



CHARTRE INFORMATIQUE

Envoyé en préfecture le 26/07/2024

Reçu en préfecture le 26/07/2024

Publié le

ID : 083-218300903-20240722-DEL2024_07_4_4-DE

Les agents et élus sont tenus à des obligations en matière d'utilisation des équipements et logiciels mis à leur disposition dans le cadre de leurs activités professionnelles.

LES OBLIGATIONS ET RESPONSABILITÉS EN MATIÈRE DE SÉCURITÉ INFORMATIQUE

Protéger les données personnelles




Je mets en évidence les données considérées privées, en faisant figurer «< PRIVE >> en tête du nom, des dossiers, et de l'objet des courriels.

Consulter la fiche «Comment protéger les données personnelles ?»

Verrouiller mon ordinateur



Je verrouille mon poste de travail dès que je m'absente afin de protéger mon travail [touches  + L ou Ctrl + Alt + Suppr]

Consulter la fiche «Comment bien utiliser mon ordinateur ?»

Ranger mon bureau



Au bureau, je ne laisse pas mes documents à la vue de tous car je risque d'exposer des informations confidentielles.

Consulter la fiche «Comment obtenir un bureau propre ?»

Stocker mes fichiers sur les serveurs



Je stocke mes données de travail sur les serveurs car ce sont les seuls espaces de stockage sécurisés et sauvegardés.

Consulter la fiche «Comment stocker sur les serveurs ?»

Utiliser uniquement les clés USB autorisées



Je ne connecte que des clés USB fournies par la DSI car je risque d'introduire un virus dans le système informatique.

Consulter la fiche «Comment obtenir une clé USB autorisée ?»

Protéger mes mots de passe



Je garde secrets mes mots de passe parce que je suis responsable de toute action réalisée à partir de mon compte

Consulter la fiche «Comment protéger mon mot de passe ?»

Protéger ma boîte mail



Je ne clique ni sur les liens ni sur les documents joints avant de m'être assuré qu'ils ne sont pas malveillants.

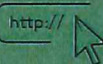
Consulter la fiche «Comment protéger ma boîte mail ?»

Respecter les règles du télétravail



Je suis scrupuleusement les consignes de télétravail pour ne pas exposer d'avantage le système informatique à des attaques.

Consulter la fiche «Comment télétravailler en sécurité ?»



L'utilisation d'internet ne doit pas porter atteinte à la collectivité ni à son bon fonctionnement.

Consulter la fiche «L'utilisation d'Internet»

SANCTIONS DISCIPLINAIRES

Groupe	Sanctions
1er Groupe	<ul style="list-style-type: none">• Avertissement Blâme• Exclusion temporaire de fonctions de 1 à 3 jours
2ème Groupe	<ul style="list-style-type: none">• Radiation du tableau d'avancement• Abaissement d'échelon immédiatement inférieur à celui détenu par le fonctionnaire.• Exclusion temporaire de fonctions de 4 à 15 jours maximum.
3ème Groupe	<ul style="list-style-type: none">• Rétrogradation au grade immédiatement inférieur, à l'échelon comportant un indice égal ou immédiatement inférieur à celui détenu par le fonctionnaire• Exclusion temporaire de fonctions de 16 jours à 2 ans
4ème groupe	<ul style="list-style-type: none">• Mise à la retraite d'office• Révocation

LES RESPONSABILITÉS CIVILES ET PÉNALES.

La négligence, l'imprudence ou la malveillance d'un utilisateur sont de nature à engager sa responsabilité pénale. Conformément à l'article 1240 et suivants du Code civil, la responsabilité civile de l'agent pourra également être engagée.



IMPORTANT

Lorsque l'on quitte son bureau il est important de verrouiller sa session, pour plusieurs raisons de sécurité.

VERROUILLER SON POSTE DE TRAVAIL

Ce qu'il peut se passer lorsque vous ne verrouillez pas votre poste de travail :



N'importe quelle personne ayant accès physiquement à votre poste pourrait **avoir accès facilement aux fichiers qui s'y trouvent, et les récupérer** (documents ouverts en cours, parfois confidentiels ou tout simplement privés)



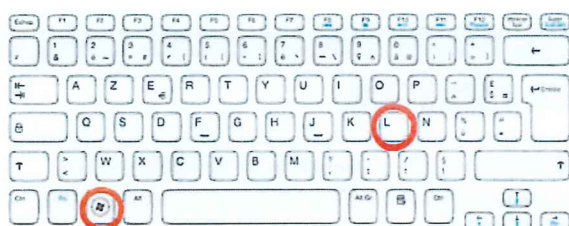
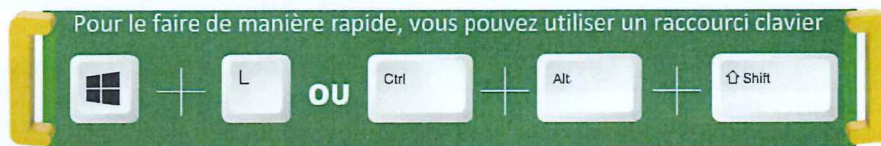
Cette personne pourrait également **accéder au réseau de votre collectivité**, notamment aux espaces de stockages et aux documents de vos collègues.



Cette personne **pourrait envoyer des mails, des documents sous votre identité**, et avoir accès à votre carnet d'adresse.

Il est donc essentiel de bien verrouiller son poste dès que l'on s'éloigne de son ordinateur.

Pour le faire de manière rapide, vous pouvez utiliser un raccourci clavier



ou



IMPORTANT

Votre clé ou disque USB personnel peut être un vecteur de diffusion d'un virus au sein de votre collectivité. Ne prenez pas ce risque !

CLÉ USB: UN PETIT OBJET QUI PEUT VOUS FAIRE TRÈS MAL

Une clé USB trouvée ou reçue en cadeau ?

01

Ne la branchez surtout pas à votre ordinateur professionnel, vous pourriez **mettre en danger vos données et celles de votre collectivité**.

02

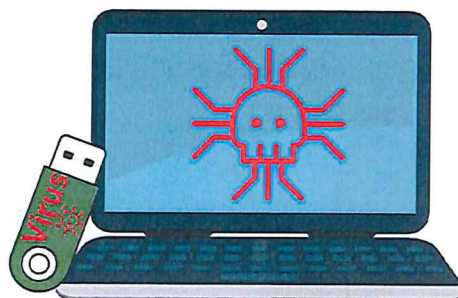
Ne branchez aucun support de stockage USB (Disque dur, Clef usb, Smartphone) **qui n'a pas été contrôlé par votre collectivité** sur votre ordinateur professionnel.

03

Une clé USB trouvée ou que l'on vous aurait offerte **peut contenir un virus ou être une clé dédiée à l'attaque**, ce qui mettrait en danger toutes nos données (destruction, corruption ou vol).

04

Malgré les protections mise en place par la mairie et en cas de doute, je fais **contrôler le dispositif externe par la DSI**.





IMPORTANT

Je ne clique ni sur les liens ni sur les documents joints avant de m'assurer qu'ils ne sont pas malveillants.

PROTÉGER MA BOITE MAIL

Soyez toujours très attentif avant de cliquer sur un lien reçu dans un e-mail !

01

En cliquant sans vérifier la validité du lien, vous pourriez vous faire **voler des informations sensibles** ou **compromettre la sécurité de votre poste de travail** et de l'intégralité des données de la collectivité.

02

Si vous ne prenez pas garde avant de cliquer sur un lien reçu par e-mail, SMS, chat ou tout autre support, vous pourriez être **victime d'un piratage**.

03

Avant de cliquer, vous devez **prendre le temps de vérifier que le lien est valide** si vous ne voulez pas prendre le risque de diffuser involontairement vos données et celles de votre collectivité à un pirate ou de compromettre la sécurité de votre poste de travail.

04

En cas de doute, il est toujours préférable **de sélectionner l'URL du site et de la copier/coller** dans votre navigateur (Google Chrome, Mozilla Firefox, Microsoft Edge, Safari).

05

Ne **jamais consulter ses mails privés** à partir de votre outil de travail. En effet, cela n'est pas sécurisé par notre outil de filtrage.





Messageries, réseaux sociaux, banques, administrations et commerces en ligne, réseaux et applications de la collectivité... la sécurité de l'accès à tous ces services du quotidien repose aujourd'hui essentiellement sur les mots de passe.

Face à la profusion des mots de passe, la tentation est forte d'en avoir une gestion trop simple. Une telle pratique serait dangereuse, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès.

Voici **10 bonnes pratiques** à adopter pour gérer efficacement vos mots de passe

- 01 Utilisez un mot de passe différent pour chaque applicatif
- 02 Utilisez un mot de passe suffisamment long et complexe.
- 03 Utilisez un mot de passe* impossible à deviner.
- 04 Utilisez un gestionnaire de mots de passe (Keepass).
- 05 Changez votre mot de passe au moindre soupçon
- 06 Ne communiquez jamais votre mot de passe à un tiers.
- 07 N'enregistrez pas vos mots de passe sur un pc partagé
- 08 Activez la «double authentification» lorsque c'est possible
- 09 Changez les mots de passe par défaut des différents services aux quels vous accédez.
- 10 Choisissez un mot de passe particulièrement robuste pour votre messagerie.

*LA MÉTHODE DES PREMIÈRES LETTRES: Un tiens vaut mieux que deux tu l'auras: ItvmQ2tl'A
LA MÉTHODE PHONÉTIQUE: J'ai acheté huit CD pour cent euros cet après-midi : ght8CD%E7am



IMPORTANT

Je suis scrupuleusement les consignes de télétravail pour ne pas exposer d'avantage le système informatique à des attaques.

RESPECTER LES RÈGLES DU TÉLÉTRAVAIL

Recommandations de sécurité pour les télétravailleurs

01

Appliquez strictement les consignes de sécurité de votre collectivité.

02

Ne faites pas en télétravail ce que vous ne feriez pas au bureau.

03

Renforcez la sécurité de vos mots de passe.

04

Sécurisez votre connexion WiFi.

05

Sauvegardez régulièrement votre travail.

06

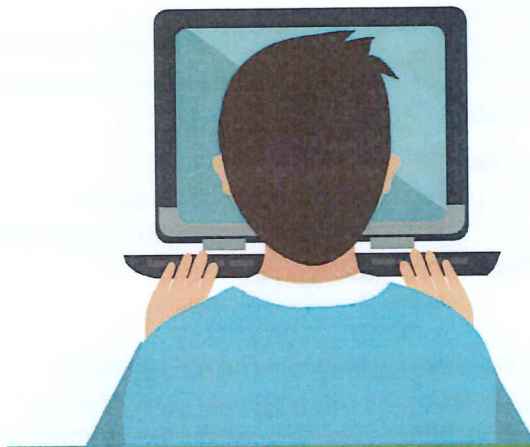
Méfiez-vous des messages inattendus.

07

N'installez vos applications que dans un cadre << officiel >> et évitez les sites suspects.

08

L'utilisation d'un ordinateur professionnel à des fins personnelles est toléré. Cependant, mélanger nos vies professionnelles et privées sur le matériel fourni par la collectivité peut nous porter préjudice, mais également nuire à la collectivité. Notre réseau pourrait subir des cyberattaques.



IMPORTANT

Je stocke mes données de travail sur les serveurs car ce sont les seuls espaces de stockage sécurisés et sauvegardés

STOCKER MES FICHIERS SUR LES SERVEURS

Les avantages du stockage sur le serveur

✓ Idéal pour la **sauvegarde** de gros volumes

✓ Restauration des données simple et ultra rapide

✓ **Intégrité** et récupération des données plus rapide

✓ **Travail collaboratif** de meilleure qualité

✓ **Travail collaboratif** de meilleure qualité

✓ **Sécurité** : les ordinateurs portables sont sujets à de nombreux vols.

Environ 800 000 ordinateurs portables sont volés et/ou perdus chaque année.

Grâce au serveur mis en place au sein de la collectivité, les données restent accessibles dans un dossier partagé ou privé et sauvegardées (puisqu'elles sont centralisées sur un serveur).

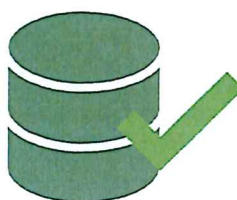
Les inconvénients du disque dur

✗ Le disque dur peut crasher à tout moment et entraîner la perte de vos fichiers. Cela n'est pas le cas avec du stockage en réseau qui va nous permettre de se prémunir contre ce risque.

✗ Le disque dur qui contient toutes vos données meurt, les informations meurent avec lui!

Lorsque vous stockez des informations localement, vous augmentez le risque de perte de données en cas de vols, d'incendies, d'inondations ou autres incidents.

✗ Le plus grand inconvénient du stockage local est que vos données sont accessibles que par vous et non sauvegardées. Il est compliqué de partager des données avec les membres de votre équipe si vous n'êtes pas tous connectés au réseau local.



IMPORTANT

Au bureau, je ne laisse pas mes documents à la vue de tous car je risque d'exposer des informations confidentielles.

RANGER MON BUREAU

Autant de gestes qui vous permettront de maintenir une confidentialité accrue dans votre collectivité et garder la confiance de vos collaborateurs.

01

Ranger et organiser son bureau

02

Classer et verrouiller les informations sensibles sur votre ordinateur.

03

Activer l'économiseur d'écran par mot de passe.

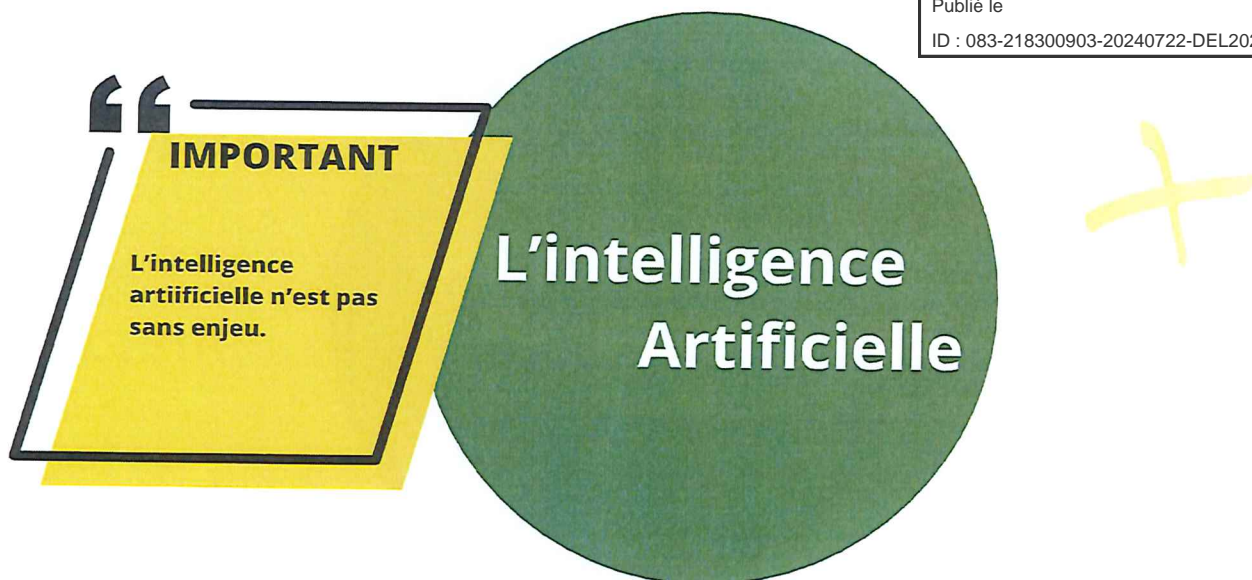
04

Détruire les post-its ou notes dont les informations peuvent être sensibles.

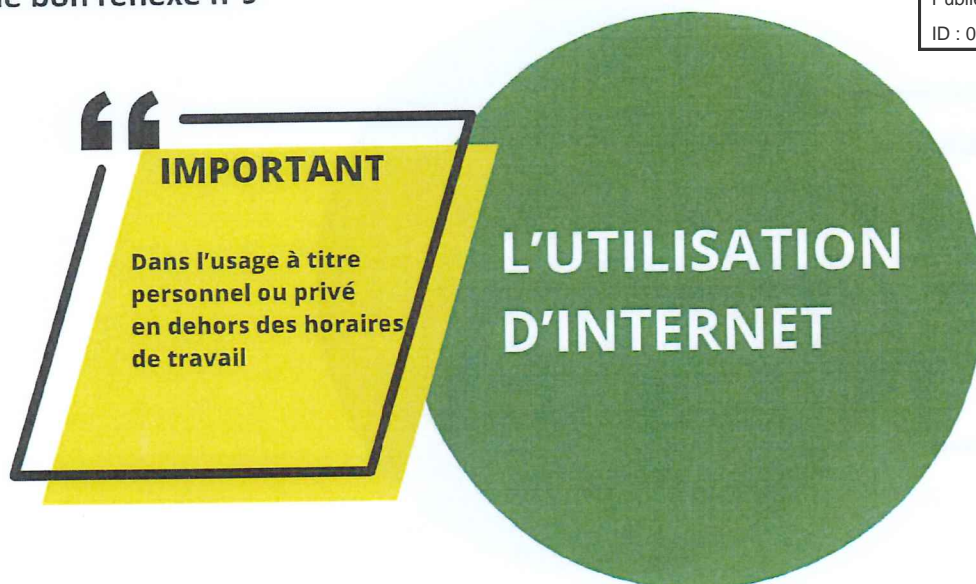
05

Étendre la culture <<bureau propre>> sur ordinateur, appareil mobile, et ranger les documents imprimés, carte d'accès, clef usb, disque dur...





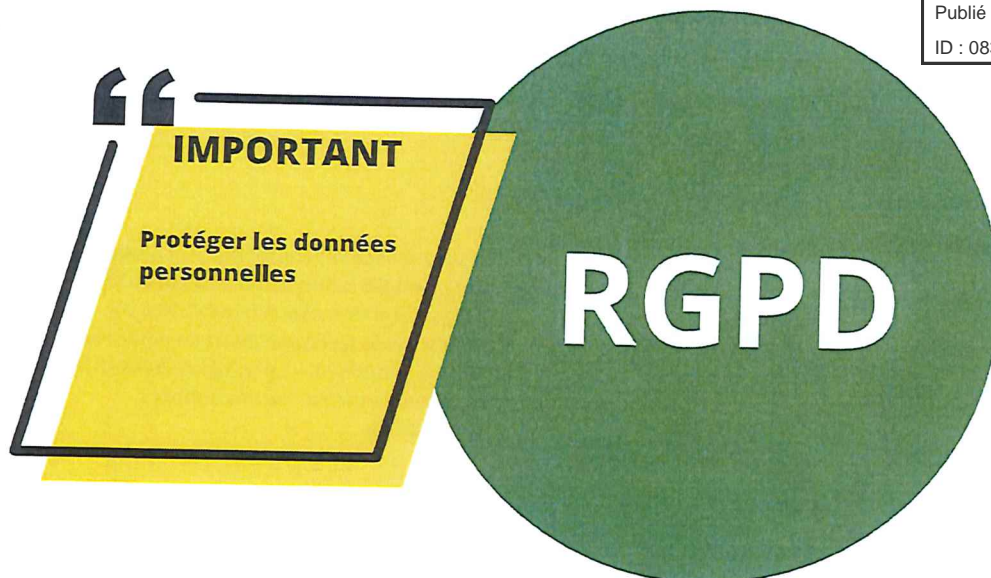
- Utilisation responsable de l'outil : L'utilisation de l'IA ne doit pas remplacer la prise de décision humaine ni négliger l'expertise humaine et le raisonnement associé.
- Gestion des risques liés à l'exactitude des informations : Les utilisateurs doivent être conscients que les réponses générées par l'IA peuvent être sujettes à des erreurs et doivent être évaluées avec soin.
- Prévention des biais et de la discrimination : Les utilisateurs doivent être conscients que l'IA peut reproduire les biais présents dans sa base de données.
- Il est de la responsabilité des utilisateurs de surveiller et de corriger les réponses générées par l'IA pour éviter tout contenu biaisé, discriminatoire ou offensant.
- Sécurité et confidentialité des données : Les utilisateurs doivent respecter le règlement général sur la protection des données et ne partager aucune donnée personnelle dans leurs interactions avec l'IA.
- Les utilisateurs doivent respecter les politiques de sécurité et de confidentialité des données de la collectivité lors de l'utilisation de l'IA.



Usage à titre privé ou personnel :

La mairie tolère une utilisation raisonnable des moyens informatiques de la collectivité à des fins privées ou personnelles, en dehors des horaires de travail, utilisation qui ne porte pas atteinte au bon fonctionnement de la collectivité, au bon fonctionnement des ressources informatiques et à la bonne exécution des missions et dont les modalités sont les suivantes :

- Cette utilisation est limitée aux pc bureautiques, téléphones, internet, mail. Cela exclut notamment les ressources métier et les espaces de stockage centralisés.
- Cette utilisation ne doit pas mettre en danger les applications professionnelles par des comportements à risque ou par une utilisation excessive des ressources disponibles, notamment les ressources de stockage et de bande passante des réseaux.
- Cette utilisation doit être à destination strictement personnelle.
- Cette utilisation doit s'opérer en conformité avec les lois en vigueur. Il est notamment interdit d'utiliser les moyens informatiques de l'entreprise pour effectuer des téléchargements illicites ou accéder à des sites illégaux, discriminants, à caractères pornographiques, racistes, antisémite, etc..
- Cette utilisation ne doit pas porter préjudice à l'image de la collectivité.
- Cette utilisation ne doit pas perturber l'activité professionnelle des collaborateurs ou des collègues de l'utilisateur.



Les collectivités territoriales traitent de nombreuses données personnelles, que ce soit pour assurer la gestion des services publics dont elles ont la charge (état civil, inscriptions scolaires, listes électorales, etc.), la gestion des ressources humaines, ou encore leur site web.

Les citoyens sont de plus en plus sensibles à la protection de leurs données et leur principal motif de crainte est la peur du piratage et du vol de données. Le développement de services en ligne constitue un levier majeur de la modernisation de l'action publique. De ce fait, les collectivités recourent de plus en plus aux téléservices, aux systèmes d'information géographique, à la vidéosurveillance, aux dispositifs de lecture automatique de plaques d'immatriculation, aux solutions de ville intelligente, etc.

Le nombre de cyberattaques et plus globalement d'incidents de sécurité ne cesse d'augmenter, et ce, quelle que soit la taille des organisations visées. Respecter les règles de protection des données personnelles est un facteur de transparence et de confiance à l'égard des administrés et des agents.

C'est aussi un gage de sécurité juridique pour les élus qui sont responsables des fichiers et des applications utilisées au sein de la commune.

Qu'est-ce qu'une donnée personnelle ?

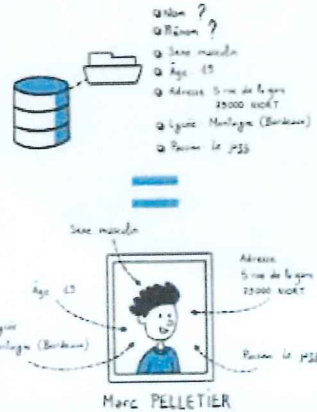
Une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ».

Une personne physique peut être identifiée :

directement (exemple : nom et prénom) ;
indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image).

l'identification d'une personne physique peut être réalisée :

à partir d'une seule donnée (exemple : nom) ;
à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre de telle association).



Par exemple, une enquête par questionnaire qui porte sur des élèves d'une école primaire peut, même lorsque les noms et prénoms ne sont pas indiqués, contenir des réponses qui combinées les unes aux autres, permettent de retrouver l'identité des enfants. C'est le cas lorsque les réponses sont précises, par exemple : 7 ans, fille, classe de CE1, redoublement dans telle école primaire de telle ville.

Qu'est-ce qu'un « traitement de données personnelles » ?

Un « traitement de données personnelles » est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé : collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement. C'est donc une notion très large : tout maniement de données, y compris une simple consultation, est un « traitement de données personnelles ».

Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

EXEMPLES DE TRAITEMENTS :

Tenue du registre d'état civil, gestion des inscriptions en crèche, scolaire et périscolaire, tenue du cadastre, gestion de la liste électorale, gestion des ordures ménagères, gestion des adhérents de la médiathèque, etc.

Il peut s'agir d'une base de données, d'un fichier papier ou numérique, d'une application mobile, de dispositifs biométriques, de sites web, etc.

La finalité

Un traitement de données doit avoir un objectif, une **finalité déterminée** préalablement au recueil des données et à leur exploitation. Autrement dit, il n'est pas permis de collecter des données lorsque l'on ne sait pas quel usage en faire. Par ailleurs, en principe, la finalité initiale doit être respectée, afin d'éviter tout « détournement de finalité ».

EXEMPLE DE FINALITÉ

Un maire ne pourra pas se servir du fichier des inscriptions scolaires pour faire de la communication politique. La liste électorale pourra en revanche être utilisée à une telle fin.

La licéité ou la base légale

Un traitement de données doit être licite. Cela signifie d'abord qu'il doit être conforme au droit en général. Par exemple, un traitement de données ne peut pas avoir pour but une discrimination illégale. Cela signifie, ensuite, qu'il doit reposer sur l'une des six « bases légales » permises par le RGPD, c'est-à-dire l'une des hypothèses dans lesquelles le RGPD autorise un opérateur à traiter les données de personnes physiques : l'obtention du consentement préalable de la personne, l'exécution d'un contrat conclu avec elle, l'accomplissement d'une mission d'intérêt public, le respect d'une obligation légale qui impose le traitement de ces données, etc.

En revanche, des coordonnées d'entreprises (par exemple, l'entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un courriel de contact générique « compagnie1@email.fr ») ne sont en principe pas des données personnelles.



Le délégué informe et conseille la collectivité

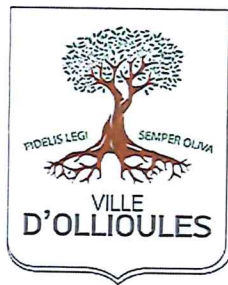


Le délégué contrôle le respect du règlement



Le délégué est le point de contact pour l'exercice des droits

RAPPEL : Le Délégué à la Protection des Données au sein de la Commune est Sarah AMRI du service juridique



Récépissé de la charte informatique

Je soussigné(e)

Nom :

Prénom :

Service :

Fonction :

Agent / Elu(e) de la commune d'Ollioules, déclare avoir pris connaissance de la charte informatique et m'engage à la respecter. Utilisateur des moyens informatiques et réseaux de la collectivité, déclare avoir pris connaissance de la présente charte et m'engage à la respecter.

Fait à

Le

Fait en deux exemplaires :

Un pour l'intéressé

Un pour la collectivité

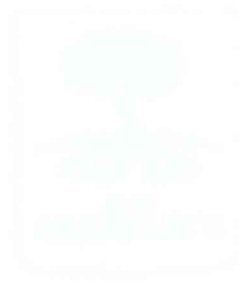
Signature

Envoyé en préfecture le 26/07/2024

Reçu en préfecture le 26/07/2024

Publié le

ID : 083-218300903-20240722-DEL2024_07_4_4-DE



Ministère de l'Intérieur

Département de la Seine-Saint-Denis

Direction des Services

Arrêté du 26 juillet 2024

relatif à la mise en œuvre de la loi n° 2017-133 du 27 septembre 2017

relative à la lutte contre le harcèlement sexuel

et à la protection des victimes

Le préfet de la Seine-Saint-Denis, vu l'arrêté du 26 juillet 2024, en vertu duquel il a été nommé préfet de la Seine-Saint-Denis, en application de l'article 171 de la loi n° 2017-133 du 27 septembre 2017 relative à la lutte contre le harcèlement sexuel et à la protection des victimes, a arrêté ce qui suit :

Article 1er.

Le directeur départemental de la police est chargé de l'exécution de l'arrêté.

Fait à Paris, le 26 juillet 2024.

Le préfet de la Seine-Saint-Denis,

Philippe BOURGEOIS

Le directeur départemental de la police,

Arrêté en vertu duquel il a été nommé préfet de la Seine-Saint-Denis, en application de l'article 171 de la loi n° 2017-133 du 27 septembre 2017 relative à la lutte contre le harcèlement sexuel et à la protection des victimes.