**Ière PARTIE : PROTECTION DES DONNEES A CARACTERE PERSONNEL**

**Article 1 : confidentialité des données**

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

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

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

**Article 2 : accès aux données par les agents**

L‘accès par les agents aux informations et documents conservés doit être limité à ceux qui leur sont propres, ainsi que ceux publics ou partagés.

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

**Article 3 : Responsable de traitements et délégué à la protection des données**

Le [Maire/Président de …] est responsable des traitements de données à caractère personnel. Le responsable de traitements veille au sein de la collectivité/de l’établissement à la bonne application des règles issues du règlement général sur la protection des données.

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

**IIème PARTIE : REPONSES AUX DEMANDES D’USAGE DES DROITS DES PERSONNES CONCERNEES PAR LES TRAITEMENTS DE DONNEES**

**Article 4 : Droits des personnes concernées par les traitements de données**

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

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

**Article 5 : Droit à l’information des personnes concernées par les traitements de données**

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

**Article 6 : Demandes d’usage des droits des personnes**

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

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

**Article 7 : Instruction des demandes d’usage des droits des personnes**

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

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

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

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

**Article 8 : Refus de la demande d’usage des droits des personnes**

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

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

Si la collectivité/l’établissement ne dispose d’aucune donnée sur la personne qui exerce son droit d’accès, une réponse précisant ce fait devra être apportée dans le délai d’un mois.

**Article 9 : Réponses aux demandes d’usage des droits des personnes**

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

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

**IIIème PARTIE : VIOLATIONS DE DONNEES A CARACTERE PERSONNEL**

**Article 10 : Constatation des violations de données**

Toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l’altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d’une manière, ou l’accès non autorisé à de telles données constitue une violation de données à caractère personnel.

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

**Article 11 : Documentation de la violation de donnée**

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

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

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

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

**Article 12 : Notification des violations de données auprès de la CNIL**

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

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

En cas d’impossibilité de réunir toutes les informations susmentionnées dans l’article 11 dans un tel délai, une notification initiale devra être déposée dans ledit délai, suivie d’une notification complémentaire dès que l’ensemble des éléments seront réunis.

Toute notification effectuée hors délais devra être justifiée.

**Article 13 : Notification des violations de données auprès des personnes concernées**

Toute violation de données susceptible de porter une atteinte excessivement élevée à la vie privée des personnes concernées par les données touchées par la violation devra, en outre de la notification mentionnée à l’article 12, faire l’objet d’une notification auprès des personnes concernées.

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

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

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

**Article 14 : Traçabilité des notifications de violations de données**

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