'un compte d'accès au réseau informatique.

Pour accéder à d'autres ressources informatiques du syndicat, l'utilisateur doit en obtenir l'accord auprès du Directeur du Syndicat.

Tout utilisateur est identifié nominativement et accède à l'aide de moyens d'accès (login / mot de passe) qui lui sont délivrés personnellement en tenant compte de sa fonction. Les accès aux traitements nécessitent une authentification fiable des utilisateurs. Des profils d'habilitation définissent les données et les fonctionnalités accessibles en fonction de ces utilisateurs.

Il convient également de réaliser une revue des accès (nouvelle demande ou suppression) en cas d'évolution des besoins, de changement d'affectation ou de changement de service.

Le Service Informatique peut également être amené à valider l'accord final en cas de présomption de risque particulier.

Article 3.5 Mots de passe

Chaque utilisateur dispose d'un compte individuel auquel il accède en utilisant un identifiant et un mot de passe. Ce mot de passe est personnel à l'utilisateur et doit être gardé confidentiel. Ces paramètres doivent être mémorisés par l'utilisateur et ne doivent 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.

La politique de complexité et de renouvellement du mot de passe est définie par le service informatique et ne peut pas être soumise à exception. De la même manière, toute nouvelle règle de sécurité du Service informatique s'imposera à l'utilisateur.

L'utilisateur doit verrouiller son ordinateur lorsqu'il quitte ou s'éloigne de son poste de travail. En fin de journée, l'utilisateur doit l'éteindre.

Lorsqu'il utilise un autre ordinateur ou équipement pour accéder à certaines applications ou environnements du Syndicat (Connexion VPN à distance…, l'utilisateur doit prendre soin de se déconnecter et refuser l'enregistrement de ses identifiants par le navigateur afin d'éviter toute utilisation par un tiers.

Si l'utilisateur a connaissance ou suspecte une perte de confidentialité de son mot de passe, il s'engage à le modifier dans les plus brefs délais par le biais du service informatique si nécessaire.

Envoyé en préfecture le 27/06/2025
Reçu en préfecture le 27/06/2025
Publié le
ID : 059-200039386-20250625-2025_12-DE

Article 4 – Règles d'usage du réseau et des espaces de stockage

L'utilisateur peut enregistrer ses données sur plusieurs répertoires :

- Sur le disque dur de l'ordinateur.

  - Il est fortement déconseillé d'y enregistrer ses données professionnelles, notamment à caractère personnel ou sensible, qui risquent d'être perdues ou divulguées en cas de changement de poste, de panne, de perte ou de vol.
  - Des documents personnels peuvent toutefois y être enregistrés, à condition de ne pas pénaliser le bon fonctionnement de l'ordinateur, mais leur sauvegarde reste sous l'entière responsabilité de l'utilisateur.

- Sur le lecteur professionnel individuel One Drive

  - Sur ce lecteur, il est déconseillé de stocker des données destinées à être partagées avec les différents services du Syndicat.

- Sur le lecteur professionnel commun One Drive La Fibre Numérique 59/62

L'utilisateur s'interdit notamment de :

Stocker ou diffuser des documents, informations, images ou vidéos illicites, ou à caractère violent, injurieux, diffamatoire, pornographique, raciste, contraire aux bonnes mœurs ou susceptibles de porter atteinte au respect de la personne humaine, de sa dignité, ainsi qu'à la protection des mineurs, portant atteinte à l'image du Syndicat à l'obligation de réserve, de discrétion ou de secret professionnel, portant atteinte à la vie privée ou au droit à l'image ou protégés par les lois sur la propriété intellectuelle, à des fins de harcèlement, injures, diffamation ou menaces, à des fins de piratage, copie de logiciels, CD, DVD ou tout autre support

-Modifier ou détruire intentionnellement les informations sur un des systèmes connectés au réseau.

-Interrompre le fonctionnement normal du réseau ou l'un des systèmes connectés au réseau,

-Tenter de lire, copier, divulguer ou modifier les fichiers d'un autre utilisateur sans y avoir été explicitement autorisé, même si ces données ne sont pas protégées.

- Prendre connaissance d'informations détenues par d'autres quand bien même ceux-ci ne les auraient pas protégées,

- Masquer sa véritable identité,

- S'approprier le mot de passe d'un autre utilisateur.

- Tenter d'intercepter des communications entre tiers,

- Porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants,

- Divulguer par le biais de moyens informatiques des informations pouvant porter préjudice au Syndicat ou à des tiers.

- Procéder à la diffusion large de messages non professionnels (par exemple : petites annonces),

- Diffuser des documents internes à l'extérieur sans autorisation.

L'utilisateur doit :

- Signaler toute tentative de violation de son compte et toute anomalie constatée,

- Terminer proprement ses sessions de travail et ne pas quitter son terminal ou son ordinateur avec une session en cours,

- Éviter l'utilisation de périphériques externes de stockage (ex : clé USB) afin de limiter les risques d'infection virale et de perte de données. Le cas échéant, il convient de réserver cette utilisation à des fins professionnelles, pour des besoins ponctuels, en s'assurant au préalable que le périphérique ne présente pas de risques pour le Système d'Information, et ne pas y stocker de données sensibles, confidentielles et/ou à caractère personnel sans mesure de protection particulière.

Article 5 – Règles d'usage de la messagerie électronique

Article 5.1Principes généraux

Un courrier électronique est un écrit qui engage personnellement son auteur et l'institution qu'il représente.

Chaque agent dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie se présentant sous la forme : prenom.nom@lafibrenumerique5962.fr.

Le courrier électronique ne dispense pas du respect des procédures administratives. La rapidité de transmission permise par la messagerie engendre une rapidité de réponse.

Article 5.2 Protection contre les courriers électroniques indésirables (spams)

Afin d'éviter l'afflux massif de courriers électroniques indésirables (spams) dans les boîtes aux lettres, un logiciel anti-spam a été mis en place. Il est nécessaire de consulter les messages jugés comme spam par le logiciel afin d'éviter certaines erreurs. En effet, si un mail professionnel a été jugé indésirable par le logiciel, vous pouvez le consulter et informer le logiciel qu'il s'agit d'un courrier légitime.

D'une manière générale, il ne faut jamais ouvrir les contenus transmis par des expéditeurs inconnus et non identifiés, dont les objets sont sibyllins ou n'ayant aucun rapport avec votre activité et dont le format (.zip, .rar, .doc, …) et le nom ne correspondent pas à des documents que vous avez sollicités à l'un de vos interlocuteurs.

Article 5.3 Accès à la messagerie professionnelle depuis un terminal mobile personnel

L'accès à la messagerie professionnelle et à l'agenda depuis un terminal mobile personnel est autorisé. Toutefois, l'utilisateur doit prendre toutes les précautions utiles afin d'empêcher que des tiers non autorisés puissent y accéder notamment en cas de perte ou de vol de l'équipement (protection par code PIN ou mot de passe robuste, effacement à distance, …).

Article 6 – Règles d'usage d'internet

L'accès Internet mis à disposition par le Syndicat doit être utilisé dans le respect des principes figurant dans l'article 3-1 (Utilisation professionnelle des moyens informatiques).

L'usage d'espaces de stockage ou de plateformes d'échange sur Internet (ex : Google Drive,

Dropbox, Wetransfer …) est fortement déconseillé et reste sous l'entière responsabilité de l'utilisateur.

Le respect de la confidentialité des fichiers stockés n'est absolument pas garanti et le service informatique ne peut assurer la sécurité et la fiabilité de ces services. Y stocker ou transférer des

fichiers confidentiels, sensibles ou comportant des données à caractère personnel est totalement interdit.

L'installation d'un accès internet personnel au sein de la collectivité et la mise en place de liaisons par les agents à partir de la collectivité vers une machine non- professionnelle sont interdits.

Les agents, disposent pour l'exercice de leurs missions, d'un accès aux réseaux sociaux et autres forums de discussion. L'usage des réseaux sociaux et autres forums de discussion est soumis au devoir de réserve. Dans tous les cas, l'utilisateur a l'obligation de veiller à respecter les règles de confidentialité, de bonne conduite, de politesse et de courtoisie. Il est rappelé aux utilisateurs que les messages qui y sont diffusés relèvent de leur responsabilité et qu'il leur appartient donc de contrôler leur contenu.

Article 7 - Règles d'usage liées au télétravail et à la mobilité

Lors des déplacements et des utilisations à distance, une vigilance particulière doit être apportée par les utilisateurs afin de limiter tout risque de vol, de perte ou de dégradation des équipements informatiques.

Lors de l'utilisation des équipements nomades (pc portable, tablettes, smartphone), les accès à Internet doivent s'effectuer depuis des réseaux de confiance (éviter notamment les réseaux wifi publics).

Il est à noter que les modalités de mise en œuvre du télétravail au sein du syndicat sont précisées au sein d'une charte spécifique.

Par ailleurs lors de la remise d'un équipement mobile (tablette, smartphone), l'utilisateur signe un engagement lié à la remise du matériel.

Article 8 – Fermeture des accès et restitution

Lors du départ d'un agent (démission, licenciement, retraite, …), ses références sont désactivées de l'annuaire informatique à la date effective communiquée par la DRH.

Tout utilisateur, doit préalablement à son départ, supprimer ses éventuelles données personnelles et transférer ses données professionnelles sur le Sharepoint La Fibre Numérique

Avant son départ, les matériels et accessoires attribués à l'agent pour l'exercice de sa mission doivent être restitués au service Informatique ou à sa hiérarchie.

Quel que soit le cas, la désactivation du compte dans l'annuaire informatique entraine automatiquement la suppression des accès (réseau informatique, boîte aux lettres de messagerie, …).

Les données stockées sur les répertoires locaux seront supprimées, et non sauvegardées.

Article 9 – Règles d'utilisation des données à caractère personnel (RGPD)

Dans le cadre de ses missions et pour mener à bien ses différentes activités, le Syndicat collecte et traite des Données à Caractère Personnel concernant notamment les agents et les partenaires….

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement (ex : nom, prénom, adresse, numéro de téléphone, adresse de messagerie, numéro identifiant, etc.).

Ces traitements répondent à des règles et obligations, en lien avec la réglementation française et européenne (Loi Informatique et Libertés, Règlement Général sur la Protection des Données - RGPD), que chaque agent doit respecter au quotidien.

L'obligation légale à laquelle est soumise le responsable de traitements au sens de l'article 6-c du RGPD

Dans ce cadre, il est rappelé que chaque traitement de données à caractère personnel doit notamment répondre aux obligations suivantes :

- Les finalités doivent être déterminées, explicites et légitimes, et les données ne peuvent pas être traitées à d'autres fins ;

- Le traitement doit être déclaré et intégré au registre de la collectivité, en se rapprochant du Délégué à la Protection des Données ;

- Les données collectées doivent être adéquates, pertinentes et limitées au strict nécessaire (minimisation des données) ;

- Les personnes concernées doivent être informées, et donner leur consentement le cas échéant ;

- Les données doivent être conservées uniquement pendant la durée nécessaire aux finalités, en prenant en compte les durées de conservation légales le cas échéant ;

- Les mesures techniques et organisationnelles doivent être mises en place pour garantir la sécurité des données et limiter ainsi tout risque de divulgation, de perte de données ou de modification non souhaitée ;

- Les données à caractère personnel sensibles (opinions philosophiques, politiques, religieuses, syndicales, origines raciales ou ethniques, relatives à la santé ou à la vie sexuelle, infractions, condamnations, mesures de sécurité) et des données perçues comme sensibles (numéro de sécurité sociale, appréciation sur les difficultés sociales, données biométriques, données bancaires) doivent faire l'objet de mesures spécifiques au vu de leur sensibilité : respect du cadre juridique et renforcement des mesures de sécurité.

Il est également à noter que les personnes concernées par un traitement de données disposent d'un droit d'accès, de rectification, de limitation des informations qui les concernent, et peuvent, pour des motifs légitimes, s'opposer au traitement des données, sauf si ce droit a été écarté par une disposition législative.

Tout incident relatif à la protection des données à caractère personnel doit être déclaré dans les plus brefs délais auprès du Délégué à la Protection des Données (CDG59) afin de respecter l'obligation de notification à la CNIL (Commission Nationale de l'Informatique et des Libertés) dans les 72h.

Les règles d'utilisation des données à caractère personnel sont précisées dans un document dédié au RGPD disponible en annexe de la présente charte.

Article 10 – Droit à la déconnexion numérique

Le Syndicat Mixte La Fibre Numérique 59 62 souhaite souligner l'importance du bon usage des moyens de communication au sein de la structure dans le respect des temps de repos et de congés ainsi qu'en prenant en compte l'équilibre entre la vie privée et la vie professionnelle.

Ainsi, l'usage de la messagerie électronique professionnelle et du téléphone sont à éviter le week-end, les jours fériés, pendant les congés et en dehors des horaires de travail, et doivent être justifiés par la gravité, l'urgence ou l'importance du sujet concerné ou les sujétions auxquels sont soumis certains agents (astreintes, permanences).

Autant que faire se peut, les agents en activité peuvent différer l'envoi des mails aux agents en congés par l'intermédiaire de l'outil proposée par la messagerie.

III – CONTROLE DE L'UTILISATION DES MOYENS INFORMATIQUES

Article 11 – Contrôles de sécurité

Pour des raisons liées à la sécurité, au bon fonctionnement des moyens informatiques et du réseau, et pour s'assurer du respect des règles décrites dans la présente charte, le syndicat se réserve le droit d'effectuer des contrôles de l'utilisation des moyens informatiques.

Ces contrôles sont effectués par le service informatique dans le respect des dispositions légales applicables, en particulier dans le strict respect des dispositions relatives au droit au respect de la vie privée et au secret des correspondances.

Principe de traçabilité : Certains accès sont sécurisés par une étape d'identification et d'authentification de l'Utilisateur, qui doit fournir son couple d'identifiant et mot de passe. Ce contrôle d'accès permet à chaque connexion de l'Utilisateur, l'attribution de droits et privilèges propres définis en considération stricte des besoins du poste qu'il occupe (ci-après le « compte Utilisateur »).

D'une manière générale, l'Utilisateur admet que toute connexion permet son identification et qu'elle constitue une acceptation implicite de l'enregistrement automatique de traces de son activité. En cas de détection de menaces informatiques ou de pratiques non conformes à la présente charte et ses annexes, des actions préventives ou correctives pourront être menées et des mesures pourront être prises conformément au paragraphe IV - Non-respect de la charte.

D'une manière générale, l'Utilisateur admet que toute connexion permet son identification et qu'elle constitue une acceptation implicite de l'enregistrement automatique de traces de son activité.

Article 11.1 Principes généraux sur les pouvoirs et limites d'intervention des administrateurs de systèmes, réseaux et ressources

Le service informatique peut être conduit par ses fonctions à avoir accès à des informations professionnelles et/ou personnelles relatives aux utilisateurs, y compris celles stockées sur les ordinateurs.

Ils ne doivent cependant pas divulguer les informations dont ils auraient eu connaissance dans le cadre de leur mission, en particulier lorsque ces informations sont couvertes par le secret des correspondances ou ont trait à la vie privée de l'agent, dès lors que ces informations ne présentent pas un risque particulier pour le syndicat.

D'une manière générale, le service informatique a un devoir d'alerte de la hiérarchie lorsqu'il constate un incident de sécurité ou qu'un utilisateur ne se conforme pas aux dispositions de la présente charte.

Article 12 – Définition de la notion de données personnelles

Tout fichier ou document stocké sur l'ordinateur, ou tout courrier électronique qui n'est pas identifié comme personnel est réputé professionnel, de sorte que l'employeur peut y accéder librement hors de la présence de l'utilisateur.

Il appartient en conséquence aux utilisateurs d'identifier les fichiers, documents ou courriers électroniques personnels en inscrivant la mention « PERSONNEL » ou « PRIVE ». L'agent ne peut qualifier des informations professionnelles en informations personnelles.

Les fichiers et courriers ne seront pas considérés comme personnels du simple fait de leur classement dans le répertoire « mes documents », dans un dossier identifié par les initiales de l'agent ou dans un fichier d'archives personnelles de la messagerie par exemple.

Article 13 – Conditions d'accès aux fichiers contenant des données personnelles

Conformément aux recommandations de la CNIL et à la jurisprudence en vigueur, le service informatique peut activer des moyens informatiques lui permettant d'accéder aux fichiers identifiés comme personnels :

- Si l'autorité judiciaire l'exige même en dehors de la présence de l'agent ;

- Sur requête de la Direction écrite et motivée notamment par des impératifs de sécurité du Système d'Information. Dans ce cas, cet accès sera réalisé en présence de l'utilisateur ou après l'avoir invité à être présent, ou hors de sa présence en cas de risques extrêmement graves pour le syndicat ou de situations sanctionnées sur le plan pénal : menaces terroristes, pédophilie, proxénétisme, etc.

Article 14 - Conditions d'accès aux courriels comportant des données personnelles

Conformément aux recommandations de la CNIL et à la jurisprudence en vigueur, le service informatique peut, uniquement si l'autorité judiciaire l'exige, activer des moyens informatiques lui permettant d'accéder aux courriels identifiés comme personnels.

Article 15 – Principe général de droit d'accès aux données professionnelles

Les outils informatiques sont des outils mis à disposition des utilisateurs pour leurs besoins professionnels. L'ensemble des données professionnelles d'un utilisateur doit donc par principe être accessible à ses collègues et/ou son ou ses supérieurs hiérarchiques.

Les messages électroniques et les fichiers qui ne sont pas identifiés comme éléments personnels selon les conditions décrites à l'article 12, sont présumés avoir un caractère professionnel de sorte que le syndicat peut y avoir accès et les ouvrir hors de la présence de l'agent.

Article 16 – Règles applicables en cas d'absence prolongée

La notion d'absence prolongée est appréciée au cas par cas au regard des fonctions de l'agent et de la nécessité d'assurer la continuité de service.

Lorsque l'accès aux informations détenues par l'utilisateur en absence prolongée, sur son poste informatique, à ses fichiers ou à sa messagerie électronique est nécessaire à la poursuite des activités du syndicat et que ces informations ne peuvent pas être obtenues par un autre moyen, il appartient à l'utilisateur, s'il en est d'accord, de communiquer son mot de passe à son supérieur hiérarchique ou à une personne de son choix au sein du service. Celui-ci se doit d'en faire une utilisation loyale dans le respect de la vie privée et du secret des correspondances. L'utilisateur absent devra en être informé et modifier son mot de passe à son retour.

En cas de désaccord ou si l'utilisateur n'est pas en capacité de donner son accord, le service informatique pourra procéder à la réinitialisation du mot de passe de l'utilisateur après réception d'une demande motivée écrite du supérieur hiérarchique. Celle-ci devra notamment stipuler le caractère de continuité de service et les démarches infructueuses entreprises auprès de l'utilisateur concerné, et devra comporter l'avis de la Direction du Syndicat. L'utilisateur absent devra en être informé par son supérieur hiérarchique et modifier son mot de passe à son retour.

En cas de décès, une demande d'accès aux fichiers et messages professionnels pourra être réalisée par le supérieur hiérarchique auprès du service informatique en précisant le caractère de continuité de service.

Les fichiers ou messages qui sont identifiés comme personnels ne doivent pas être consultés par l'utilisateur mandataire ou le supérieur hiérarchique.

En cas de non-respect avéré des principes énoncés au présent article par un supérieur hiérarchique, celui-ci s'expose à des sanctions disciplinaires. En cas de détection d'accès aux fichiers d'un agent ou à sa messagerie pendant son absence, le service informatique saisira la hiérarchie qui prendra les mesures nécessaires.

Il convient de rappeler que si le viol du secret des correspondances est susceptible d'être sanctionné par l'administration en ce qu'il constitue une faute disciplinaire, il constitue également une infraction pénale, définie comme un délit pénal par l'article 226-15 du Code Pénal. La sanction est d'autant plus lourde que le délit est commis par une personne dépositaire de l'autorité, comme un supérieur hiérarchique notamment.

Lorsque l'absence de l'agent est prévue (notamment pour congé annuel), il est fortement recommandé que l'utilisateur active le gestionnaire d'absence de sa messagerie électronique et s'assure de l'accessibilité des documents professionnels nécessaires au bon fonctionnement du syndicat afin d'éviter toute demande de communication de son mot de passe pendant son absence.

Le message d'absence devra notamment faire apparaître la durée de l'absence ainsi que le(s) nom(s) du ou des collègues au(x)quel(s) il convient de s'adresser en son absence.

IV – NON RESPECT DE LA CHARTE

En cas d'utilisation non conforme aux principes figurant dans la présente charte et ses annexes, constatée notamment par le supérieur hiérarchique ou le service informatique dans le cadre des opérations de contrôle et d'assistance, différentes mesures pourront être prises, en fonction des circonstances et de la gravité des faits. Notamment :

- Rappel des bonnes pratiques auprès de l'utilisateur concerné et le cas échéant information de son supérieur hiérarchique et/ou alerte de la Direction des Ressources Humaines ;

- Mesures conservatoires, telles que la suppression de droits d'accès (accès Internet, répertoires réseaux, applications, etc.) ;

- Mesures disciplinaires.

- Engage la responsabilité civile et administrative de l'employeur qui peut être condamné à indemniser la victime du préjudice causé par l'indiscrétion.

- Constitue pour le professionnel une faute susceptible de sanction disciplinaire pouvant aller jusqu'au licenciement. Ce manquement seul ne saurait en revanche faire l'objet de poursuites pénales de son auteur, sauf dépôt de plainte pour conséquences graves dont il appartiendra aux juges d'apprécier la pertinence.

En cas de réquisition judiciaire ou sur demande de la Direction, le service informatique procédera ou fera procéder à la recherche d'éléments de preuve.

La violation des dispositions de cette charte peut constituer une faute susceptible d'entraîner des sanctions disciplinaires et / ou d'engager la responsabilité civile et pénale de celui qui commet cette violation.

Elle s'applique dès sa signature par l'agent.

V - ENTREE EN VIGUEUR ET DUREE DE LA CHARTE

Article 17 – Entrée en vigueur, durée et révision

Etablie pour une durée indéterminée, la présente charte peut être modifiée selon les mêmes formalités que celles respectées pour son entrée en vigueur.

Article 18 – Diffusion de la charte, publicité et opposabilité

La présente charte est portée à la connaissance des utilisateurs par tous moyens jugés adéquats par le syndicat. Constitue notamment un moyen adéquat et suffisant l'un des moyens suivants : Note de service ou notification via la messagerie électronique

Envoyé en préfecture le 27/06/2025
Reçu en préfecture le 27/06/2025
Publié le
ID : 059-200039386-20250625-2025_12-DE

ANNEXE 1: RGPD

Dans le cadre de ses missions, le Syndicat peut être amené à collecter et traiter des Données à Caractère Personnel (DCP).

Constitue une donnée personnelle toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement. Ces traitements répondent à des règles et obligations que chaque agent doit respecter au quotidien.

Article 5 du RGPD - Principes relatifs au traitement des données à caractère personnel :

Les données à caractère personnel doivent être :

- Traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;

- Collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités) ;

- Adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;

- Exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ;

- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

- Traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ;

Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).

Collecte des données à caractère personnel (DCP)

Tout traitement de DCP doit respecter les législations et réglementations françaises et européennes en vigueur notamment la loi du 6 janvier 1978 Informatique et Liberté modifiée et le Règlement Général sur la Protection des données.

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.

Traitements de données 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, origines raciales ou ethniques, relatives à la santé ou à la vie sexuelle ; 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 du Délégué à la Protection des Données (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. Seule la conservation de ces pièces selon la politique d'archivage en vigueur et/ou 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.

- S'assurer que la protection des données est bien assurée (notamment lors de leur stockage et de leur transfert) et alerter la DPD en cas de violation de ces données.

L'agent s'engage à :

- Vérifier que le traitement est déclaré dans le registre ou à se rapprocher du DPD en cas de doute.

- 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.

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 (ex : Excel, 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.

Archivage ou suppression des données

La conservation de données des agents est soumise à des obligations légales qui Imposent une suppression ou un archivage de celles-ci dans les délais prévus par la loi ou par les règles d'archivage.

L'agent doit appliquer les durées légales de conservation des données des administrés qu'il est amené à traiter. Il doit également respecter les procédures en vigueur relatives à l'archivage ou à la purge des données.

Lorsque les données ne sont pas soumises à une obligation d'archivage, 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.

Sanctions

Le non-respect des obligations RGPD peut entrainer pour le Syndicat des sanctions pouvant s'élever à 20 000 000 d'euros. Le montant des amendes sera variable selon la nature, la gravité et

la durée de la violation et compte tenu de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes affectées et le niveau de dommage qu'elles ont subi. Le degré de responsabilité du responsable de traitement ou du sous-traitant est également pris en compte ainsi que les différentes mesures techniques et organisationnelles déjà mises en place pour assurer la conformité de l'institution.

Code pénal (Partie Législative) - Art. 226-16 :

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 3° du III de l'article 20 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

ANNEXE 2: Charte de bon usage - Mobilité numérique

L'emploi de tablettes tactiles, téléphones mobiles, d'ordinateurs portables et d'assistants personnels favorise le transport et l'échange d'informations.

Quelles sont les informations concernées ?

Que ce soit dans un contexte personnel ou professionnel, de plus en plus de contenus numériques sont conservés sur ces terminaux.

Parmi ces informations, certaines peuvent présenter une sensibilité importante (contacts, agendas, mails, pièces jointes, fichiers, photos, vidéos, SMS, historique des appels, boîte vocale, données des applications métiers, …) tant pour les utilisateurs que pour le syndicat.

Les utilisateurs ont par ailleurs recours à un nombre croissant de services connectés à Internet, qu'il s'agisse des messageries électroniques, des réseaux sociaux ou des banques en ligne.

Quels sont les risques pour les utilisateurs de terminaux mobiles ?

Tous les jours des appareils sont perdus ou volés. Les informations qui y sont stockées peuvent être récupérées et exploitées par une autre personne, notamment à des fins d'usurpation d'identité et avoir des conséquences importantes voir catastrophiques pour les utilisateurs ou le syndicat.

Il existe un vol d'informations personnelles (localisation, mails, contacts, pièces jointes, …) si l'utilisateur installe des applications malveillantes qui accèdent aux données du téléphone ou de la tablette.

Par ailleurs, en dehors de la connexion au réseau wifi du syndicat, l'accès à Internet depuis les terminaux mobiles ne dispose pas de filtrage lié aux sites consultés. Cet accès direct à Internet présente certains risques auxquels l'utilisateur doit être sensible afin de limiter tout incident : accès ou redirection à l'insu de l'utilisateur vers des sites aux contenus douteux (infectés par un virus, contraires à l'ordre public ou aux bonnes mœurs, …) ou même totalement illicites et pénalement répréhensibles.

Ces types de sites peuvent être gérés par des personnes malveillantes (pirates) à l'affût de toute connexion leur permettant d'infiltrer notre réseau informatique interne. Ils sont également sous la surveillance des autorités publiques dont les brigades spécialisées peuvent identifier les utilisateurs s'y étant connectés et mettre en cause le syndicat

Face à ces risques, comment se prémunir ?

- Ne pas laisser son terminal mobile sans surveillance ou à des personnes non habilitées,

- Ne pas débrider (jailbreak, rooting, …) le système d'exploitation sachant qu'un contrôle de conformité est réalisé,

- Ne pas installer des applications qui ne sont pas de sources officielles,

- Lire attentivement les conditions générales d'utilisation des applications avant leur installation, et ajuster les restrictions d'accès des applications installées afin d'éviter toute fuite d'information ou accès non souhaité (accès à la liste des contacts, appareil photo, micro, localisation, etc.),

- Définir des mots de passe comportant un certain degré de complexité (en évitant les mots de passe « évidents ») et ne pas les diffuser ou les inscrire sur quelque support que ce soit,

- Installer régulièrement les mises à jour et autres correctifs de sécurité officiels proposés par les éditeurs,

- Ne pas utiliser de services de stockage des données sur Internet pour lesquels la sécurité ne peut être garantie,

- Il est également rappelé que l'utilisateur d'internet s'interdit notamment de télécharger, stocker, diffuser, distribuer, d'accéder à des serveurs web, des documents, informations, images ou vidéos

illicites, ou à caractère violent, diffamatoire, pornographique, religieux, sectaire, raciste, contraire aux bonnes mœurs ou susceptibles de porter atteinte au respect de la personne humaine, de sa dignité, ainsi qu'à la protection des mineurs, portant atteinte à l'image du syndicat, à l'obligation de réserve, de discrétion ou de secret professionnel, portant atteinte à la vie privée ou au droit à l'image, protégés par les lois sur la propriété intellectuelle, à des fins de harcèlement, injures, diffamation ou menaces, à des fins de piratage, copie de logiciels, CD, DVD ou tout autre support

L'ensemble des règles décrites dans la charte de bon usage des moyens informatiques restent applicables.

En cas de perte ou de vol

En cas de perte ou de vol, il est nécessaire d'informer immédiatement son responsable ainsi que le service informatique

Il est également demandé de changer obligatoirement et au plus vite les mots de passe, pour limiter tout risque d'intrusion ou d'usurpation d'identité.