Vandœuvre
LÈS-NANCY

Notice d'information sur le télétravail et la protection des données

Pour permettre à ses agents de télétravailler, la commune de Vandoeuvre déclare un traitement à la CNIL et met à disposition de ses salariés les outils de communication et le matériel informatique nécessaire.
Dans ce cadre, la commune est responsable de la protection des données utilisées :

- La protection de vos données personnelles collectées lors du télétravail.
- La protection des données personnelles des usagers ou tiers que les services sont amenés à utiliser durant les périodes de télétravail.

Finalités-Bases légales et responsabilité du traitement

Le traitement mis en œuvre pour déployer le télétravail à Vandœuvre est placé sous la responsabilité du Maire et juridiquement basé sur l'intérêt légitime, conformément à l'article 6.1.f du Règlement européen (RGPD) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et de la Loi n° 2018-493 du 20 juin 2018 sur la protection des données.

Les agents qui formulent une demande de télétravail sont tenus de communiquer aux services gestionnaires des informations personnelles les concernant. Ces informations font l'objet d'un traitement informatisé destiné au déploiement du télétravail à la Métropole et à assurer le lien avec l'encadrement hiérarchique. En aucun cas ce traitement n'est destiné à contrôler individuellement par appels téléphoniques ou suivi de la connexion informatique l'activité des télétravailleurs.

Données traitées

Conformément au principe de minimisation, seules les données directement indispensables au traitement sont recueillies. Il s'agit des données d'identification de l'agent pour la collectivité, des jours de télétravail demandés, de l'existence d'une assurance (correspondant au formulaire de demande de Télétravail).
A cela s'ajoutent les données de « journalisation », horaires de connexion et traces informatiques correspondantes à vos utilisations du réseau et des logiciels DSIT), en lien avec votre adresse IP (celle fixe de votre ordinateur professionnel et périodique du routeur informatique utilisé sur le lieu de télétravail).
Ces données ne peuvent être utilisées par la collectivité ou la DSIT à des fins de contrôle ou autre.

Dans certains cas un numéro de téléphone privé voire un mail privé pourront être demandés. Pour leur utilisation, il convient de préciser que les responsables hiérarchiques habilités à en disposer (N+1, voire N+2) ne les utiliseront qu'en cas d'urgence, dans le souci de préserver la vie privée de l'agent.

Les données sont conservées dans ce traitement pendant toute la durée de l'engagement à télétravailler. L'agent peut exercer son droit d'accès ou de rectification aux données le concernant (nom, prénom, numéros d'inventaire, adresses mail personnelles ou professionnelles, numéros de téléphones personnels ou professionnels, jour télétravaillé dans la semaine, plages horaire de travail) auprès du service gestionnaire.
Pour toute question sur la légalité de ce traitement, il est possible de joindre la Déléguée à la Protection des Données au 03.57.80.06.57.ou par courriel à cnil@grandnancy.eu.

Précautions de sécurité

L'employeur est responsable de la sécurité des données personnelles de l'ensemble des traitements de la collectivité, y compris lorsque les agents accèdent à ces traitements de façon distante. Cela nécessite pour les agents de redoubler d'attention et de vigilance pour réduire au maximum les risques sur lesquels il est possible d'agir (intrusion, virus, chevaux de Troie…) lors de l'utilisation d'équipement professionnels à la maison.

A son tour, tout agent de la collectivité a l'obligation de protéger les données personnelles des usagers, du public, des partenaires, des associations, entreprises et établissements publics qui interagissent avec la commune de Vandoeuvre.
Le non-respect de cette obligation peut avoir des conséquences importantes pour ces personnes. Il s'agirait d'un manquement à nos obligations. Outre les sanctions administratives, dans les cas les plus graves, la CNIL peut prononcer des sanctions pécuniaires et la justice des sanctions pénales.

Les données personnelles qui nous sont confiées sont protégées :

- Par la seule utilisation des matériels informatiques, des logiciels et des applications validées par la DSIT.
- Par **l'interdiction de sortir tous documents papiers** porteurs de données personnelles. Cela implique l'obligation de les scanner et de les transférer, dans le respect des procédures de la DSIT, sur des outils en réseau protégés si vous devez en disposer à distance. Les supports physiques qui pourraient être facilement égarés sont à proscrire (disque externe, clé USB, carte SD…).
- Par votre bon sens et votre vigilance à respecter les recommandations de sécurité transmises en fin du présent document.

Engagement à respecter le RGPD et les procédures internes associées

Nom : _____

Prénom : _____

Fonction : _____

Service : _____

Nom et Date *(mention obligatoire en clair)* :

Signature

Recommandations de sécurités informatiques

Les recommandations de sécurité pour les télétravailleurs sont préconisées par l'ANSSI (Agence Nationale de Sécurité des Systèmes Informations).
Cette liste de recommandations est adaptée à la collectivité et doit être actualisée régulièrement.

1. Le télétravail est réalisé avec les moyens informatiques professionnels uniquement. Cela garanti la maîtrise des risques informatiques pour la collectivité et la DSIT. Les consignes de sécurité de la DSIT sont à respecter scrupuleusement. En cas de difficulté, d'anomalie, de suspicion ou d'intrusion, l'information doit être immédiatement remontée auprès de la DSIT ou à défaut du service informatique. Les consignes de sécurité induites ne peuvent être contournées.

2. Il est demandé de renforcer la sécurité des mots de passe : mots de passe suffisamment longs, complexes et différents sur tous les équipements et services auxquels la personne accède, qu'ils soient personnels ou professionnels. La majorité des attaques est due à des mots de passe trop simples ou réutilisés. Au moindre doute ou même en prévention, il est nécessaire de les changer. La double authentification doit être privilégiée, chaque fois que cela est possible.
Il est demandé de séparer les usages professionnels et ceux liés à la vie privée résiduelle en utilisant des mots de passe différents pour les uns et pour les autres.

3. Les connexions WiFi doivent être sécurisées : Le télétravail s'opère principalement sur les connexions WiFi personnelles. Il est donc primordial de bien les sécuriser pour éviter toute intrusion sur son réseau qui, au-delà de la problématique personnelle peut aussi permettre d'attaquer la collectivité. Là aussi les mots de passe doivent être suffisamment longs et complexes et la connexion doit être chiffrée en WPA2. Les «box Internet» doivent être remises à jour régulièrement en les redémarrant ou depuis les interfaces d'administration.

4. Le travail doit être sauvegardé régulièrement. La sauvegarde est le seul moyen qui permet de retrouver ses données en cas de cyberattaques, de panne ou de perte de son équipement. Si cela est possible, la sauvegarde réseau est à privilégier, ainsi que les supports externes mis à dispositions que vous débranchez une fois la sauvegarde effectuée (clé ou disque USB).

5. Les messages inattendus ou alarmistes (e-mail, SMS, chat) constituent souvent une attaque par hameçonnage visant à dérober des informations confidentielles (mots de passe). Il faut demander une confirmation à l'émetteur par un autre moyen avant de les ouvrir. De même les applications sont à installer dans un cadre «officiel ». Les sites internet ou frauduleux (téléchargement, vidéo, streaming illégaux) peuvent également piéger vos équipements.