wiseorga
Transformation d'entreprise & numérique

LEXING
ALAIN BENSOUSSAN AVOCATS

Accompagnement à la mise en place du règlement général de protection des données (RGPD)

laCourneuve

Commune de La Courneuve

Sensibilisation Référents Informatique et Libertés (RILs)

23/09/2022

SOMMAIRE

1/ DÉFINITIONS ET ENJEUX DE LA PROTECTION DES DONNÉES PERSONNELLES

2/ LES EXIGENCES POUR LA COURNEUVE

3/ MISE EN ŒUVRE OPÉRATIONNELLE VIA UN RESEAU DE RILS

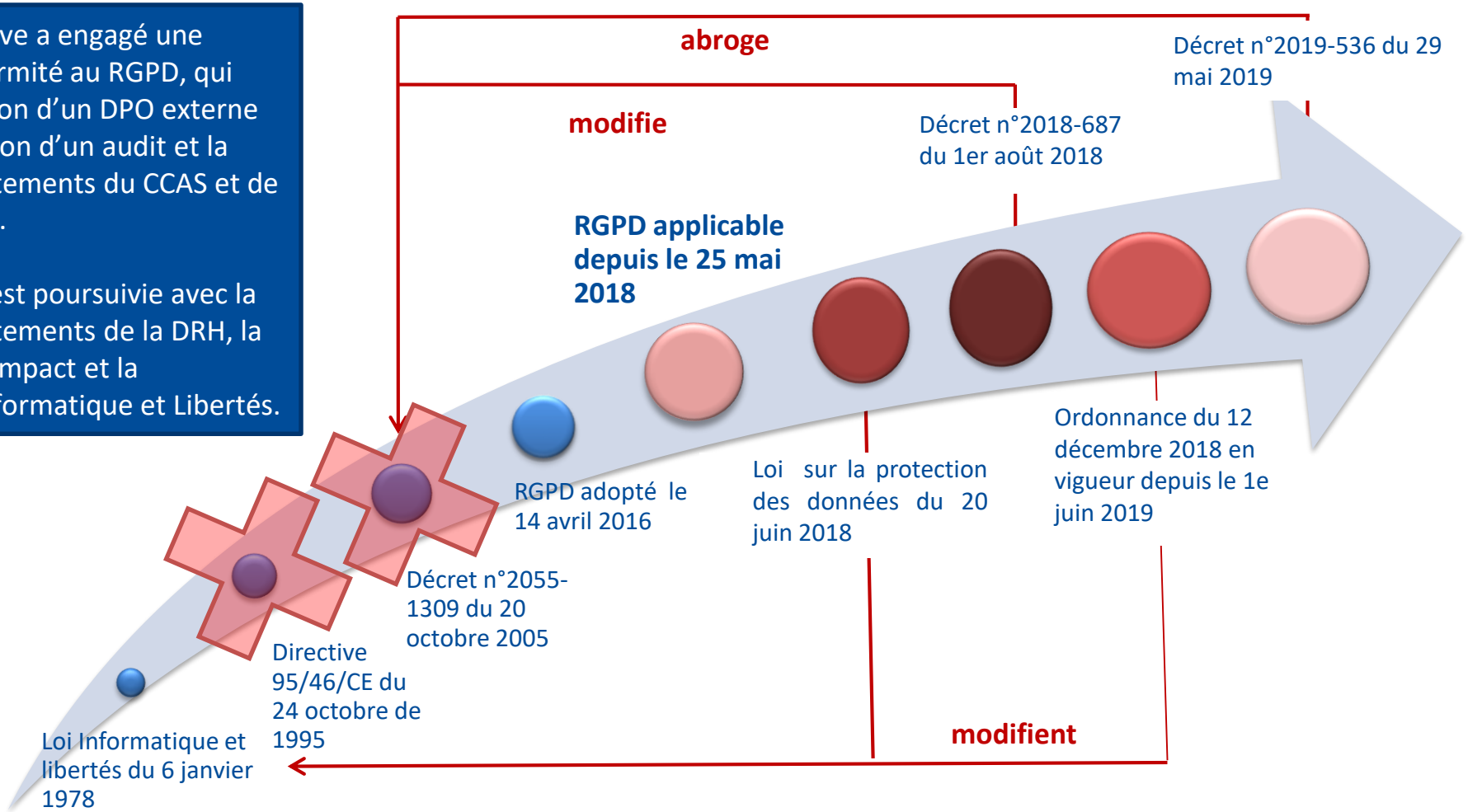
•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

1/ DEFINITIONS ET ENJEUX DE LA PROTECTION DES DONNÉES PERSONNELLES

Historique de la réglementation en matière de données à caractère personnel

La Commune de La Courneuve a engagé une démarche de mise en conformité au RGPD, qui s'est traduit par la désignation d'un DPO externe en 2020, puis par la réalisation d'un audit et la mise en conformité des traitements du CCAS et de la Caisse des Ecoles en 2021.

En 2022, cette démarche s'est poursuivie avec la mise en conformité des traitements de la DRH, la réalisation d'une analyse d'impact et la désignation de Référents Informatique et Libertés.



•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

1/ DEFINITIONS ET ENJEUX DE LA PROTECTION DES DONNÉES PERSONNELLES

Quelques rappels – données à caractère personnel

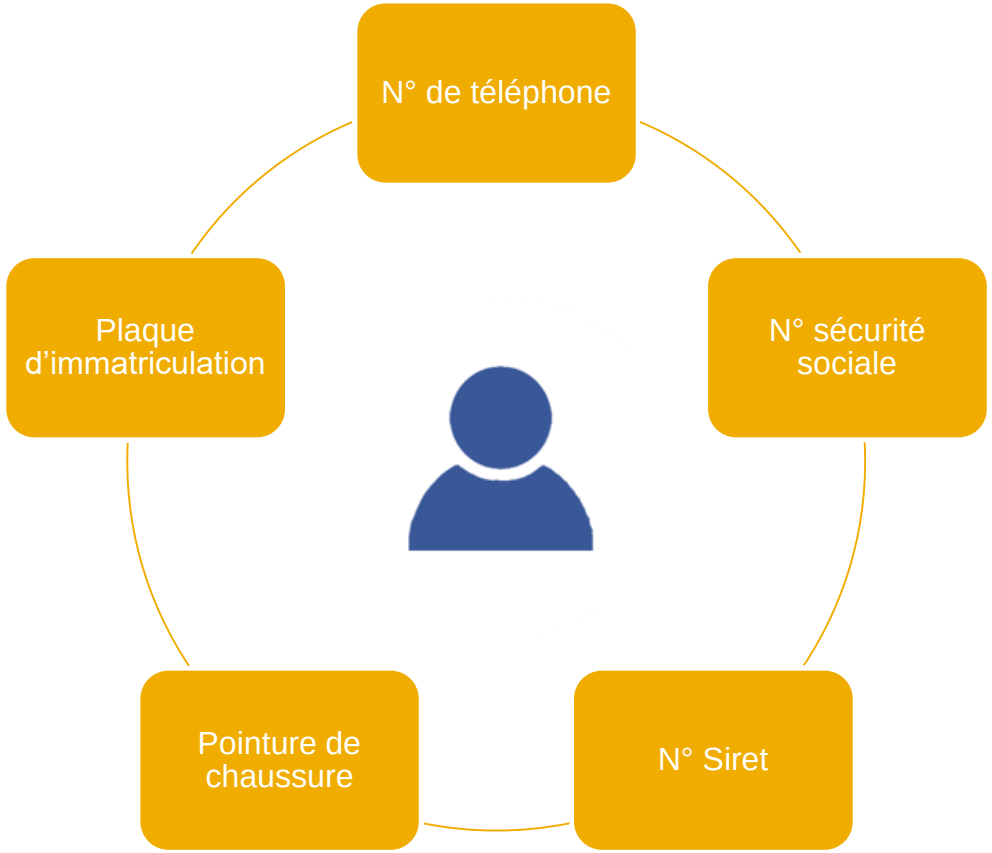
- Une **donnée personnelle** est toute information se rapportant à une personne physique **identifiée** ou **identifiable**.

- Une personne peut être identifiée :
  - **directement (exemple : nom, prénom)**
  - **indirectement** (exemple : par un identifiant (matricule), une donnée biométrique, mais aussi la voix ou l'image.

Les catégories de données à caractère personnel
Etat civil, identité, données d'identification, images…
Vie personnelle
Informations d'ordre économique et financier
Informations d'ordre professionnel
Données de connexion
Données de localisation

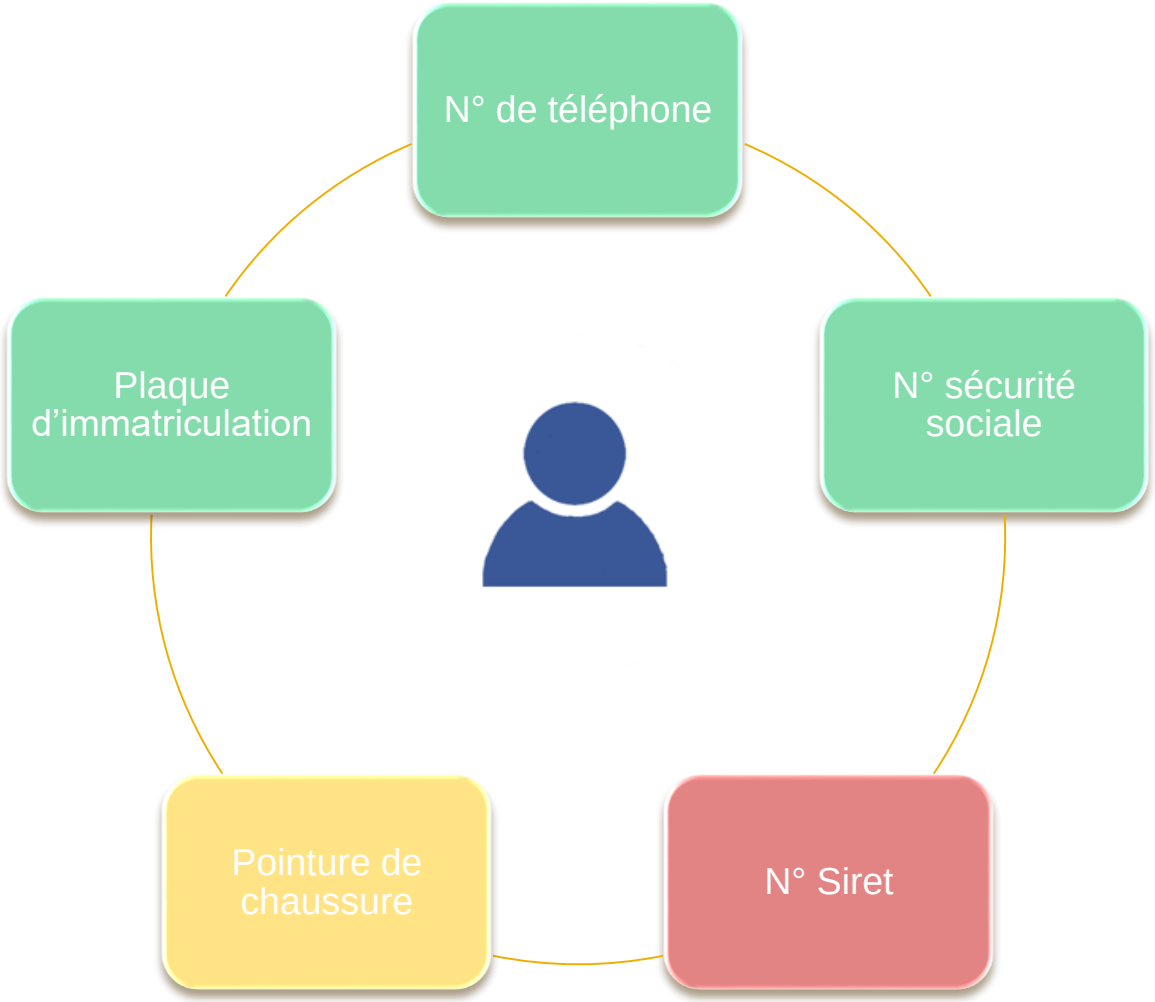
•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

- **Parmi ces données, lesquelles sont des données à caractère personnel ?**



•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

- **Parmi ces données, lesquelles sont des données à caractère personnel ?**



• Une donnée à caractère personnel est **toute information se rapportant à une personne physique** (tel un administré, un agent territorial, un prestataire etc.) **identifiée ou identifiable directement ou indirectement**.

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

1/ DEFINITIONS ET ENJEUX DE LA PROTECTION DES DONNÉES PERSONNELLES

Quelques rappels – catégories particulières de données à caractère personnel ?

Certaines données personnelles sont qualifiées de « **particulières** » et ont un régime particulier : le **traitement de ce type de données est par principe interdit**, sauf exceptions.

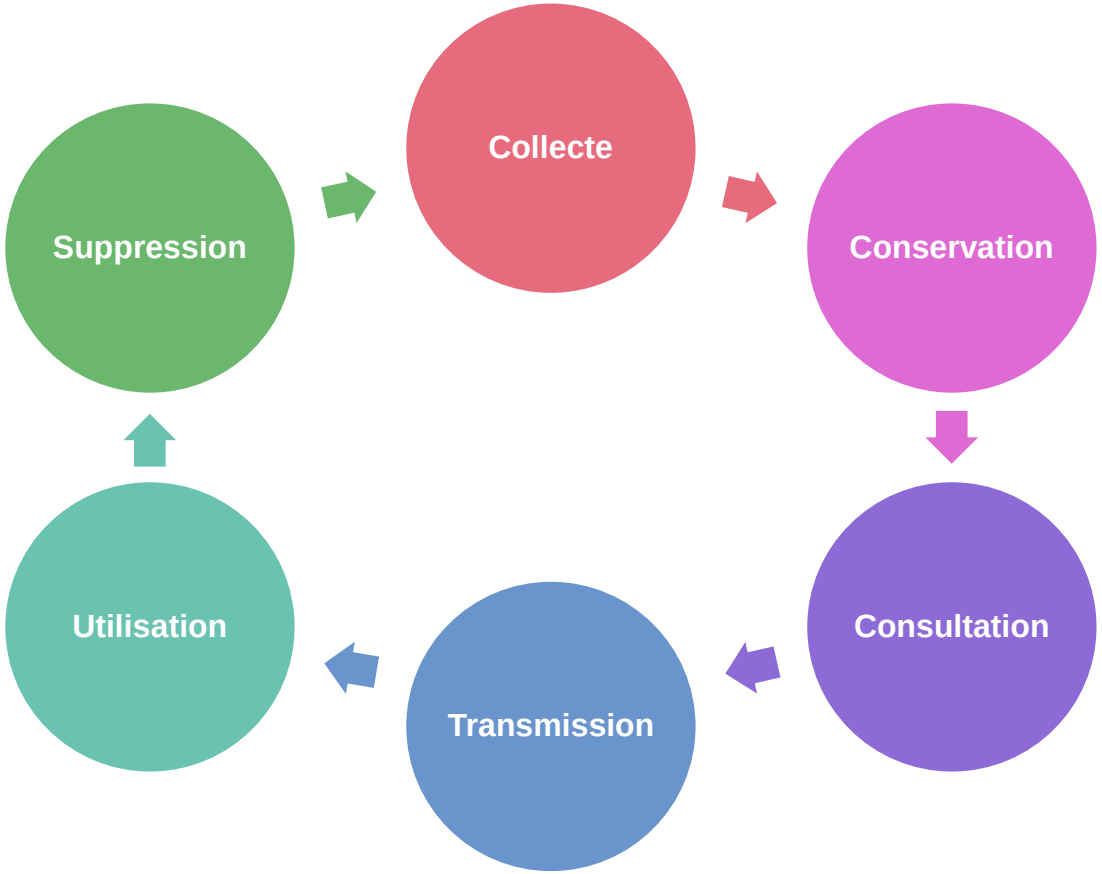
•Origines raciales ou ethniques	• « d'origine africaine » • « couple de Roms »
•Opinions politiques	• « est de droite » • « sympathisant PS »
•Convictions religieuses ou philosophiques	• « Franc-maçon » • « est en pèlerinage à Lourdes »
•Appartenances syndicales	• « CGT » • « syndiqué FO »
•Données génétiques ou biométriques	• « Analyse de l'ADN » • Empreintes digitales comme mode d'identification
•Données sur la vie sexuelle ou l'orientation sexuelle	• « couple gay » • « a deux femmes »
•Données de santé	• « schizophrénie » • Souffre d'alcoolisme »

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

1/ DEFINITIONS ET ENJEUX DE LA PROTECTION DES DONNÉES PERSONNELLES

Quelques rappels – Traitement de données à caractère personnel ?

Un « traitement » se définit comme **toute opération ou tout ensemble d'opérations** effectuées ou non à l'aide de procédés automatisés et appliqués à des données personnelles.



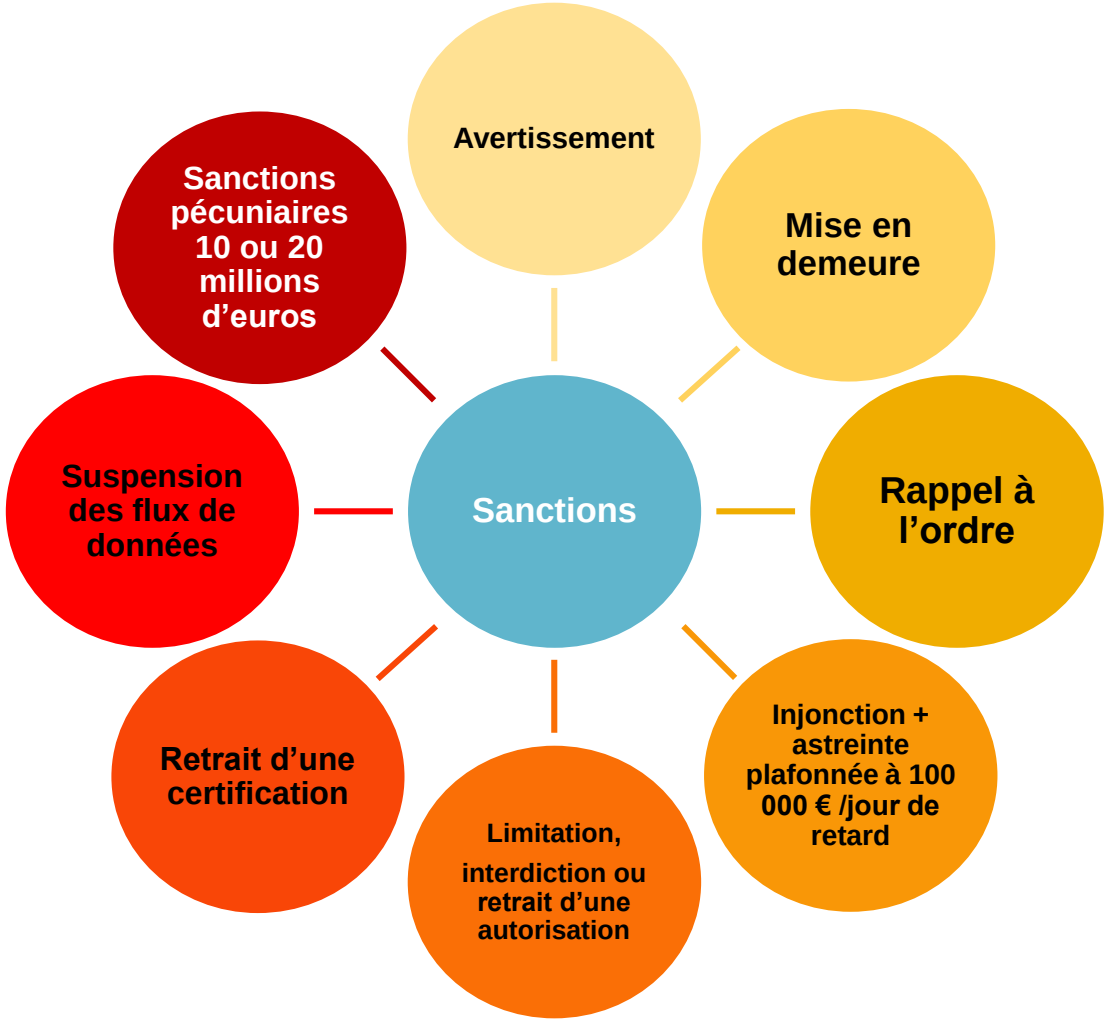
Les traitements effectués sur des **supports papiers** sont également concernés.

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

1/ DEFINITIONS ET ENJEUX DE LA PROTECTION DES DONNÉES PERSONNELLES

Quelles sanctions ?

Les **sanctions** prévues en cas de non respect de la règlementation s'appliquent à La Courneuve



•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

1/ DEFINITIONS ET ENJEUX DE LA PROTECTION DES DONNÉES PERSONNELLES

Qu'est ce que le RGPD, pourquoi ce règlement et quel est le principal changement amené par le RGPD ?

•1 Harmoniser la protection des données personnelles dans l'Union Européenne.

Le RGPD est directement applicable dans l'ensemble des Etats membres de l'Union Européenne (UE), harmonisant ainsi la protection des données personnelles dans l'UE.

•2 Responsabiliser les acteurs publics qui traitent des données personnelles.

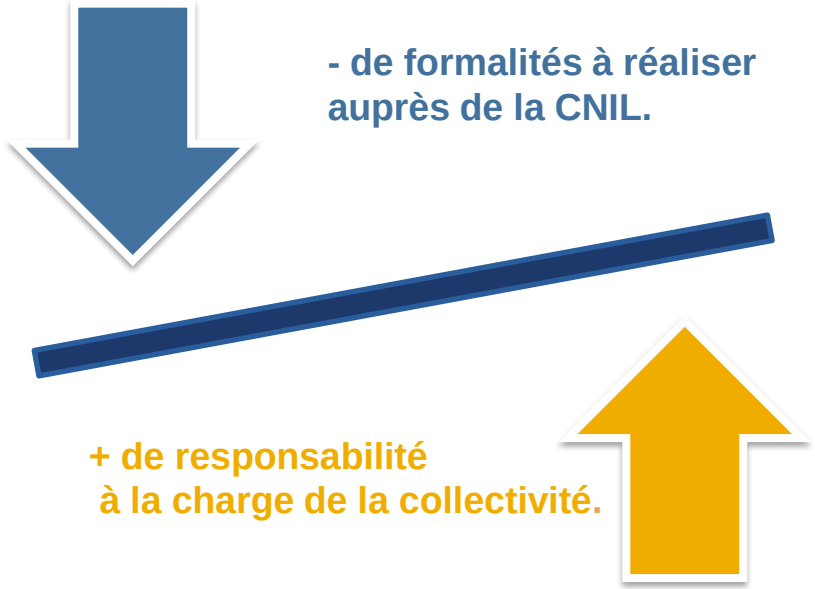
Une collectivité doit, à tout moment, être en mesure de prouver sa conformité au RGPD (à l'aide de politiques, procédures, contrôles, formations, …)

•3 Renforcer les droits des personnes concernées

Le RGPD renforce les droits préexistants des personnes (droit d'accès, d'opposition, de rectification) et en crée de nouveaux (droit à la limitation, à la portabilité, …)

•4 Sanctionner la non conformité

La CNIL est désormais en mesure de sanctionner une collectivité à hauteur de 20 000 000 € en cas de non respect des dispositions du RGPD.



Les acteurs publics doivent désormais être en mesure de prouver leur conformité au RGPD, à tout moment !
C'est le principe de responsabilisation (*accountability*).

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

SOMMAIRE

1/ DÉFINITIONS ET ENJEUX DE LA PROTECTION DES DONNÉES PERSONNELLES

2/ LES EXIGENCES POUR LA COURNEUVE

3/ MISE EN ŒUVRE OPÉRATIONNELLE VIA UN RESEAU DE RILS

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

2/ LES EXIGENCES POUR LA COURNEUVE

Pourquoi protéger les données personnelles à La Courneuve ?

Le secteur public, un secteur exposé

- **Développement de l'e-administration** : les téléservices, l'open data, les systèmes d'information géographique, le cloud computing, etc.
- Les **personnes concernées** (agents, usagers et administrés) sont **sensibilisées** à la protection des données et font de plus en plus souvent usage de leurs droits.

Un nombre important de traitements de données personnelles réalisé par La Courneuve

- La Courneuve traite dans le cadre de ses activités, un **grand nombre de données personnelles** relatives à ses administrés, ses agents et fournisseurs, pour des finalités diverses (gestion administrative, sécurisation des locaux, gestion de la téléphonie, gestion des demandes de logement, gestion des listes électorales …).
- Certains de ces traitements font par ailleurs l'objet **d'une attention particulière de la part du régulateur**, en raison de leur sensibilité (fichiers d'aide sociale, fichiers de la police municipale, …).

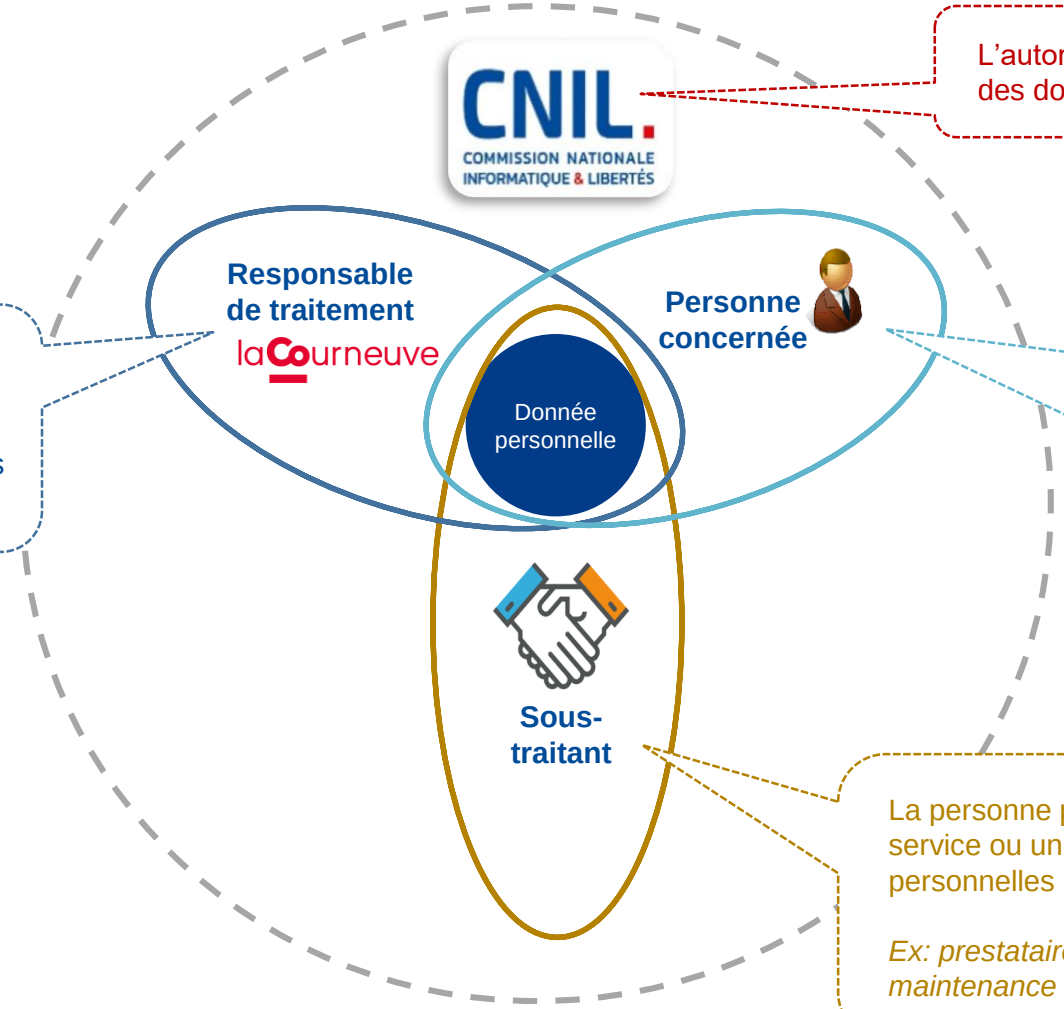
Une augmentation exponentielle des données échangées, une ouverture croissante des systèmes d'information, qui sont autant d'opportunités mais également de risques à maîtriser.

La protection des données à La Courneuve est à intégrer au quotidien à l'ensemble des activités

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

2/ LES EXIGENCES POUR LA COURNEUVE

Les acteurs impliqués



L'autorité de contrôle en matière de protection des données personnelles en France

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui détermine les finalités et les moyens du traitement

La personne physique dont les données personnelles font l'objet d'un traitement

Ex: collaborateur, fournisseur, client, prestataire…

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données personnelles pour le compte de La Courneuve

Ex: prestataires, éditeur de logiciel en charge de la maintenance

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

➢ Nommer un Délégué à la Protection des Données (ou « DPO »)

Délégué à la protection des données

=

« DPD » ou « DPO » (Data Protection Officer) : « Chef d'orchestre » de la conformité au RGPD de la commune

➢ Les principales missions du « DPD » :

- **Informer** et **conseiller** la commune sur les sujets relatifs à la protection des données personnelles ;
- **Contrôler** le respect du Règlement et du droit national en matière de protection des données ;
- Conseiller l'organisme sur la réalisation d'une **analyse d'impact** relative à la protection des données et en vérifier l'exécution ;
- **Coopérer avec l'autorité de contrôle** et être le point de contact de celle-ci.

Le cabinet Lexing Alain Bensoussan Avocats est le DPD de la commune de La Courneuve.
Une adresse mail dédiée a été créée : dpo@lacourneuve.fr

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

- **Chaque traitement doit respecter le principe de « Protection par défaut »**

Notion

Prendre les mesures techniques et organisationnelles appropriées pour garantir que par défaut seules les données qui sont nécessaires au regard de la finalité spécifique du traitement sont traitées

Application

Volume de données

Etendue de leur traitement

Durée de conservation

Accessibilité

Exemple

Limiter le risque d'accès à des applications par la mise en place d'une gestion centralisée des habilitations

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

2/ LES EXIGENCES POUR LA COURNEUVE

Les obligations pour La Courneuve

- Chaque nouveau traitement doit respecter le principe de « **Protection dès la conception** »

Elaboration d'une méthodologie/procédure permettant de l'intégrer concrètement dans les projets et de s'assurer de la conformité du produit ou service tout au long de son cycle de vie

↓

Mécanismes permettant de s'assurer de la conformité Informatique et libertés

↓

Implémentation d'outils appropriés

↓

Mise en place d'une organisation adaptée

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

2/ LES EXIGENCES POUR LA COURNEUVE

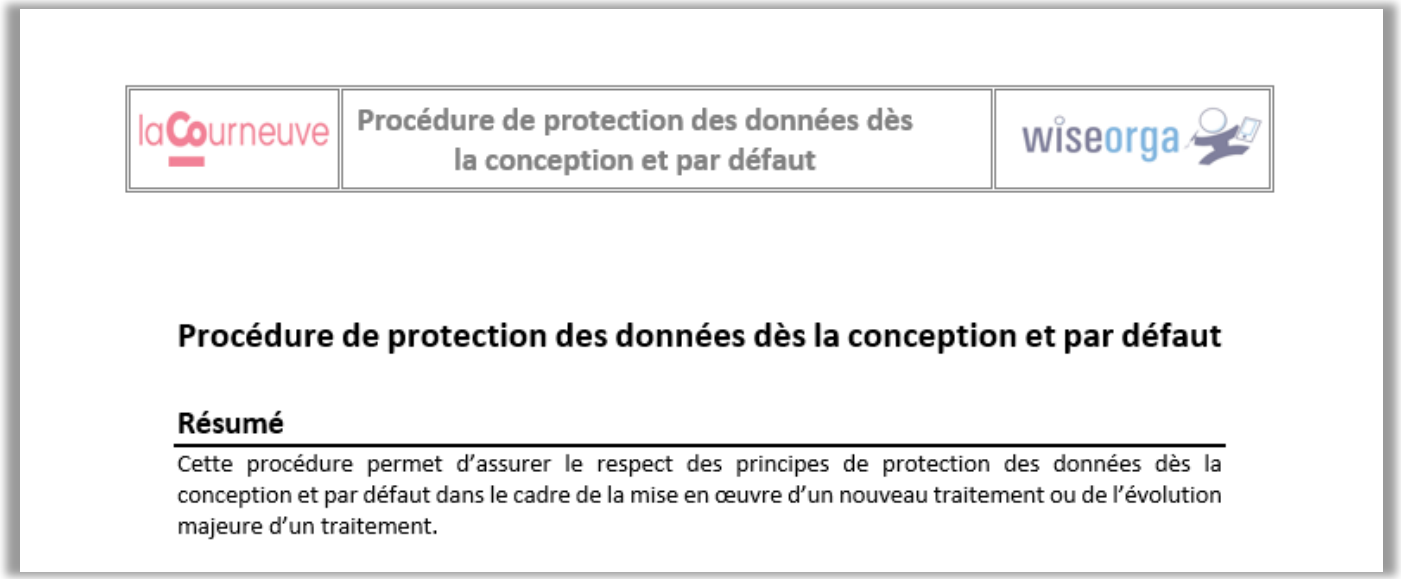
Les obligations pour La Courneuve

Les **trois registres des activités de traitement** (celui de la commune, celui du CCAS et celui de la Caisse des Ecoles) sont **initialisés**.

Le **DPO** identifie les éventuelles **non conformités** et les **actions** à réaliser afin de rendre le traitement conforme.

Une fois que les actions ont été réalisés par les RILs et / ou le DPO, la **mise à jour du traitement** est ajoutée au registre des activités de traitement.

Lorsqu'un nouveau traitement est mis en œuvre, la **politique de protection dès la conception** est appliquée.



laCourneuve	Procédure de protection des données dès la conception et par défaut	wiseorga

Procédure de protection des données dès la conception et par défaut

Résumé

Cette procédure permet d'assurer le respect des principes de protection des données dès la conception et par défaut dans le cadre de la mise en œuvre d'un nouveau traitement ou de l'évolution majeure d'un traitement.

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

2/ LES EXIGENCES POUR LA COURNEUVE

Les obligations pour La Courneuve

➢ Chaque traitement doit respecter les **principes relatifs au traitement de données**

Licéité, loyauté, transparence	Le traitement a un **fondement juridique**, les personnes sont **informées** du traitement de leurs données	*Ex: le traitement est fondé sur l'une des 6 bases légales (art. 6) , des mentions légales, politiques de protection des données interne et externe sont rédigées*
Limitation des finalités	Les finalités du traitement sont **déterminées**, **explicites** et **légitimes** et **interdiction du détournement** de finalité	*Ex : Respecter les objectifs du traitements (ex: gestion des accès aux locaux)*
Qualité de la donnée	Les données doivent être **adéquates**, **pertinentes**, **limitées** à ce qui est nécessaire, **exactes** et tenues **à jour**	*Ex : Ne pas collecter de données non nécessaires au traitement, ne pas conserver des données obsolètes*
Limitation de la conservation	Pour chaque traitement il y a lieu de déterminer les **durées de conservation** des données	*Ex : Prévoir l'archivage et la suppression des données une fois les objectifs du traitement remplis*
Confidentialité et intégrité	Des **mesures techniques et organisationnelles** sont à mettre en œuvre pour assurer la conformité des traitements	*Ex : Respecter les profils d'habilitation, les politiques en matière de sécurité, alerter des violations de données*

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

- **La Courneuve a pour obligation de disposer d'un registre des activités de traitement de données à caractère personnel**

Contenu du registre des activités de traitement	
	Identité et coordonnées du responsable de traitement
	Identité et coordonnées du responsable conjoint du traitement
	Identité et coordonnées du DPD
	Finalités
	Catégories de personnes concernées
	Catégories de données à caractère personnel
	Catégories de destinataires
	Transferts de données
	Délais prévus pour l'effacement
	Description générale des mesures de sécurité techniques et organisationnelles

- Le registre des activités de traitement a été initialisé
- Dans les cas où La Courneuve est sous-traitante, elle devra également tenir un registre sous-traitant

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

2/ LES EXIGENCES POUR LA COURNEUVE

Les obligations pour La Courneuve

- **La Courneuve, son CCAS et sa Caisse des Ecoles doivent tenir un registre des activités de traitement**
- **Le registre doit refléter les traitements existant au sein de la commune**
  - Les traitements ont été identifiés lors de l'audit mais ils doivent être mis à jour régulièrement.

Quand mettre à jour le registre?

- Vous faites **évoluer un processus**
- Vous souhaitez utiliser un **nouveau logiciel**
- Vous réalisez un **nouveau partenariat**
- Vous collectez une **nouvelle donnée**
- Vous décidez de **conserver plus longtemps** les données que vous collectez
- Vous transmettez les données à un **nouveau destinataire**
- Etc.

Comment mettre à jour le registre?

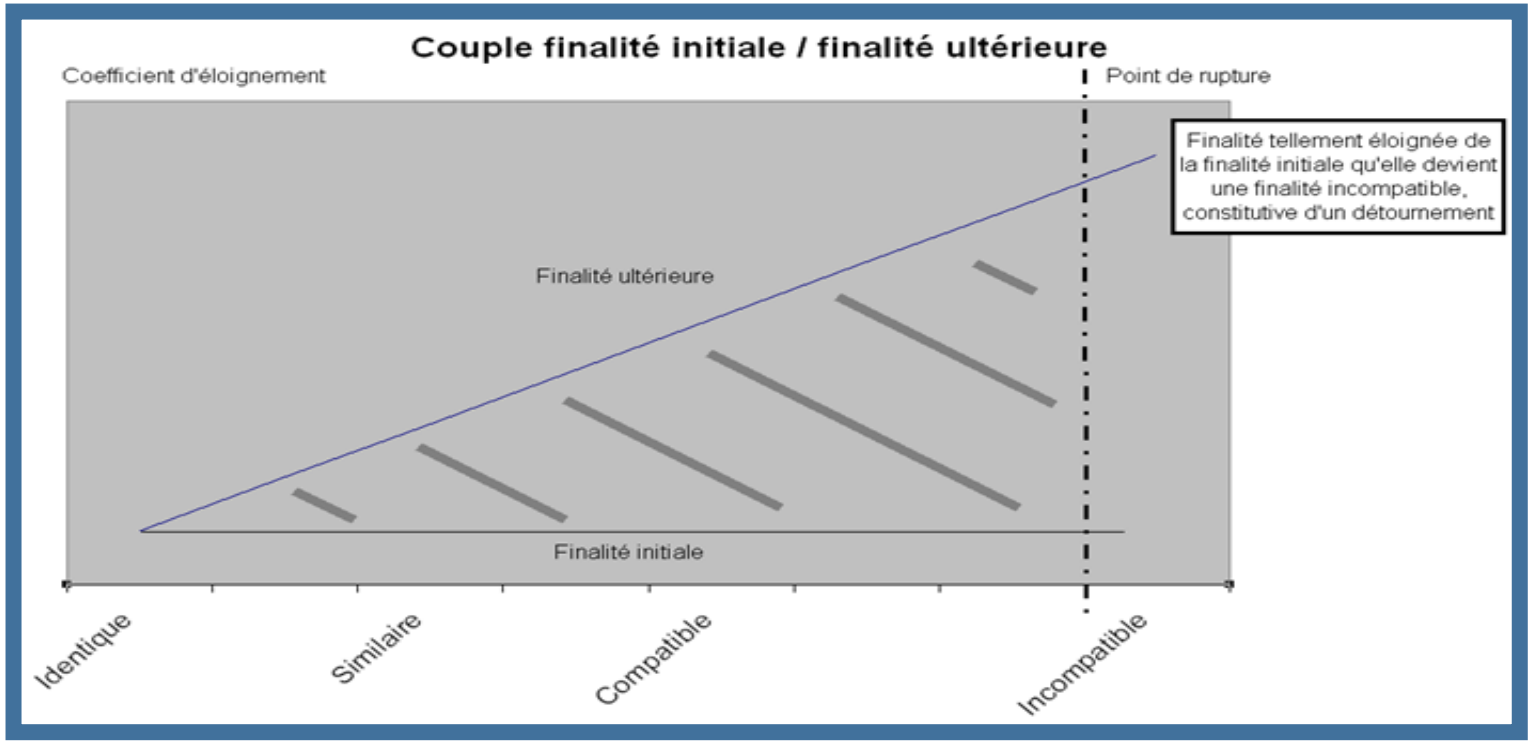
•**Mettre à jour la fiche** de traitement correspondante ou **créer une nouvelle fiche** de traitement avec l'accord du DPO

154 Fiches de Traitement ont été formalisées (144 pour la Commune, 7 pour le CCAS et 3 pour la Caisse des Ecoles)

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

➢ Chaque traitement doit respecter le principe de finalité

Les données doivent être collectées pour des **finalités déterminées, explicites et légitimes** et **ne pas être traitées ultérieurement d'une manière incompatible** avec ces finalités

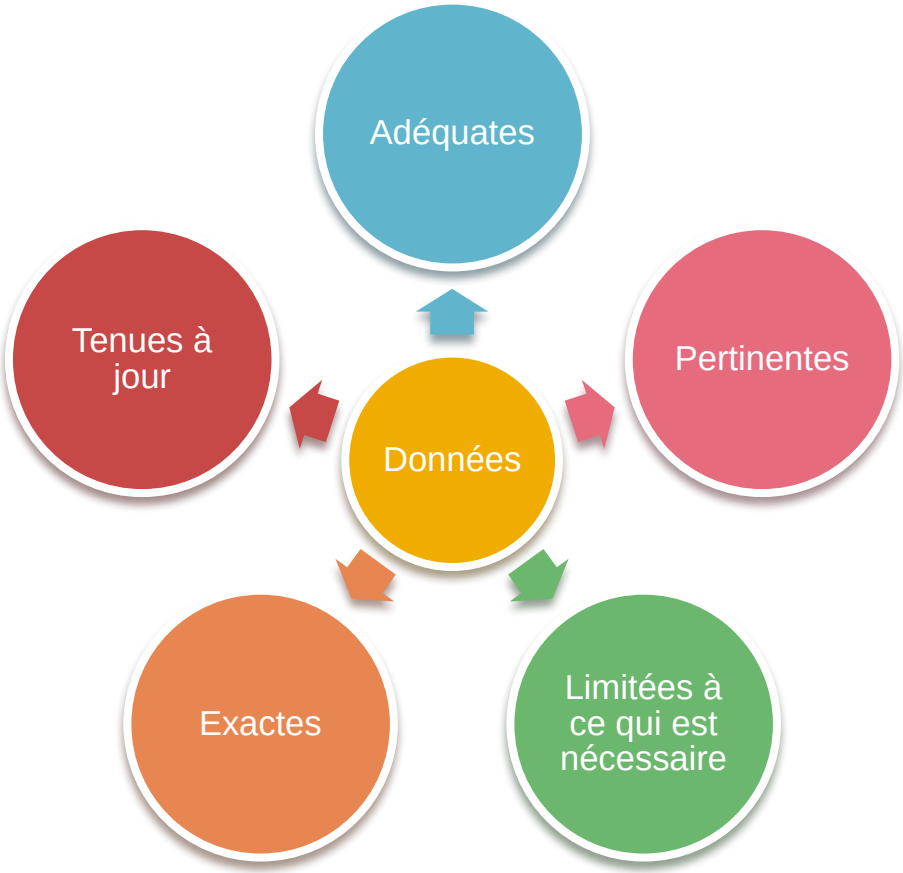


•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

2/ LES EXIGENCES POUR LA COURNEUVE

Les obligations pour La Courneuve

- **Les données de chaque traitement doivent respecter le principe de minimisation, être pertinentes, adéquates, tenues à jour et exactes**



•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

2/ LES EXIGENCES POUR LA COURNEUVE

Les obligations pour La Courneuve

- **Les durées de conservation des données doivent être cohérentes et justifiées au regard de l'objectif de leur traitement.**
- 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

1. Détermination des durées de conservation pour chaque traitement
2. Les intégrer au sein d'une politique de durée de conservation
3. Prévoir une purge définitive des données personnelles

Prescriptions / dates butoirs

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

➢ Exemple de référentiel

N°	TRAITEMENT	PRECISION CONCERNANT LE TRAITEMENT	ARCHIVAGE COURANT	ARCHIVAGE INTERMEDIAIRE	ARCHIVAGE DEFINITIF
1.	Gestion du recrutement	Candidatures retenues (lettre, CV, fichier de suivi, compte-rendu d'entretien)	Durée du recrutement	Eléments versés au dossier individuel de l'agent (cf. dossier individuel des agents, conservation jusqu'au 80 ans de l'agent à compter de la cessation de fonctions[1])	N/A
		Candidatures non retenues (lettre et CV) et réponse négative aux candidats	2 ans à compter du dernier contact avec le candidat[2]	3 ans à compter de la fin de l'archivage courant[3] (le délai de prescription de l'action en réparation du préjudice résultant d'une discrimination est de 5 ans à compter de la révélation de la discrimination sous réserve du délai butoir de 20 ans[4])	N/A
2.	Gestion administrative du personnel	Dossier individuel des agents (format papier)	1 an après la cessation de fonctions[5]	Jusqu'au 80 ans de l'agent à compter de la cessation de fonctions[6]	Tri interne à effectuer[7]
		Compte rendu d'évaluation de l'entretien annuel	15 ans[8]		Conservation[9]

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

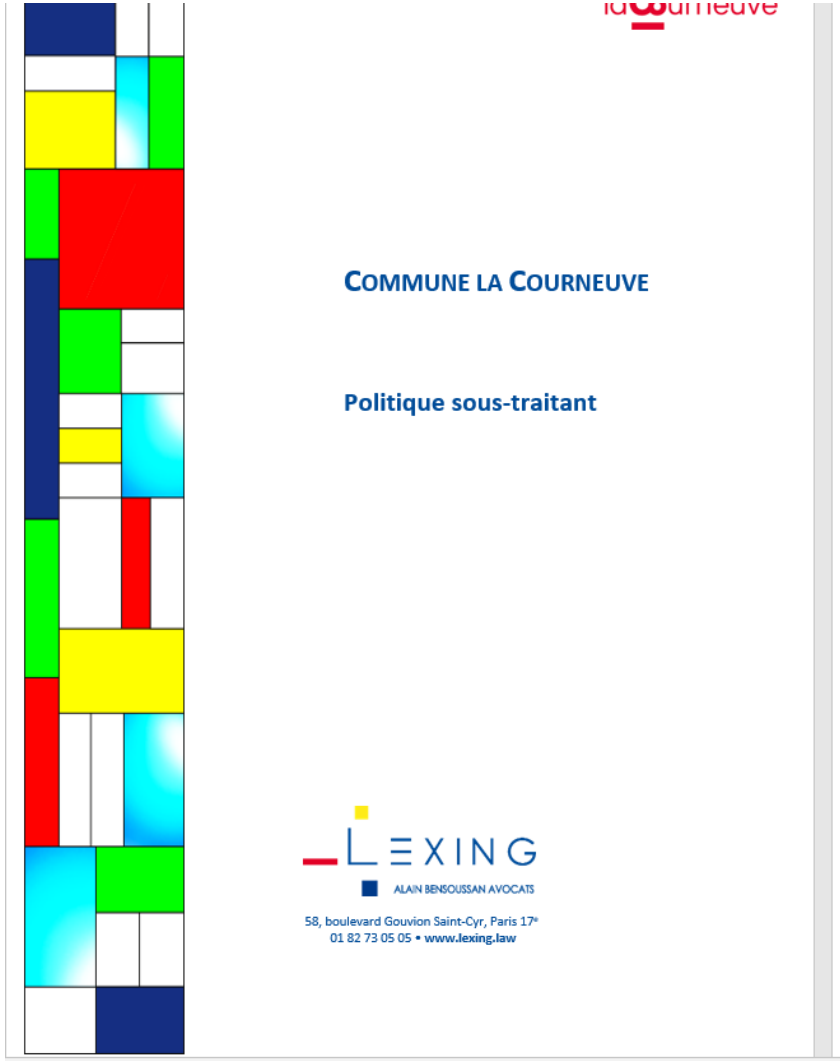
➢ La sous-traitance doit être encadrée

- Donner des garanties suffisantes sur la mise en œuvre de mesures appropriées
- Conclure un contrat de sous-traitance avec le responsable de traitement → ST ne traite des données que sur instructions écrites du RT
- Garantir la sécurité et la confidentialité des données traitées et garantir l'exercice des droits des personnes concernées
- Mise à disposition du client des informations lui permettant de démontrer qu'il a respecté ses obligations en qualité de responsable du traitement ou pour permettre la réalisation d'audits
- Notification au client, dans les meilleurs délais après en avoir pris connaissance, de toute violation de ses données
- Obtenir l'autorisation préalable du client en cas de sous-traitance et faire appel à un sous-traitant qui présente des garanties suffisantes ; conclure un contrat avec le sous-traitant ultérieur
- Tenir un registre des catégories d'activités de traitement mis en œuvre pour le compte du client

Exemple de sous-traitance : une collectivité peut décider de confier la maintenance informatique à une société. La société est alors le sous-traitant de la collectivité au sens du RGPD.

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

➢ Politique sous-traitant

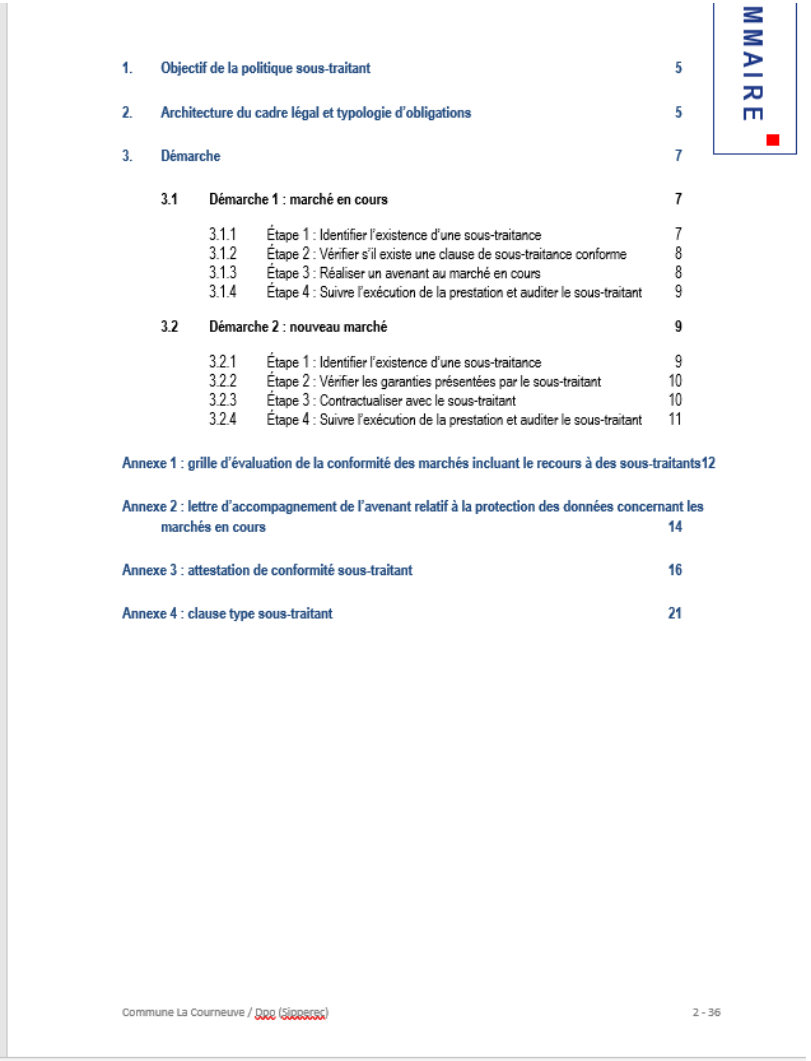


COMMUNE LA COURNEUVE

Politique sous-traitant

LEXING
ALAIN BENSOUSSAN AVOCATS

58, boulevard Gouvion Saint-Cyr, Paris 17e
01 82 73 05 05 • www.lexing.law



MMAIRE

1. Objectif de la politique sous-traitant 5

2. Architecture du cadre légal et typologie d'obligations 5

3. Démarche 7

3.1 Démarche 1 : marché en cours 7

3.1.1 Étape 1 : Identifier l'existence d'une sous-traitance 7
3.1.2 Étape 2 : Vérifier s'il existe une clause de sous-traitance conforme 8
3.1.3 Étape 3 : Réaliser un avenant au marché en cours 8
3.1.4 Étape 4 : Suivre l'exécution de la prestation et auditer le sous-traitant 9

3.2 Démarche 2 : nouveau marché 9

3.2.1 Étape 1 : Identifier l'existence d'une sous-traitance 9
3.2.2 Étape 2 : Vérifier les garanties présentées par le sous-traitant 10
3.2.3 Étape 3 : Contractualiser avec le sous-traitant 10
3.2.4 Étape 4 : Suivre l'exécution de la prestation et auditer le sous-traitant 11

Annexe 1 : grille d'évaluation de la conformité des marchés incluant le recours à des sous-traitants 12

Annexe 2 : lettre d'accompagnement de l'avenant relatif à la protection des données concernant les marchés en cours 14

Annexe 3 : attestation de conformité sous-traitant 16

Annexe 4 : clause type sous-traitant 21

Commune La Courneuve / Dpo (Sipparsc) 2 - 36

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

➢ Modèle de clause de sous-traitance

Annexe 4 : clause type sous-traitant

1. Clause à insérer au sein des marchés

1. DONNÉES A CARACTÈRE PERSONNEL

[À compléter] a la qualité de sous-traitant de la Commune de La Courneuve et effectue des traitements de données à caractère personnel pour son compte.

[À compléter] déclare être en conformité avec la réglementation en vigueur applicable aux traitements de données à caractère personnel et en particulier au règlement (UE) 2016/679 du 27 avril 2016 ainsi qu'aux dispositions de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Les termes « Responsable de traitement » et « Sous-traitant » doivent être compris au sens de l'article 4 du règlement (UE) 2016/679 du 27 avril 2016.

Les rôles et responsabilités de chacune des Parties en matière de protection des données personnelles sont fixés en Annexe X.

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

2/ LES EXIGENCES POUR LA COURNEUVE

Les obligations pour La Courneuve

- **Les mesures de sécurité doivent permettre de réduire les risques sur les traitements**

Gérez les habilitations et sensibilisez les utilisateurs

- définissez des profils d'habilitation
- supprimez les permissions d'accès obsolètes
- documentez les procédures d'exploitation

Authentifiez les utilisateurs

- définissez un identifiant (login) unique à chaque utilisateur
- respectez une politique de mot de passe utilisateur rigoureuse
- obligez l'utilisateur à changer son mot de passe régulièrement

Sécurisez les postes de travail

- limitez le nombre de tentatives d'accès à un compte
- installez un « pare-feu » (firewall)
- utilisez des antivirus régulièrement mis à jour
- prévoyez une procédure de verrouillage automatique de session

Sauvegardez et prévoyez la continuité d'activité

- effectuez des sauvegardes régulières
- stockez les supports de sauvegarde dans un endroit sûr
- chiffrez les sauvegardes

Sécurisez l'informatique mobile

- prévoyez des moyens de chiffrement pour les ordinateurs portables et les unités de stockage amovibles (clés USB, CD, DVD…)

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

➢ Définir et diffuser les règles en matière de protection des données

Encadrez la maintenance

- enregistrez les interventions de maintenance dans une main courante
- effacez les données de tout matériel avant sa mise au rebut
- prévoyez de rendre impossible l'accès au contenu des bases de données aux prestataires techniques

Protégez le réseau informatique interne

- limitez les flux réseau au strict nécessaire
- sécurisez les accès distants des appareils informatiques nomades par VPN

Tracez les accès et gérez les incidents

- prévoyez un système de journalisation
- notifiez aux personnes concernées des accès frauduleux à leurs données

Sécurisez les serveurs et les applications

- adoptez une politique de mot de passe administrateur rigoureuse
- installez sans délai les mises à jour critiques
- assurez une disponibilité des données

Sécurisez les échanges

- chiffrez les données avant leur envoi
- assurez-vous qu'il s'agit du bon destinataire

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

➢ Conduire des analyse d'impact quand un traitement présente un risque pour les droits et libertés des personnes

Une procédure est en vigueur au sein de la commune et doit être suivie dans le cadre de la réalisation d'une analyse d'impact

laCourneuve	Politique et procédure d'Analyse d'Impact	wiseorga

Politique et procédure d'Analyse d'Impact (Art.35 RGPD)

Résumé

Cette procédure permet d'expliciter la démarche relative aux analyses d'impact relative à la protection des données et d'assurer, le cas échéant, leur mise en place dans le cadre de la mise en œuvre d'un nouveau traitement ou de l'évolution majeure d'un traitement risquant d'engendrer un risque élevé sur les droits et libertés des personnes.

Exemples de traitements soumis à l'analyse d'impact : Gestion des aides légales et facultatives, gestion de la vidéoprotection, gestion de la paie et des déclarations obligatoires concernant les agents, gestion des risques sanitaires..

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

➢ Réaliser des analyses d'impact pour les traitements à risque

Lorsque les traitements de données personnelles sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées, il est nécessaire de réaliser une analyse d'impact

- Evaluation ou notation
- Prise de décisions automatisée avec effet juridique ou effet similaire significatif
- Surveillance systématique
- Données sensibles ou données à caractère hautement personnel
- Données traitées à grande échelle
- Croisement ou combinaison d'ensembles de données
- Données concernant des personnes vulnérables
- Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles
- Traitements en eux-mêmes qui empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat

→ Si deux critères ou plus sont remplis, une analyse d'impact est nécessaire.

➢ Qui réalise les analyses d'impact ?

La direction mettant en œuvre le traitement est en charge de l'analyse d'impact.
Le délégué à la protection des données personnelles conseille sur l'opportunité de mener une analyse d'impact et supervise sa réalisation.

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

➢ Les violations de données doivent être suivies

Une violation de données personnelles se comprend comme une atteinte à (critères non cumulatifs) :

la **CONFIDENTIALITÉ** : un tiers non autorisé a accès à la donnée

- Un agent de La Courneuve communique par erreur un fichier contenant une base de données clients à un tiers non autorisé
- Vol d'un ordinateur de La Courneuve

l'INTÉGRITÉ : la donnée a été altérée

- Un hacker s'introduit dans le système d'information RH et modifie les salaires de l'ensemble des agents de La Courneuve

la **DISPONIBILITÉ** : la donnée n'est plus accessible

- Un agent supprime accidentellement une partie d'une base de données, non sauvegardée par ailleurs, ne permettant plus l'utilisation des applicatifs de gestion

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

2/ LES EXIGENCES POUR LA COURNEUVE

Les obligations pour La Courneuve

- **En cas de violation de données personnelles, il peut être nécessaire de notifier à la CNIL dans les 72 heures**

Afin de protéger les administrés et les agents et de se conformer à la réglementation, la commune doit mettre en place des mesures visant à :

- **PRÉVENIR** d'éventuelles violations de données
  - *détections informatiques automatisées*
  - *sensibilisations des agents*, etc.

- **RÉAGIR** de manière appropriée en cas de violation
  - *procédure de remontée d'information*
  - *processus de notification CNIL*
  - *registre des violations de données*

Chaque violation de donnée à caractère personnel doit a minima faire l'objet d'une inscription au sein d'un **registre** prévu à cet effet au sein de la commune

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

➢ Les demandes d'exercice de droit doivent être gérées et suivies

Droit d'**accès**

Droit de **rectification**

Droit d'**opposition**

Droit d'**information renforcée**

Droit à l'**effacement** (droit à l'**oubli**)

Droit à la **limitation** du traitement

Droit à la **portabilité** des données

Nouveautés issues du RGPD

➢ Comment gérer une demande d'exercice de droit ?

La Courneuve doit répondre à une demande d'exercice de droit dans un délai d'un mois à compter de la date de réception de la demande

A l'issue de ce délai, la personne concernée peut déposer une plainte auprès de la Cnil

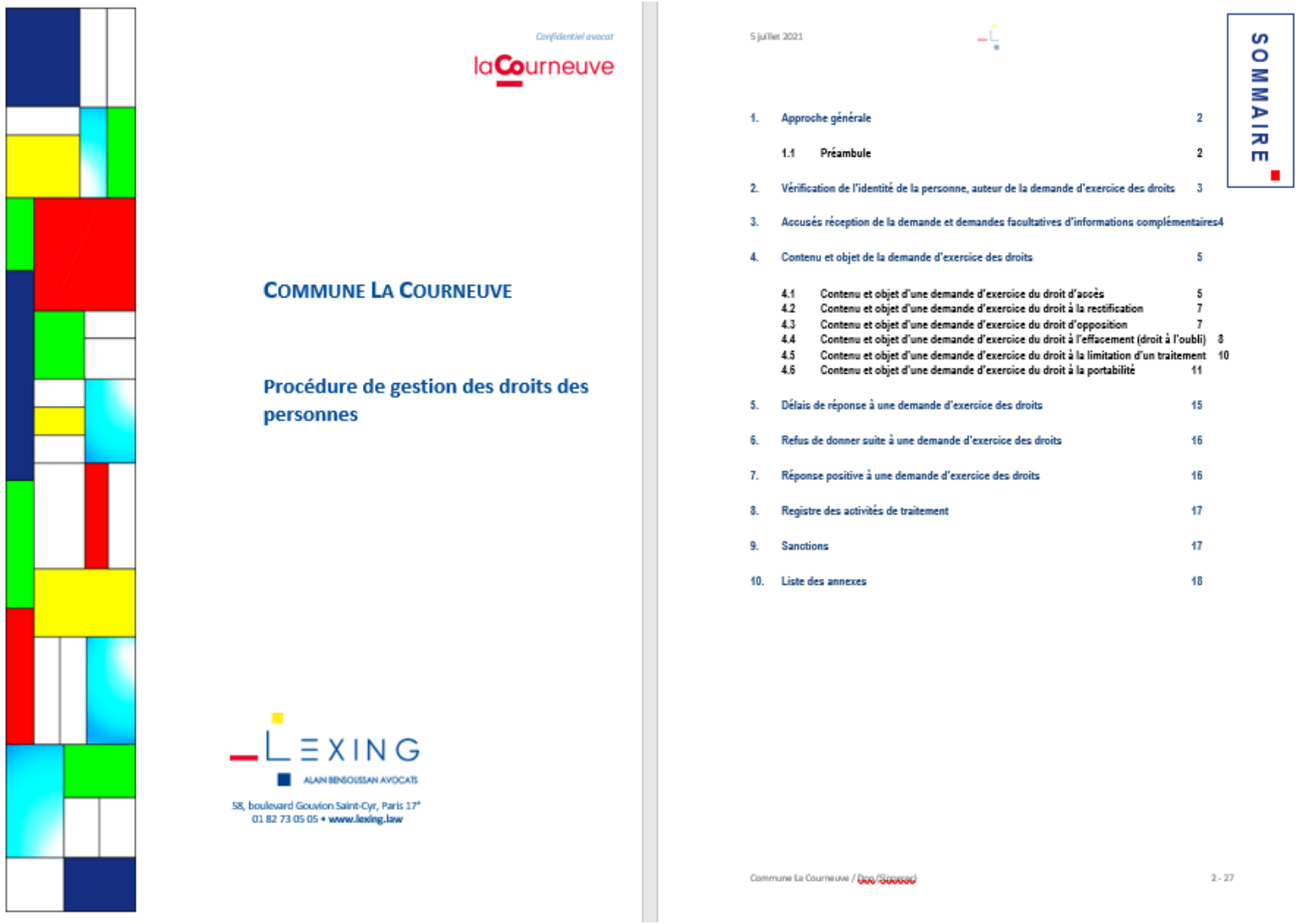
Remonter immédiatement la demande d'exercice de droit au DPO

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

2/ LES EXIGENCES POUR LA COURNEUVE

Les obligations pour La Courneuve

➢ Procédure de gestion des droits des personnes



Confidentiel avocat

laCourneuve

COMMUNE LA COURNEUVE

Procédure de gestion des droits des personnes

LEXING
ALAIN BENSOUSSAN AVOCATS
58, boulevard Gouvion Saint-Cyr, Paris 17e
01 82 73 05 05 • www.lexing.law

5 juillet 2021

SOMMAIRE

1. Approche générale 2
   1.1 Préambule 2
2. Vérification de l'identité de la personne, auteur de la demande d'exercice des droits 3
3. Accusés réception de la demande et demandes facultatives d'informations complémentaires 4
4. Contenu et objet de la demande d'exercice des droits 5
   4.1 Contenu et objet d'une demande d'exercice du droit d'accès 5
   4.2 Contenu et objet d'une demande d'exercice du droit à la rectification 7
   4.3 Contenu et objet d'une demande d'exercice du droit d'opposition 7
   4.4 Contenu et objet d'une demande d'exercice du droit à l'effacement (droit à l'oubli) 8
   4.5 Contenu et objet d'une demande d'exercice du droit à la limitation d'un traitement 10
   4.6 Contenu et objet d'une demande d'exercice du droit à la portabilité 11
5. Délais de réponse à une demande d'exercice des droits 15
6. Refus de donner suite à une demande d'exercice des droits 16
7. Réponse positive à une demande d'exercice des droits 16
8. Registre des activités de traitement 17
9. Sanctions 17
10. Liste des annexes 18

Commune La Courneuve / Dpo (Sioueed) 2 - 27

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

➢ Dès modèles figurent en annexe de la procédure

[Chère Madame, Cher Monsieur]

Nous accusons bonne réception de votre demande de droit [indiquer le droit exercé] exercée par [lettre recommandée avec demande d'avis de réception du (.) / courriel du (.)] dans laquelle / lequel vous formulez une demande de droit [indiquer le droit exercé] [en votre qualité de mandataire de Madame/Monsieur (.)].

Nous traitons votre demande dans les meilleurs délais et, en tout état de cause, dans un délai d'un mois à compter de la réception de votre courrier.

Vous souhaitant bonne réception de la présente, veuillez agréer, [Chère Madame, Cher Monsieur], nos salutations distinguées.

[Délégué à la protection des données]

Afin de pouvoir traiter votre demande d'exercice des droits, la Commune de La Courneuve a besoin de recueillir des informations vous concernant. Vos données à caractère personnel sont en effet nécessaires pour nous permettre de répondre à votre demande d'exercice du droit [indiquer le droit exercé]. Ce traitement est effectué conformément à une obligation légale à laquelle la Commune de La Courneuve est soumis. Ces informations sont destinées aux personnes habilitées de la Commune de La Courneuve et sont conservées pendant un an à compter du jour de votre demande. Conformément à la réglementation en matière de protection des données personnelles, vous pouvez accéder aux données vous concernant, les rectifier, demander leur effacement ou exercer votre droit à la limitation du traitement de vos données. Vous disposez également d'un droit d'opposition à ce que vos données soient utilisées à des fins de prospection commerciale. Vous disposez enfin du droit de définir la manière dont vous entendez que soient exercés ces droits après votre décès.

Ces droits peuvent être exercés en adressant un courrier à l'adresse suivante : dpo@ville-la-courneuve.fr ou à l'adresse postale suivante : Mairie de la Courneuve, Délégué à la protection des données, Avenue de la République,93120 La Courneuve, France ; vous pouvez justifier de votre identité par tout moyen.
Si vous estimez, après nous avoir contactés, que vos droits ne sont pas respectés, vous pouvez adresser une réclamation à la Commission nationale de l'informatique et des libertés.

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

➢ **Définir et diffuser les règles en matière de protection des données**

Politiques générales

- Politique de protection des données/de confidentialité
- Charte des systèmes d'information

Politiques thématiques

- Politique cookies et bandeau cookies
- Politique de gestion des droits des personnes et processus
- Politique sous-traitant
- Mentions légales
- Mentions d'information
- Politique d'analyse d'impact
- Politique de protection des données dès la conception et par défaut

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

SOMMAIRE

1/ DÉFINITIONS ET ENJEUX DE LA PROTECTION DES DONNÉES PERSONNELLES

2/ LES EXIGENCES POUR LA COURNEUVE

3/ MISE EN ŒUVRE OPÉRATIONNELLE VIA UN RESEAU DE RILS

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

3/ MISE EN ŒUVRE OPERATIONNELLE VIA UN RESEAU DE RILS

Un réseau de RILs au service de la protection des données

La cellule interne est composée de :

- **Florence LAGERE (DGA Ressources) - Sponsor**
- François PERRIN (DRH)
- Belkacem CHIKH (Responsable des affaires financières et de la commande publique)
- Catherine SOUTOUL (DSI)
- Mamadou INDFAI (Chef de projet SI)
- Olivier LEGRAS (Responsable unité technique)
- Andres GIRON TAFOURT (Chargé des affaires juridiques et du contentieux)
- Pascale FOURNIER (Directrice de la Communication)

DPO / Assistance DPO et cellule transverse

Responsables Opérationnels des traitements par Direction

Référents Informatiques et Libertés (RILs)

• La cellule de protection des données interne s'assure de la **mise en conformité de la commune de La Courneuve ainsi que de son maintien**
• Une **instance de contrôle permanent** sera à mettre en place à terme
• Le DPO **coordonne et s'assure de la conformité de la commune au RGPD** dans le temps.

Les Directeurs et directrices des services sont chargés de :

- **valider les Fiches de traitement** ;
- s'assurer de la **mise en œuvre des préconisations du DPO** par les RILs dans leurs périmètres de responsabilités ;
- s'assurer que le **RIL dispose du temps nécessaire à la bonne exécution de sa mission**.

- Les Référents Informatiques et Libertés au niveau des services sont chargés :
- **relais descendant** : Le RIL **diffuse au sein de son service** les bonnes pratiques et procédures à respecter. Il devra participer à des revues ;
- **relais ascendant** : Le RIL doit **remonter au DPO** les questions, les difficultés rencontrées ou les spécificités locales telles que des exigences règlementaires spécifiques afférentes à l'activité, des contraintes métiers particulières etc … .

- Ils sont les **appuis récurrents au sein des directions métiers** afin de diffuser et remonter les informations et bonnes pratiques RGPD.

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

Référents Informatiques et Libertés (RILs)

Le RIL remplit trois rôles :

- **Rôle de prévention et médiation** : *ambassadeur de la protection des données (information, sensibilisation, communication, suivi de réalisation des actions), point de contact et coordinateur* ;
- **Rôle de conseil et d'accompagnement** : *aider les équipes à anticiper les besoins de protection des données, à identifier les traitements et enjeux, apporter conseil et méthode aux équipes pour assurer la conformité des traitements* ;
- **Rôle d'orchestrateur et de contrôleur de la conformité** : *reporting, mise à jour du registre, suivi des plans d'action et mesures, alerte et transmission des informations en cas de violation de données, accompagnement de la réalisation des demandes d'exercice de droits, participation aux cellules de crise*.

Extrait de la fiche de mission du RIL

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS

3/ MISE EN ŒUVRE OPERATIONNELLE VIA UN RESEAU DE RILS

Les activités opérationnelles du RIL

Ambassadeur de la protection des données (information, sensibilisation, communication, suivi de réalisation des actions), point de contact et coordinateur

Être le relai des bonnes pratiques en matière de protection des données avec les opérationnels, participer aux sessions de sensibilisation / aux sessions d'animation organisées avec l'équipe DPO, déployer les bonnes pratiques de protection des données (processus, politiques) auprès des opérationnels

Aider les équipes à anticiper les besoins de protection des données, à identifier les traitements et enjeux, apporter conseil et méthode aux équipes pour assurer la conformité des traitements

Collecter des informations nécessaires à la création / modification des fiches de traitement, évaluer le niveau de sensibilité des nouveaux sous-traitants et proposer des clauses RGPD adaptées, informer l'équipe DPO en cas de nouveau traitement / nouvel outil / nouveau formulaire, faire le relais entre l'équipe DPO et l'équipe opérationnelle et les sous-traitants dans le cadre de la réalisation d'analyses d'impact…

Garantir le maintien en conformité des traitements et transmettre un *reporting* régulier

Réaliser des contrôles réguliers des traitements, formaliser les résultats des contrôles dans un tableau de bord, transmettre régulièrement le tableau de bord des contrôles réalisés à l'équipe DPO…

Alerte et transmission des informations en cas de violation de données, accompagnement de la réalisation des demandes d'exercice de droits, participation aux cellules de crise

Collecter les informations utiles sur les violations de données, informer l'équipe DPO sans délai en cas de violation, participer aux cellules de crise, informer l'équipe DPO des demandes d'exercice de droits, collecter les données personnelles demandées en cas d'exercice du droit d'accès, transmettre rapidement les éléments à l'équipe DPO…

•© Ce document ne peut pas être diffusé ou reproduit sans l'autorisation du Groupement WISEORGA SAS et ALAIN BESOUSSAN AVOCATS