seine-saint-denis
LE DÉPARTEMENT

Réglement Général sur la Protection des Données

Règlement Général de la protection des données (RGPD)

Conférence « 25 mai 2018 : les jours d'après »
11 octobre2018

+ Offre de services de la DSA

MOIS EUROPÉEN DE LA CYBERSÉCURITÉ

Délégué à la protection des données

Fabrice IDIER RSSI / DPO

Sommaire

Le RGPD POURQUOI ? Enjeux

seine-saint-denis
LE DÉPARTEMENT

RESSOURCES
ET MOYENS
DES SERVICES

- Le règlement européen RGPD consiste à **protéger les données personnelles** pour les résidents de l'Union Européenne,
- harmonise les législations européennes en matière de protection des données à caractère personnel,
- cadre l'économie numérique Européenne,
- Favorise l'innovation tout en garantissant un niveau de protection élevé.

Impacts :

- **renforce les droits** en matière de respect de la vie privée,
- **impose des mesures de sécurité** pour protéger l'intégrité et la confidentialité des données,

S'intègre à la stratégie numérique départementale adoptée en décembre 2016, Ambition 2 « mettre nos biens communs numériques au service des innovations de demain »

Qu'est ce que le RGPD ?

seine-saint-denis
LE DÉPARTEMENT

RESSOURCES
ET MOYENS
DES SERVICES

Réglementation

- ✓ Définissant les **droits des individus**
- ✓ Etablissant les **obligations** de ceux qui traitent et de ceux qui sont responsables du traitement des données
- ✓ Etablissant les **méthodes** permettant d'assurer la conformité ainsi que la portée des **sanctions** de ceux qui ne respectent pas les règles

RGPD = Loi informatique et Libertés modifiée

+ Nouvelles Obligations

- Formalités déclaratives préalables

En complément ,

la **LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles** complète ou modifie la loi 78-17 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés (LIL 3)

Une LIL 4 est prévue avant le 20 juin 2019

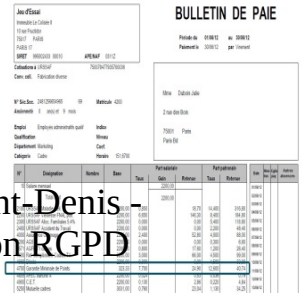
Une étendue très large des Données à Caractère Personnel (« DCP »)

seine-saint-denis
LE DÉPARTEMENT

RESSOURCES ET MOYENS DES SERVICES

se rapportant à une personne physique identifiée ou identifiable Directement ou Indirectement

- Identité individuelle (nom, lieu & date de naissance , NIR, adresse, immatriculation véhicule, taille, poids, voix , image…)
- Vie personnelle (habitudes de vie, situation familiale,…)
- Informations professionnelles (CV, statut professionnel, scolarité, formation professionnelles, salaire,…)
- Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, ..)
- Données bancaires & fiscales (N° carte bancaire, IBAN, situation fiscale,…)
- Données de connexion ((adresse IP, journaux d'événements, traces internet)
- Données de localisation (géolocalisation, données GPS, déplacements ,…)



« DONNEES SENSIBLES » :

seine-saint-denis
LE DÉPARTEMENT

RESSOURCES ET MOYENS DES SERVICES

Interdiction de principe du traitement de données personnelles sensibles sauf exception

- Données révélant l'origine raciale ou ethnique
- Données révélant les opinions politiques
- Données révélant les convictions religieuses ou philosophiques
- Données révélant l'appartenance syndicale
- Données **génétiques**
- Données **biométriques** aux fins d'identifier une personne physique de manière unique
- Données concernant la santé
- Données concernant la vie sexuelle ou **l'orientation sexuelle**

Protection particulière de certaines données « à risques » :

- Données relatives à des condamnations pénales et aux infractions ou mesures de sûreté
- Numéro d'identification national unique (NIR pour la France) : soumis à autorisation préalable de la CNIL, après avis motivé et publié de la CNIL, essentiellement limité à la sphère SANTE-SOCIAL-TRAVAIL
- Données relatives aux mineurs
- Données bancaires (RIB)
- …

Est défini comme :
« toute opération ou tout ensemble d'opérations effectués ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel »

- Ces traitements **NUMERIQUES** OU **PAPIERS** peuvent être liés tant au fonctionnement, à la gestion de l'administration, qu'à ses missions ou son cœur d'activité :
  1. Traitements liés au fonctionnement (**INTERNE**)
  2. Traitements liés à ses missions (**USAGERS**)

Quelques exemples d'opérations considérées comme des traitements :

- la collecte
- l'enregistrement
- l'organisation, la structuration,
- la conservation
- l'adaptation ou la modification
- l'extraction, la consultation,
- l'utilisation
- la communication par transmission,
- la diffusion ou toute autre forme de mise à disposition
- le rapprochement ou l'interconnexion,
- la limitation
- l'effacement ou la destruction

Les acteurs de la mise en œuvre des traitements

seine-saint-denis
LE DÉPARTEMENT

RESSOURCES ET MOYENS DES SERVICES

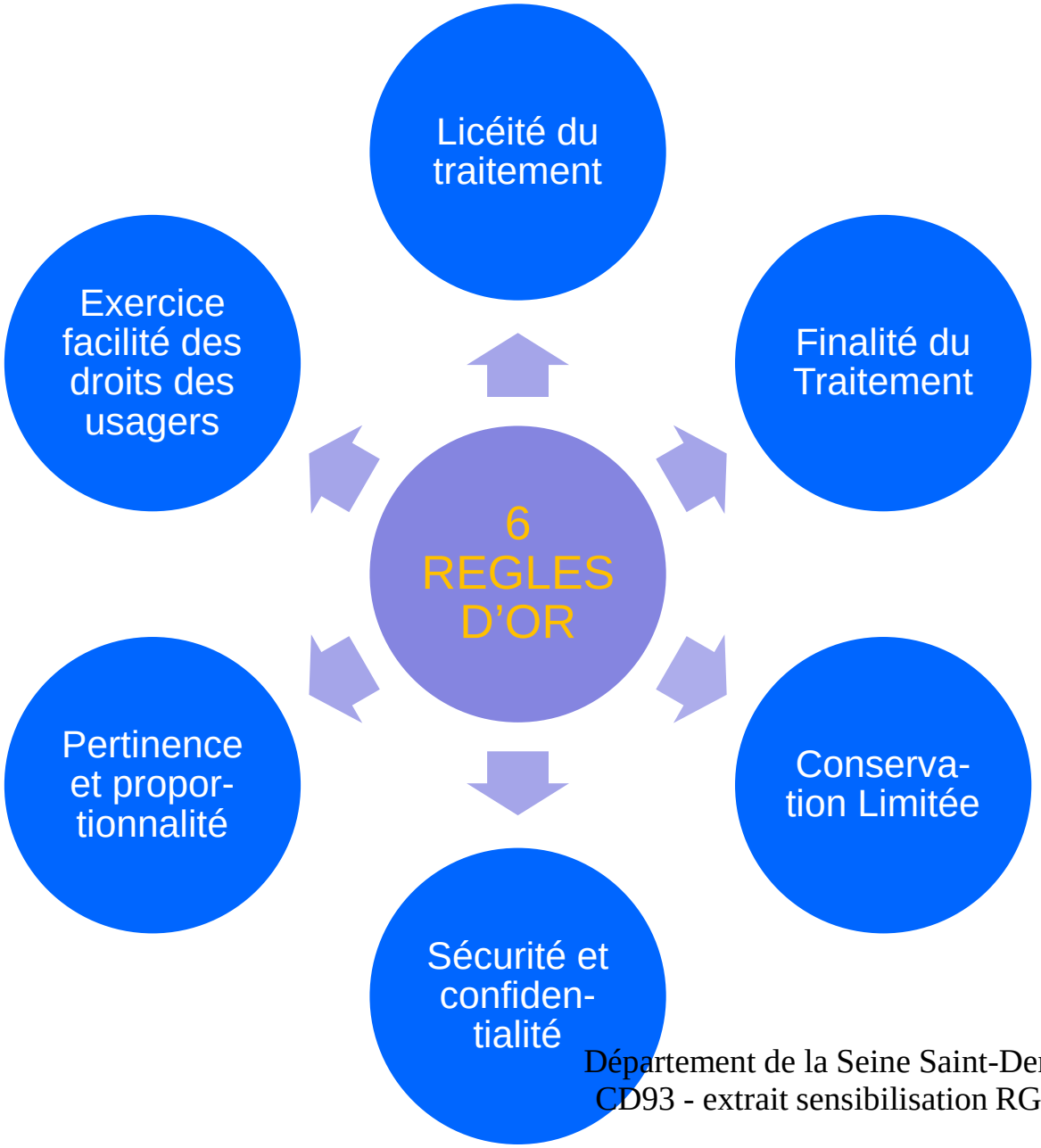
- **Le responsable du traitement (RT) = responsable de la collecte et l'exploitation des données**
  - Le président du Conseil départemental
  - Les directeurs et chefs de service qui déterminent les finalités et les moyens du traitement, qui organisent la collecte et le traitement des données

- **Le sous-traitant (ST) = titulaire d'un marché public ou d'un contrat :**
  - Toute personne traitant des données à caractère personnel pour le compte, sous la direction et la responsabilité du responsable du traitement .
  - Doit présenter des garanties suffisantes pour assurer la sécurité et la confidentialité des données
    - un enjeu de marché public
- **L'urbaniste :**
  - Aide les directions métiers à définir et optimiser leurs traitements
- **L'auditeur :** s'assure de la mise en œuvre des processus et règles indispensables dans les directions métiers
- Le Correspondant Informatique et Libertés laisse la place au **Délégué Protection des données** :

Synergie RSSI / DPO

Un RSSI devenu indispensable
Définir la politique de sécurité des systèmes d'information
Sensibiliser aux enjeux de la sécurité informatique
Auditer la sécurité (vérification des mesures prises, tests d'intrusion, …)
Analyser les risques sur le système d'information ou les projets informatiques
Coopérer avec les autorités de contrôle, auditeurs, DPO
Mettre en place des indicateurs de la sécurité des systèmes d'information (incidents de sécurité, violation DCP,…)

Un Délégué à la protection des données obligatoire
Définir la politique de la donnée à caractère personnel
Sensibiliser aux enjeux de la protection des données
Informer , conseiller , accompagner
Contrôler le respect du règlement y compris en ce qui concerne les audits s'y rapportant (article 39, al.1 b)
Conseiller le responsable de traitement sur l'opportunité de réaliser une **analyse d'impact sur la vie privée** et d'en vérifier l'exécution
Recevoir et répondre aux réclamations relatives à la protection des données
Coopérer avec la CNIL et être son point de contact dans la collectivité



IMPACT ADMINISTRATION :

- Principe de protection des données par défaut dès la création / conception d'un traitement :
- Apurement régulier des données :
- Information des usagers sur leurs droits
- Mesures de sécurité

➡ *des nouvelles fonctionnalités à exiger dans les logiciels utilisés*

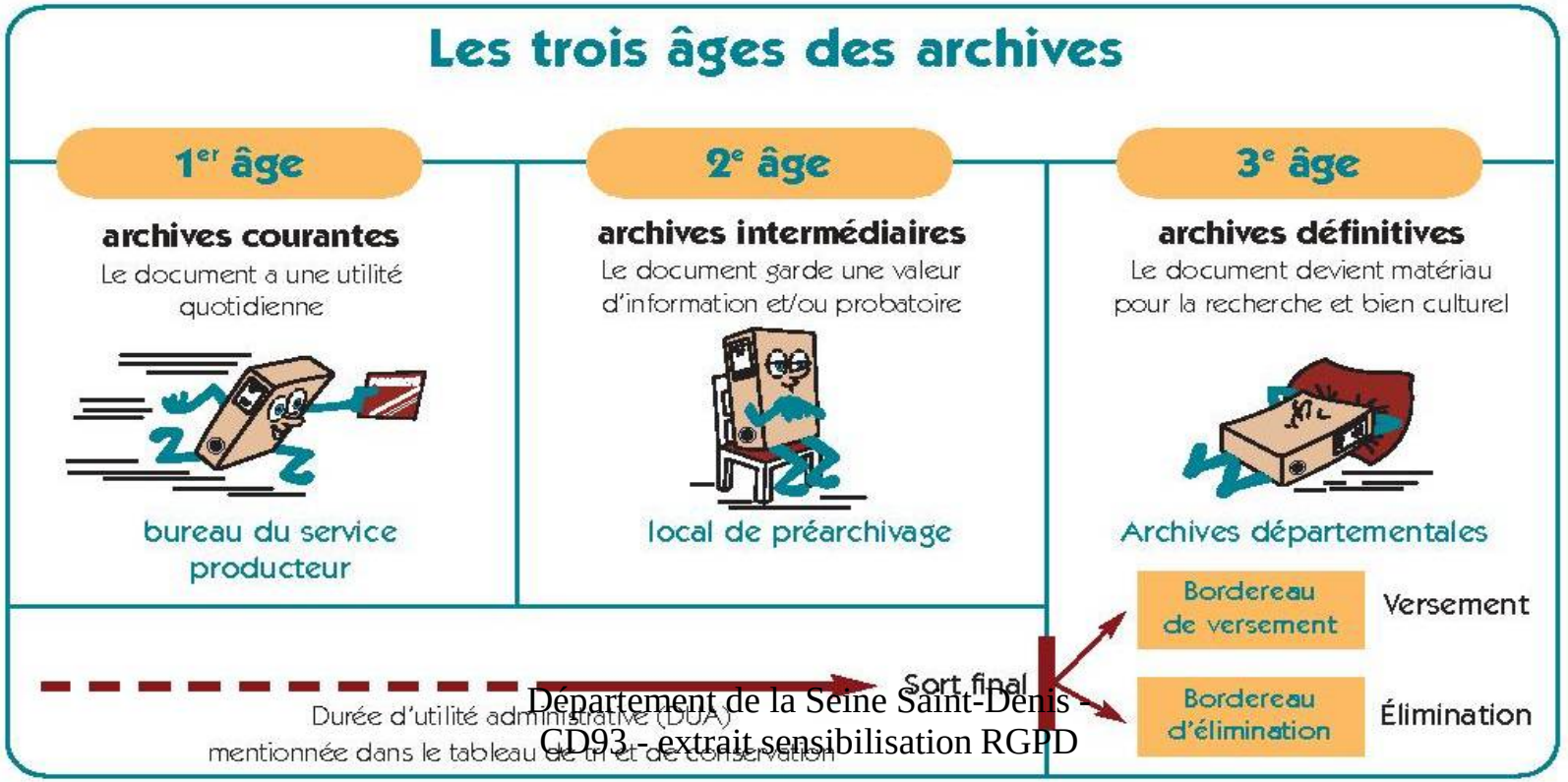
➡ *Conventions à modifier*

Qu’entend-on par archives?

RESSOURCES ET MOYENS DES SERVICES

- « Les **archives** sont l'ensemble des documents, y compris les données, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité. » (*Code du patrimoine*, article L211-1).

- Le Département produit des **archives publiques**. Elles sont :
  - Inaliénables
  - Imprescriptibles



Les archives dans le RGPD

seine-saint-denis
LE DÉPARTEMENT

RESSOURCES ET MOYENS DES SERVICES

- Le RGPD prévoit un **régime dérogatoire** pour les archives publiques.

L'exercice des droits des personnes est limité, le RGPD pose des conditions.

- **Art.5 du RGPD** (principes relatifs aux traitements) → Le traitement des données à des fins archivistiques n'est pas considéré comme incompatible avec les finalités initiales.
- **Art.17 du RGPD** (droit à l'effacement ou « droit à l'oubli ») → Le droit à l'effacement ne s'applique pas lorsque le traitement des données est nécessaire à l'exécution d'une mission d'intérêt public ou « à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ».
- **Art. 89 du RGPD et art.14 de la Loi CNIL 3**. → Les articles 15 (accès), 16 (rectification), 18 à 21 (limitation, portabilité, opposition) ne s'appliquent pas si le traitement des données est mis en œuvre par un service public d'archives « à des fins archivistiques [...] ».

- Le RGPD vise les **données à caractère personnel, quelque soit leur support** (numérique, papier, audiovisuel...).

La DSA vous accompagne

seine-saint-denis
LE DÉPARTEMENT

RESSOURCES
ET MOYENS
DES SERVICES

- Par son accompagnement des services dans leur archivage, **la DSA contribue à leur mise en conformité au RGPD** :

✓ conseil pour l'organisation des archives.

✓ information sur les durées de conservation des archives et validation des demandes d'éliminations (principe de limitation des traitements).

✓ informations sur les délais de communicabilité (respect de la vie privée).

✓ aide à l'organisation des données dans un processus de dématérialisation.

- **Des outils sont disponibles sur** e-acteurs

  Mes essentiels > J'utilise mes outils de travail > Les guides utiles.

- **Contacts :**

P. J, responsable du service des archives publiques

N. L., cheffe de projet Archives électroniques et système d'information

NOUVEAU MODE DE REGULATION : Principe de responsabilité

seine-saint-denis
LE DÉPARTEMENT

RESSOURCES ET MOYENS DES SERVICES

- **Principe de responsabilité (art.24) :** le responsable des traitements est responsable de l'ensemble des actions mises en œuvre pour protéger les données avec l'obligation de veiller au respect du règlement par le sous-traitant éventuel (art.29) .

Vers une nouvelle logique de responsabilité : AUDIT ET CONTRÔLE DE LA CNIL

Avec le RGPD, ce n'est plus l'autorité de contrôle (CNIL) qui doit prouver la non-conformité, c'est désormais le responsable de traitement de la collectivité qui doit démontrer sa conformité.

La CNIL s'oriente vers le soutien aux réseaux sectoriels, régionaux ou métiers qui deviendront ses interlocuteurs privilégiés.

IMPACT ADMINISTRATION :

- Disparition pour l'essentiel des formalités préalables
- Nécessité d'une documentation « auditable »
- Mener les analyses d'impact (PIA) avant la mise en œuvre de tout traitement de données susceptibles de présenter un risque élevé
  - principes et droits fondamentaux non négociables
  - La gestion des risques sur la vie privée

DANS QUEL CAS DECLENCHER UNE ANALYSE D'IMPACT DES RISQUES SUR LA VIE PRIVEE DES PERSONNES CONCERNEES ?

Les traitements qui remplissent au moins 2 des critères suivants doivent faire l'objet d'une analyse d'impact (PIA) :

- **collecte de données sensibles,**
- **collecte de données personnelles à large échelle,**
- **croisement de données,**
- **personnes vulnérables (patients, personnes âgées, enfants, etc.),**
- évaluation / scoring (y compris le profilage),
- décision automatique avec effet légal ou similaire,
- surveillance systématique,
- usage innovant (utilisation d'une nouvelle technologie),
- exclusion du bénéfice d'un droit/contrat.

NOUVELLE OBLIGATION : Traitement des violations de données à caractère personnel

RESSOURCES ET MOYENS DES SERVICES

Principe d'obligation d'information de la CNIL et des personnes concernées en cas de failles de sécurité sur des données personnelles (art. 33)

- Dans tous les cas, traiter l'incident de sécurité
- Informer la CNIL dans un délai maximum de 72 heures
- Informer les personnes concernées

ACTIONS	ACTEURS	CAS 1 : La violation n'engendre pas de risques sur les personnes	CAS 2 : La violation engendre un risque sur les personnes	CAS 3 : La violation engendre un risque élevé sur les personnes
Mise à jour du registre interne	DPO	X	X	X
Notification à la CNIL (dans les 72 heures)	DIRECTION METIER + DPO		X	X
Communication aux personnes concernées	a – Agents (interne) : DGP b - Usagers : DIRECTION METIER + DIR. COMM. c - Usagers Partenaires : DIRECTION METIER + Partenaire			X

seine-saint-denis
LE DÉPARTEMENT

RESSOURCES
ET MOYENS
DES SERVICES

1 politique de la donnée à caractère personnel
4 chantiers pour la protection des données

- ✓ Note plan d'action mise en conformité
- ✓ Note gestion des violations de données
- ✓ Modification de la fiche de déclaration interne
- ✓ Mentions Droits des personnes
- ✓ Site collaboratif RGPD

- ✓ Méthode CNIL : inventaire des traitements
- ✓ Réunion spécifique
- ✓ Demande d'avis au DPO
- ✓ Méthode urbanisation : modélisation des processus (priorité SI Solidarité - IODAS)

- ✓ PIA SI SPAS – SSD- PMI
- ✓ Politique mot de passe boite de structure
- ✓ Plan de sécurisation SI
- ✓ Analyse de risque du RSSI
- ✓ Indice Maturité RGPD des directions

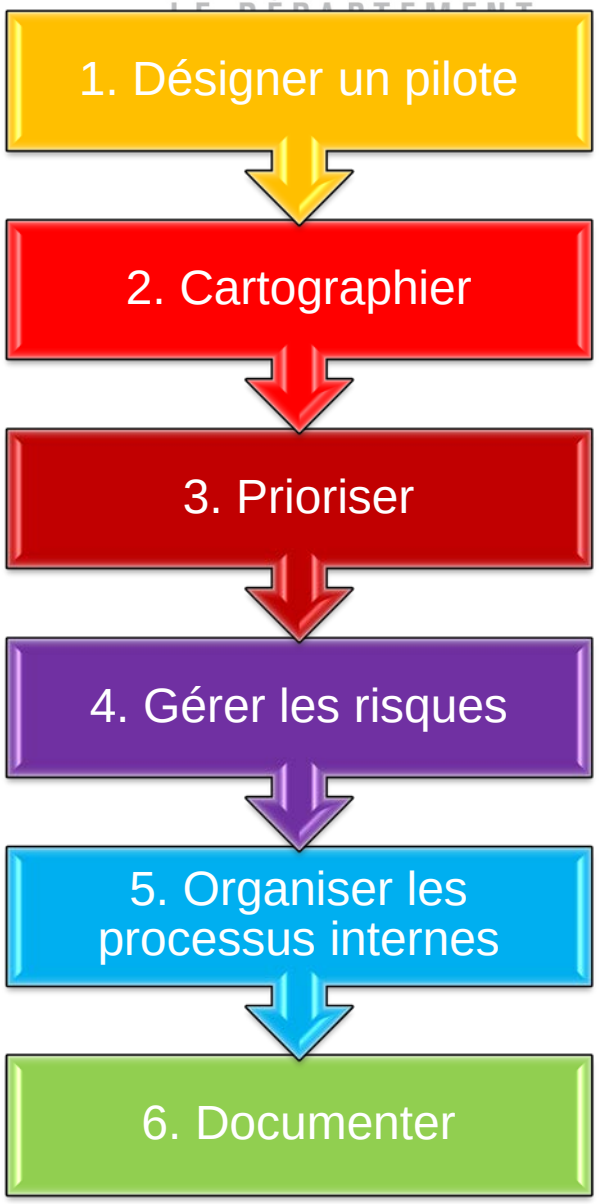
- ✓ Courriers des éditeurs
- ✓ Projet SI SPAS-SSD-PMI (PIA en cours)
- ✓ Projet à risques : NCS (à venir)
- ✓ Conventions

Points MAJEURS à travailler dans les directions :

- Inventaire / cartographie des traitements (opportunité des nouveaux projets, anciens traitement à planifier)
- Information des droits des usagers : Mentions légales / affichage (vigilance sites internet)
- Organisation de la gestion de l'exercice des droits (agents / usagers)
- Sensibilisation des agents en commençant par la hiérarchie
- Formalisation des processus internes / production de documentations « auditables »
- Protection des données dès la conception des projets : Analyse de risques à mener et à formaliser (métiers + dpo + dinsi) pour les traitements à « Risques »

RGPD : Mise en œuvre dans les métiers

seine-saint-denis
LE DÉPARTEMENT



Politique départementale de la donnée	Au sein de la direction métier
Informer , conseiller , contrôler en interne	
Recenser de façon précise les traitements de données personnelles **Tenir une documentation interne** décrivant les traitements mis en œuvre et les mesures de mise en conformité y afférentes ;	
Identifier les actions à mener pour se conformer aux obligations Prioriser les actions au regard des risques	
Réaliser une analyse de l'impact du traitement de données portant tant sur les **risques** de sécurité et techniques que sur les risques juridiques pour les personnes **Signaler à la Cnil les incidents de sécurité** impliquant les données personnelles	
Mettre en place des procédures permettant de garantir **la sécurité et la confidentialité des données,** dans le respect de la politique sécurité des systèmes d'information	
Réexaminer, constituer et regrouper les documentations ; **Porter une attention particulière à l'encadrement contractuel des prestations des tiers fournisseurs de services** dont la prestation implique le traitement des données	

Votre direction

1. Désigner un pilote

2. Cartographier

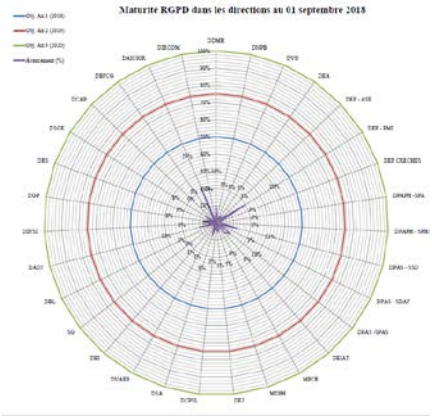
Un Relais RGPD sensibilisé : **Assurer le respect des droits des personnes**

Etat des lieux des traitements identifiés dans votre direction :**Tenir à jour une documentation interne** décrivant les traitements mis en œuvre et les mesures de mise en conformité y afférentes ;

BASE DE CALCUL Indice de Maturité RGPD d'une direction

seine-saint-denis
LE DÉPARTEMENT

RESSOURCES
ET MOYENS
DES SERVICES



UNE APPROCHE EN PARALLELE

URBANISATION :

1. Analyse Métiers : détermination des grands domaines de traitements, critères d'importance (nombre d'acteurs, nombre d'activités, complexité,…)

2. Quels sont les traitements les plus importants par rapport au métier ? Établir la priorité des actions (planification prévisionnelle)

3. Modélisation des processus (urbanisation) : Livrables attendus processus et données associés
4. Consolidation avec la mise en conformité RGPD

Mise en conformité RGPD :

1. Mise à jour des déclarations des traitements existantes
2. Déclaration des traitements manquants

3. Détermination des priorités d'actions, planification

4. Consolidation réglementaire avec les études d'analyse d'impact nécessaires

5. Consolidation avec la modélisation des processus

MISE EN COHERENCE DES LIVRABLES

Ateliers pour aller plus loin :

1. Comment remplir un formulaire déclaration de traitement
2. Les bases pour réaliser un PIA
3. Sensibilisation à la sécurité informatique
4. Sécurité thématique (utilisateurs) : panorama de la sécurité, mot de passe, appareil mobiles, usages pro-perso, hameçonnage, fraudes, …
5. Sécurité thématique (développeurs) : sécurité site Web, développement Web,
6. SAAS / cloud : recommandations à prendre en compte
7. Marchés publics et RGPD
8. Modélisation de processus (BPMN)

INSCRIPTIONS :