CHARTE INFORMATIQUE

Conformément à la législation en vigueur, la présente politique de confidentialité et de traitement des données personnelles, définie dans cette charte, vise à informer tous les utilisateurs de la manière dont la fédération Trisomie 21 France traite, protège et conserve les informations collectées que les salariés et bénévoles utilisent dans le cadre de leurs missions.

La fédération T21 France accorde une vigilance toute particulière au respect de la vie privée des personnes comme à celle des utilisateurs et de leurs données personnelles. A ce titre, la fédération Trisomie 21 France s'engage à respecter scrupuleusement :

- La Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (loi informatique et liberté)
- Le Règlement de l'Union Européenne 2016/679 du 27 avril 2016 dit Règlement Général sur la Protection des Données, (RGPD), est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel.
- La loi n° 2018- 493 du 20 juin 2018 relative à la protection des données à Caractère personnel
- Le décret 2018-687 pris en application de la loi CNIL 3
- Les Délibérations CNIL n° 2018-327 et 2018-328 du 11 octobre 2018 relatives aux analyses d'impact
- L'ordonnance 2018-1125 du 12 décembre 2018.
- Les recommandations de la CNIL (Commission Nationale Informatique et Liberté)

La politique de confidentialité et de traitement des données de la fédération fera l'objet d'adaptations afin de rester conforme aux évolutions législatives, règlementaires, jurisprudentielles ou technologiques.

PRÉAMBULE

La Fédération Trisomie 21 France met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique, ainsi que des outils mobiles que les salariés, dans l'exercice de leurs fonctions, sont conduits à utiliser.

L'utilisation du système d'information et de communication doit se faire exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte. Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information et de communication, la présente charte pose les règles relatives à l'utilisation de ces ressources. Elle définit aussi les moyens de contrôle et de surveillance de cette utilisation mise en place, non seulement pour la bonne exécution du contrat de travail des salariés, mais aussi dans le cadre de la responsabilité pénale et civile de l'employeur. Elle dispose d'un aspect réglementaire et est annexée au règlement intérieur de la Fédération Trisomie 21 France. Elle ne remplace en aucun cas les lois en vigueur que chacun est censé connaître.

La présente charte constitue une adjonction au règlement intérieur de la Fédération, au sens de l'Article L.1321-5 du Code du Travail.

DÉFINITIONS

La charte rappelle les définitions suivantes établies par la CNIL :

Donnée personnelle[1] :

« *Toute information identifiant directement ou indirectement une personne physique (ex. nom, n° d'immatriculation, n° de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale...)* ».

Donnée sensible[2] :

« *Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. Le Règlement européen interdit de recueillir ou d'utiliser ces données, sauf dans certains cas :*

- *Si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée),*
- *Si les informations sont rendues publiques par la personne concernée,*

[1] https://www.cnil.fr/fr/definition/donnee-personnelle
[2] https://www.cnil.fr/fr/definition/donnee-sensible

- *Si elles sont nécessaires à la sauvegarde de la vie humaine,*
- *Si leur utilisation est justifiée par l'intérêt public et autorisé par la CNIL,*
- *Si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.* »

Traitement des données à caractère personnel[3] :

« *Toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, ...)* »

Délégué à la protection des données (DPD)[4] :

« Le délégué à la protection des données (DPD) est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.

Sa désignation est obligatoire dans certains cas. Un délégué, interne ou externe, peut être désigné pour plusieurs organismes sous conditions. Pour garantir l'effectivité de ses missions, le délégué doit disposer de qualités professionnelles et de connaissances spécifiques et doit bénéficier de moyens matériels et organisationnels, des ressources et du positionnement lui permettant d'exercer ses missions. »

Ainsi, le délégué, nommé au sein de la Fédération s'apparente à une fonction externe pour les associations fédérées.

Le DPD est obligatoire pour les organismes et les entreprises publiques, et les entreprises dont le traitement des données est suffisamment spécifique pour justifier le recrutement de cette fonction. Plus exactement, selon l'article 37 du RGPD, il est nécessaire de recruter un DPD dans les cas suivants :

- Lorsque la gestion des données personnelles exige un suivi régulier et systématique à grande échelle des personnes concernées, il ne s'agit pas que de volume mais également de durée ou d'étendue géographique
- Lorsqu'il s'agit d'un traitement à grande échelle de données dites « sensibles » (données de santé, données biométriques, opinions politiques, convictions religieuses…) et de données à caractère personnel relatives à des condamnations pénales et à des infractions
- Dans tous les cas, il s'avère nécessaire de désigner un pilote pour la gestion des données personnelles au sein des associations compte tenu de la nature des données qu'elles manipulent. Ce pilote est désigné par l'association en tant que référent territorial du DPD national.

[3] https://www.cnil.fr/fr/definition/traitement-de-donnees-caractere-personnel
[4] https://www.cnil.fr/fr/definition/delegue-protection-donnees

Droit à l'information[5] :

« *Toute personne a un droit de regard sur ses propres données ; par conséquent, quiconque met en œuvre un fichier ou un traitement de données personnelles est obligé d'informer les personnes fichées de son identité, de l'objectif de la collecte d'informations et de son caractère obligatoire ou facultatif, des destinataires des informations, des droits reconnus à la personne, des éventuels transferts de données vers un pays hors de l'Union européenne.* »

Droit d'accès[6] :

« *Toute personne peut prendre connaissance de l'intégralité des données la concernant dans un fichier en s'adressant directement à ceux qui les détiennent, et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction.* »

Droit de rectification[7] :

« *Toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations la concernant lorsqu'ont été décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.* »

Sanction[8] :

« *A l'issue de contrôle ou de plaintes, en cas de méconnaissance des dispositions du RGPD ou de la loi de la part des responsables de traitement et des sous-traitants, la formation restreinte de la CNIL peut prononcer des sanctions à l'égard des responsables de traitements qui ne respecteraient pas ces textes.*
Avec le RGPD (Règlement Général sur la Protection des Données), le montant des sanctions pécuniaires peut s'élever jusqu'à 20 millions d'euros ou dans le cas d'une entreprise jusqu'à 4 % du chiffre d'affaires annuel mondial. Ces sanctions peuvent être rendues publiques.

Lorsque des manquements au RGPD ou à la loi sont portés à sa connaissance, la formation restreinte de la CNIL peut :

- *Prononcer un rappel à l'ordre ;*
- *Enjoindre de mettre le traitement en conformité, y compris sous astreinte ;*
- *Limiter temporairement ou définitivement un traitement ;*
- *Suspendre les flux de données ;*
- *Ordonner de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte ;*
- *Prononcer une amende administrative.* »

---

[5] https://www.cnil.fr/fr/definition/droit-linformation
[6] https://www.cnil.fr/fr/definition/droit-dacces
[7] https://www.cnil.fr/fr/definition/droit-de-rectification
[8] https://www.cnil.fr/fr/definition/sanction

ARTICLE 1 : CHAMP D'APPLICATION

1.1 Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication de la fédération, quel que soit leur statut, administrateurs, salariés en CDI, CDD, intérimaires, stagiaires, prestataires, visiteurs occasionnels. Elle sera annexée aux contrats de prestations.

La Fédération Trisomie 21 France veille à faire accepter valablement les règles posées dans la présente charte à toute personne à laquelle elle permettrait d'accéder au système d'information et de communication.

L'intrusion non autorisée dans le système d'information de la Fédération Trisomie 21 France peut être qualifiée d'infraction conformément à l'Article 323-1 alinéa 1 du Code Pénal[9].

1.2 Système d'information

Le système d'information et de communication de la Fédération est notamment constitué des éléments suivants : ordinateurs (fixes ou portables), périphériques y compris clés USB, assistants personnels, réseau informatique (serveurs, routeurs et connectique), photocopieurs, téléphones, smartphones, tablettes et clés 3G, logiciels, fichiers, données et bases de données, système de messagerie, connexion internet, intranet, extranet, abonnements à des services interactifs.

Les utilisateurs ne sont pas autorisés à modifier, copier les documents support de la Fédération Trisomie 21 France sauf accord de leur hiérarchie ou à installer tout nouveau logiciel.

1.3 Administrateur du système d'information

Le responsable du système d'information de la Fédération Trisomie 21 France veille à la protection, la maintenance au bon fonctionnement du système d'information en lien avec les prestataires de la Fédération T21 France : SociaNova, EIG et XEFI. Il s'assure du respect de la présente charte et de sa concordance avec celle de chacun de nos fournisseurs d'accès. Ils sont soumis au règlement Général de la Protection des Données (RGPD). Il ne peut cependant être tenu responsable de l'utilisation du système d'information et de leur utilisation dans les associations et services.

ARTICLE 2 : CONFIDENTIALITÉ

Chaque utilisateur accède aux outils informatiques et de communication, nécessaires à l'exercice de son activité professionnelle dans les conditions définies par la Fédération T21 France. Ainsi l'accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiant, mot de passe).

[9] 2ans d'emprisonnement et 30 000€ d'amende

2.1 Paramètres d'accès

Ces paramètres sont personnels à l'utilisateur et doivent être gardés **confidentiels.** Ils permettent en particulier de contrôler l'activité des utilisateurs. Ils ne doivent être communiqués, uniquement qu'à l'employeur ou son représentant. Dans la mesure du possible, l'utilisateur mémorise ses paramètres d'authentification et ne doit pas les conserver, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles. À chaque accès, l'utilisateur saisit ses identifiants qui, en aucun cas, ne sont conservés en mémoire dans le système d'information.

La direction élabore des règles de sécurité. Actuellement, le mot de passe comporte 8 caractères minimum combinant chiffres, lettres, majuscules et caractères spéciaux. Il ne doit comporter ni le nom, prénom ni l'identifiant d'ouverture de la session de travail. Pour assurer une sécurité maximum, il devrait être modifié tous les trois mois.

Aucun utilisateur, excepté le responsable du système d'information, ne doit se servir pour accéder au système d'information de la Fédération T21 France d'un autre compte que celui qui lui a été attribué. Il ne doit pas non plus déléguer à un tiers les droits d'utilisation qui lui sont propres.

2.2 Données

Chaque utilisateur est responsable pour ce qui le concerne du respect du secret professionnel et de la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser. Les règles de confidentialité ou d'autorisation préalable avant diffusion externe ou publication sont définies par la direction et applicables quel que soit le support de communication utilisé.

L'utilisateur doit être particulièrement vigilant sur le risque de divulgation de ces informations dans le cadre d'utilisation d'outils informatiques, personnels ou appartenant à la Fédération, dans des lieux autres que ceux de la Fédération (hôtels, lieux publics…).

La loi n° 78-17 du 6 janvier 1978 et le règlement européen sur la protection des données personnelles définissent les conditions dans lesquelles des traitements de données personnelles peuvent être opérés.

2.3 Réseau interne

La fédération T21 France s'est dotée d'un serveur qui permet de sécuriser les données et les dossiers à visée professionnelle constitués par les utilisateurs.

L'utilisation d'autres modalités d'enregistrement constitue un risque de perte de ceux-ci et vont à l'encontre de leur sécurisation.

Il est recommandé d'utiliser le serveur afin de garantir leur sécurisation.

2.4 Internet

Dans le cadre de leur activité, les utilisateurs ont accès à Internet. Pour des raisons de sécurité ou de déontologie, l'accès à certains sites peut être limité ou prohibé par la direction qui est habilitée à imposer des configurations du navigateur et à faire installer des mécanismes de filtrage limitant l'accès à certains sites.

Seule la consultation de sites ayant un rapport avec l'activité professionnelle est autorisée. Il est interdit de se connecter à des sites Internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information ou engageant financièrement celle-ci. L'utilisation d'internet à des fins professionnelles exclut la consultation de certains sites tels que les réseaux sociaux ou forums.

Enfin, le téléchargement même légal de fichiers, multimédias ou autres, est, sauf besoin professionnel, à proscrire. Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer sur Internet à une activité illicite ou portant atteinte aux intérêts de la fédération.

Ils sont informés que le prestataire informatique enregistre leur activité sur Internet et que ces traces pourront être exploitées à des fins de statistiques, de contrôle et de vérification dans les limites prévues par la loi, en particulier en cas de perte importante de bande passante sur le réseau.

2.5 Messagerie

Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique normalisée, attribuée par la direction.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les salariés sont invités à informer la direction et le responsable du système d'information des dysfonctionnements qu'ils constateraient dans ce dispositif de filtrage.

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier postal, il obéit donc aux mêmes règles, en particulier en matière d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer le message, il convient d'en référer à son supérieur.

Un message électronique peut être communiqué très rapidement à des tiers et il convient de 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 la responsabilité civile ou pénale de la Fédération et de l'utilisateur.

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises. En présence d'informations à caractère confidentiel, ces vérifications doivent être renforcées. Pour rappel, il est strictement interdit d'utiliser, à des fins personnelles, toutes données, contenus de messages, documents… appartenant à la Fédération et aux services en gestion directe, de se les transférer sur une boite mail personnelle ou par quelque moyen que ce soit.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent pas comporter d'éléments illicites, tels que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

La forme des messages professionnels doit respecter les règles définies par la direction, pour ce qui concerne la mise en forme et surtout la signature des messages.

En cas d'absence prévisible supérieure à 3 jours, le salarié doit mettre en place un message d'absence comportant le nom du salarié susceptible de traiter la demande.

2.6 Consultation de la messagerie

Les courriels reçus sur la messagerie professionnelle peuvent être consultés par l'employeur, excepté ceux identifiés comme « personnel ». En effet, ces derniers sont protégés par le secret de la correspondance. Ils ne peuvent être ouverts, consultés sans que le salarié soit présent ou dûment informé de cette démarche.

Pour donner un caractère personnel à sa correspondance, le salarié indique de manière explicite que le contenu de son courriel envoyé ou reçu, via sa messagerie professionnelle relève du secret de la correspondance en indiquant : « personnel », « perso », ou « privé ». Utiliser la messagerie professionnelle à des fins personnelles doit relever de l'exception.

Toutefois, ces fichiers, mails… peuvent être consultés par l'employeur s'il existe un risque particulier pour la Fédération et les associations.

Ainsi, tout dossier ou fichier créé, enregistré sur l'ordinateur professionnel est réputé avoir un caractère professionnel, c'est une règle constante. L'employeur peut accéder à ces fichiers, sans que le salarié soit présent. Concernant la messagerie les règles s'apparentent à celles énoncées ci-dessus ; les courriels envoyés et reçus sont consultables puisqu'ils sont réputés comme ayant un caractère professionnel.

En ce qui concerne les identifiants de connexion aux postes de travail et aux applications, ils sont jugés comme étant absolument personnels, cependant le salarié doit communiquer son mot de passe si l'employeur en fait la demande. « Dès lors qu'il s'agit d'un outil professionnel, l'ordinateur doit être accessible à l'employeur, que le salarié soit ou non présent sur le lieu de travail. En effet, les fichiers qui s'y trouvent sont présumés être professionnels puisqu'ils sont hébergés par un outil de travail relevant de la propriété de l'entreprise. L'employeur y a donc légitimement accès ».

2.7 Sanctions

Si un salarié consulte les courriels d'un collègue sans son autorisation ou sans qu'il ait délégation du Président de la Fédération pour le faire, il peut être sanctionné. En effet, son comportement constitue une violation de ses obligations découlant de son contrat de travail. Son attitude doit être regardée comme un manquement à son obligation de loyauté. La sanction disciplinaire peut aller jusqu'au licenciement pour faute grave.

Si un salarié utilise des documents, fichiers, contenus de courriel à des fins personnelles, les transfère sur une boite personnelle, il peut être sanctionné. En effet, son comportement constitue une violation de ses obligations de confidentialité découlant de son contrat de travail et du règlement intérieur. Son attitude doit être regardée comme un manquement à son obligation de loyauté. La sanction disciplinaire peut aller jusqu'au licenciement pour faute grave.

ARTICLE 3 : CONFORMITÉ

La Fédération T21 France s'est entourée de prestataires s'assurant de la sécurisation des données dans des conditions normales d'utilisation.

Elle se conforme aux prescriptions de la CNIL sur le RGPD. Pour ce faire, un correspondant aux données personnelles est nommé, joignable par mail dpd@trisomie21-france.org. Ce correspondant accompagne les associations dans la conformité au règlement RGPD.

ARTICLE 4 : INFORMATION ET SANCTIONS

4.1 Contrôles automatisés

Le système d'information et de communication s'appuie sur des fichiers journaux ("logs"), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information.

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Sont notamment surveillées et conservées les données relatives :

- À l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers
- Aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites ou le téléchargement de fichiers
- Aux appels téléphoniques émis ou reçus à partir des postes fixes ou mobiles pour surveiller le volume d'activités et détecter des dysfonctionnements.

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

Il est précisé que chaque utilisateur pourra avoir accès aux informations enregistrées lors de ces contrôles le concernant sur demande préalable à la direction. De plus, les fichiers journaux énumérés ci-dessus sont automatiquement détruits dans un délai maximum de 6 mois après leur enregistrement.

4.2 Information

La présente charte est affichée publiquement en annexe du règlement intérieur. Elle est communiquée individuellement à chaque salarié par voie électronique. La direction et le responsable SI sont à la disposition des salariés pour leur fournir toute information concernant l'utilisation du système d'information, en particulier sur les procédures de sauvegarde et de filtrage. Elle les informe régulièrement sur l'évolution des limites techniques du système d'information et de communication ainsi que sur les menaces susceptibles de peser sur sa sécurité. Chaque utilisateur doit se conformer aux procédures et règles de sécurité édictées par la direction dans le cadre de la présente charte. En cas de besoin, les salariés pourront être formés par le responsable système d'information pour appliquer les règles d'utilisation du système d'information et de communication prévues.

4.3 Sanctions

Le manquement aux règles et mesures de sécurité décrites dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des sanctions, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires et proportionnées à la gravité des faits concernés. Dans ce dernier cas, les procédures prévues dans le règlement intérieur et dans le Code du travail seront appliquées. L'utilisation reconnue à des fins personnelles de certains services payants à travers le système de communication de l'entreprise donnera également lieu à remboursement de la part de l'utilisateur concerné.

Le Président ou son représentant légal, se réserve également le droit d'engager ou de faire engager des poursuites pénales indépendamment des sanctions disciplinaires mises en œuvre, notamment en cas de fraude informatique, de non-respect des droits d'auteur ou de violation du secret des correspondances.

ARTICLE 5 : RÈGLES DE PUBLICITÉ

La présente charte a été soumise à l'avis :

- Du CSE le 17 décembre 2019
- A l'approbation du conseil d'administration le 29 juin 2019

La charte informatique a été communiquée, accompagnée de cet avis, à Monsieur l'Inspecteur du travail en date du *23 Janvier 2020,* adressé au secrétariat du Conseil des Prud'hommes de *Saint Etienne et de Lille* en date du *23 décembre 2020* et affiché à la même date.

Elle entre en application le *23 Janvier 2020*.

Fait à *Saint Etienne*

Le *17 décembre 2019*