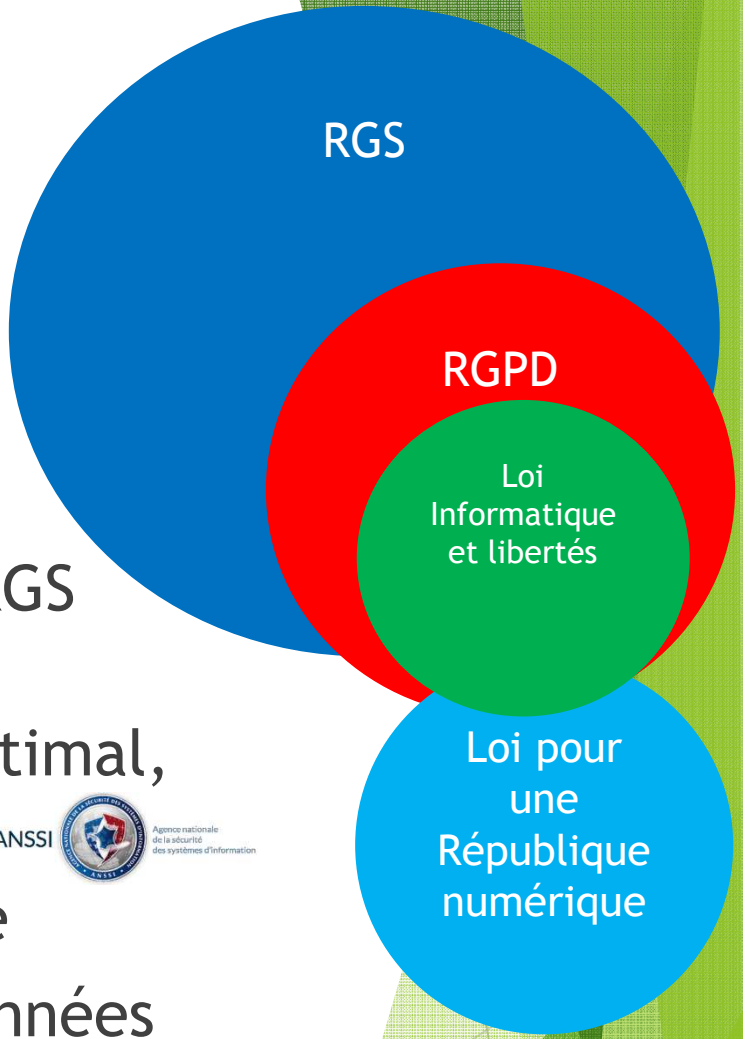
Règlement européen de protection des données
RGPD

Règlement (UE) 2016/679
du Parlement européen et du Conseil du 27 avril 2016

Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,

Conseil Municipal du 11 octobre 2018
Mogneneins

4 textes de loi sur les données personnelles



- Référentiel Général de Sécurité > RGS

Améliorer la sécurité informatique et prenant toute mesure et à un coût optimal, préventive et continue

ANSSI Agence nationale de la sécurité des systèmes d'information

- Loi pour une République Numérique

Nouveaux droits du citoyen sur les données personnelles et opendata

- Loi Informatique et Libertés > CNIL
- **Règlement Général Protection Données** > RGPD

Loi pour une République Numérique

1 - Favoriser la circulation des données et du savoir

- **Ouverture des données publiques par défaut, par principe**

- Toute personne morale de droit public de droit privé chargée d'une mission de service public de **+ 50 agents - Collectivités +3500 habitants**

2 - Œuvrer pour la protection des individus dans la société du numérique

- **Bases de données produites ou reçues par la collectivité mises à jour de façon régulière d'intérêt économique, social, sanitaire, environnemental**

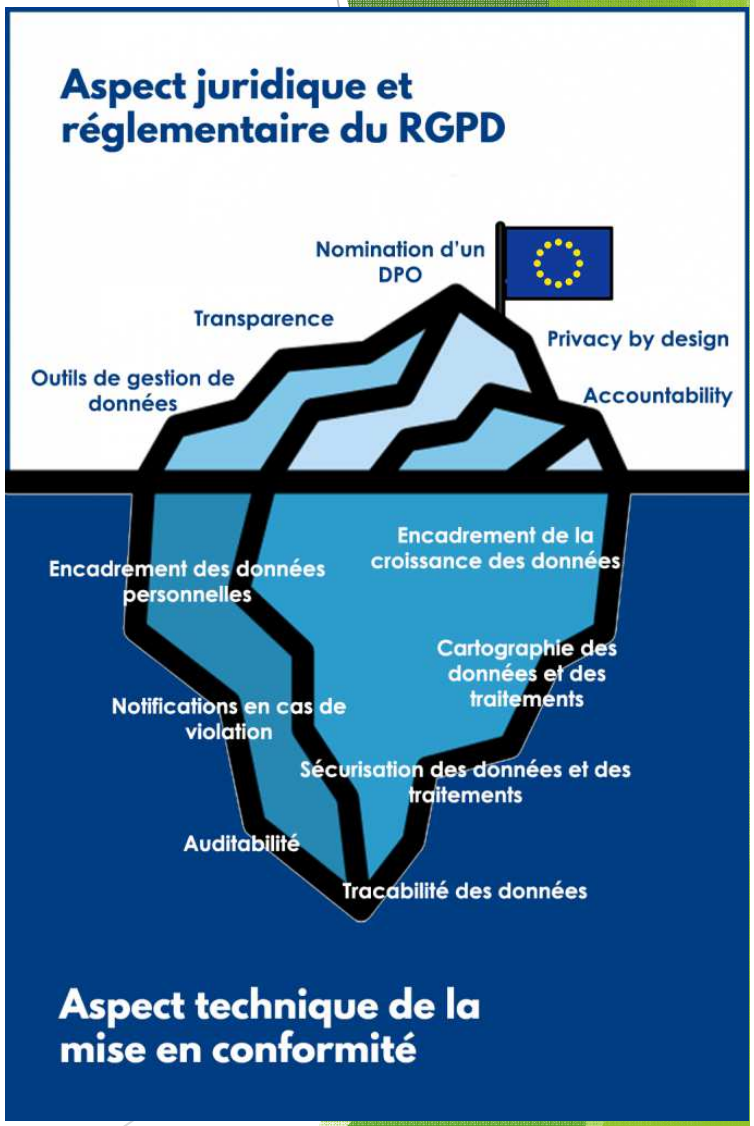
- Données diffusées obligatoirement dans un standard ouvert et aisément réutilisables

3 - Garantir l'accès au numérique pour tous

>>> Oct.2018 !

Règlement européen Général sur la Protection des Données

- **Qui** : tout organisme public ou privé, et ses sous-traitants, qu'il soit (UE ou hors UE), effectuant un ou des traitements de données à caractère personnel dans le cadre d'activités opérées sur le territoire de l'Union européenne ou relatives à des personnes se trouvant sur ce territoire.
- **Quand** : Adopté le 27 avril 2016 par les eurodéputés, publié le 04 mai 2016 au Journal Officiel de l'Union Européenne et entre en vigueur le 25 mai 2018.
- **Quoi** : Le RGPD établit les règles relatives à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et des règles relatives à la libre circulation de ces données.



Règlement européen Général sur la Protection des Données

- **le** RGPD a vocation à offrir le **même niveau de protection des données à caractère personnelle sur tout le territoire européen**
- **Un contrôle renforcé du citoyen sur ses données personnelles** : accès de l'usager/utilisateur clair, accessible et compréhensible, recueil obligatoire d'un consentement clair et explicite avant toute réutilisation des données, extension des droits des personnes au droit à l'oubli, à la portabilité des données, à l'informations s/ piratage de ses données, protection accrue des mineurs,
- **Une harmonisation des législations nationales** via ce règlement européen applicable à toutes les entreprises opérant au sein de l'UE (y compris si elles n'y sont pas établies),
- **Une unification des autorités de régulation avec la création du Comité européen de protection des données** (réunit les CNIL européennes), **nouveaux pouvoirs de décision et de sanction** pour les CNIL européennes, pouvoir de sanction accru //entreprises (jusqu'à 4% du chiffre d'affaires mondial
- **Une protection accrue des données des victimes/témoins/suspects** dans le cadre de la coordination police-justice européenne.

Règlement européen Général sur la Protection des Données

Des notions fondamentales de la protection des données personnelles :

- **Donnée à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement.**
(identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale (RGPD – Article 4). NB : le RGPD ne couvre pas les traitements de données effectués par des personnes physiques dans le cadre d'activités exclusivement personnelles/domestiques)

- **Traitement de données :** toute **opération** ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que 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 (RGPD – Article 4)

- **Responsable de traitement** : personne physique ou morale, autorité publique, service ou autre organisme qui, seul ou conjointement avec d'autres, **détermine les finalités et les moyens** du traitement; (RGPD – Article 4)

- **Finalité du traitement** : indique à quoi va servir le traitement de données; elle doit être **pertinente** (limitée au stricte nécessaire), **déterminée** (définie en amont de la collecte et utilisation des données), **légitime** (adéquate et justifiée/missions de l'organisme) et **explicite**, puis **respectée dans le temps** de manière stricte dans l'utilisation des fichiers de données (Définition CNIL)

- **Durée de conservation :** Les données personnelles ont une date de péremption. La durée de conservation des données, fixée par le responsable du traitement, est la durée **nécessaire aux finalités** de collecte et de traitement des données (Loi Informatique & Libertés - article 6). La CNIL peut établir des normes en matière de durée de conservation (Loi Informatique & Libertés - article 24).

Règlement européen Général sur la Protection des Données

- **Des conditions plus strictes de recueil du consentement** : Obtention d'un consentement **actif, libre, spécifique, éclairé et univoque** (Art. 4 RGPD)
- **Révocabilité du consentement** : droit au retrait du consentement à tout moment et de manière simple (Art.7 RGPD) et information de l'usager/utilisateur sur son droit au retrait
- Exigence d'un consentement parental pour les mineurs < 16 ans.
- **Une réaffirmation des principes fondamentaux de la protection** : licéité, loyauté et **minimisation** de la collecte de données, finalités initiales **et ultérieures** déterminées, explicites et légitimes, exactitude, intégrité et confidentialité, limitation et respect effectif de la durée de conservation.
- **Une transparence renforcée vis-à-vis des personnes -** (Art. 4 RGPD) Extension du devoir d'information des personnes les finalités et la base juridique du traitement, les destinataires, la durée de conservation, portabilité, droit à réclamation auprès d'une autorité de contrôle etc. l'existence d'une contrainte légale, réglementaire ou contractuelle imposant la fourniture des données, l'existence d'une prise de décision automatisée.
- **Des notifications en cas de fuite de données (Art.33 RGPD) :** les responsables de traitement seront tenus de notifier dès que possible toute violation* grave de données à l'autorité nationale de protection, c'est-à-dire la CNIL, et aux usagers concernés dans certains cas.
- **Des sanctions plus importantes :** le règlement donne aux autorités nationales de contrôle le pouvoir d'infliger des sanctions financières lourdes

Règlement européen Général sur la Protection des Données

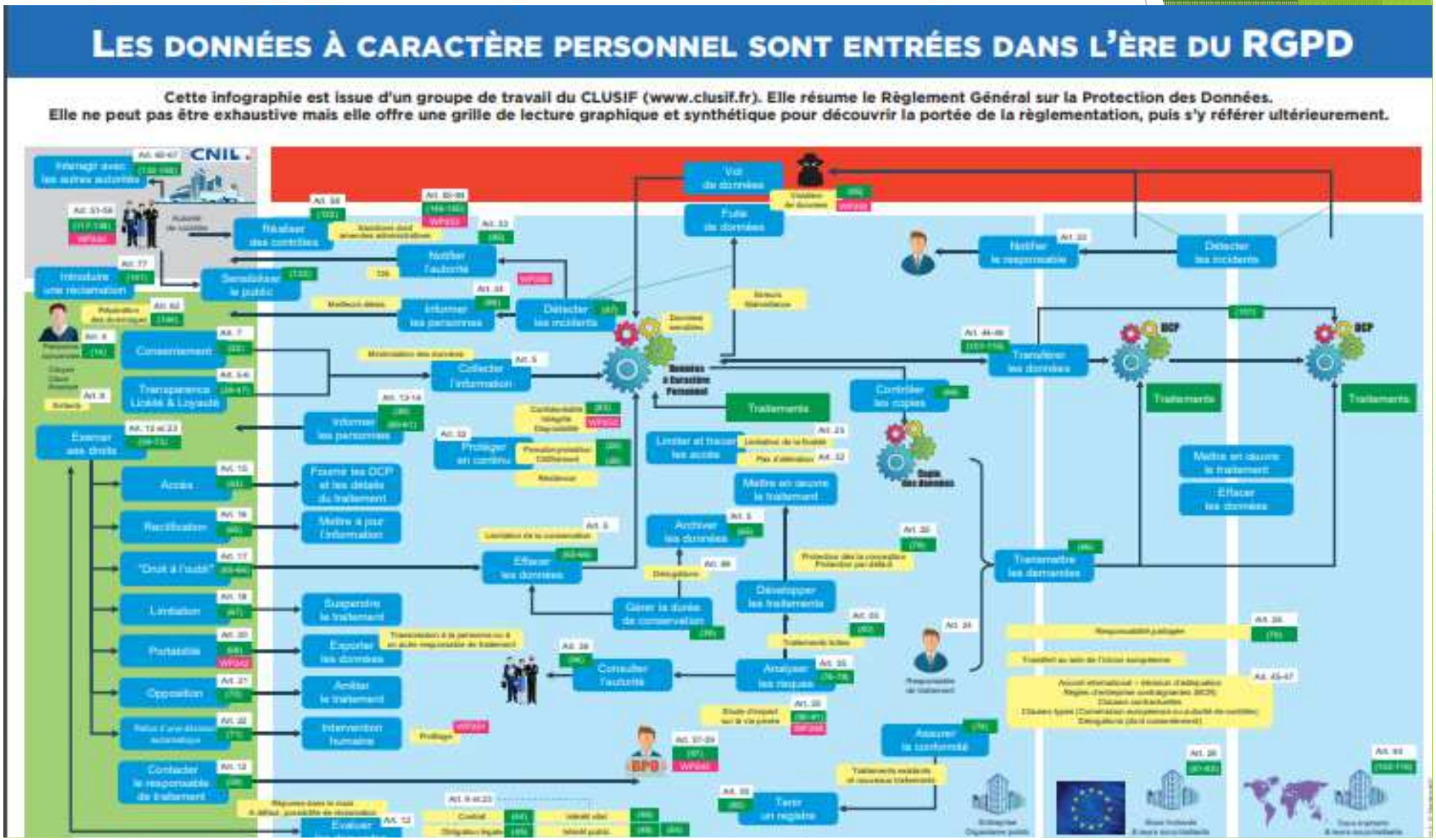
De nouveaux droits pour les personnes concernées :

- **Le droit à la portabilité des données** : droit de demander la restitution ou le transfert de ses données à un autre prestataire sous format lisible par une machine, sous réserve que ces données aient été fournies par la personne elle-même, aient fait l'objet d'un traitement automatisé et aient été traitées sur la base du consentement ou de l'exécution d'un contrat.

- **Le droit à l'effacement des données :** droit de demander l'effacement des données sous certaines conditions (retrait de consentement, traitement illicite, etc.) et hors des traitements nécessaires à l'exécution d'une mission de SP ou relevant de l'exercice de l'autorité publique.

- **Un droit d'information accru sur les décisions automatisées.**

Plan d'action RGPD
Commune de Mogneneins



RGPD

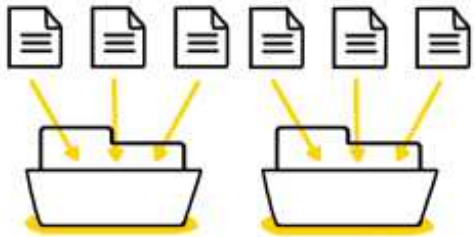
PASSEZ À L'ACTION

en 4 étapes

1

Constituez un registre de vos traitements de données

2



Faites le tri dans vos données

3

Respectez les droits des personnes

4

Sécurisez vos données

Plan d'action RGPD
Commune de Mogneneins 1/2

- Réalisation d'un inventaire des traitements de données à caractère personnel par la commune de Mogneneins et identification des points de non-conformité à corriger
- Recueil du consentement de l'usager, garantir la traçabilité de l'obtention de ce consentement, informer l'usager de son droit au retrait du consentement, sauf obligation légale ou réglementaire de la commune ne permettant pas de proposer à l'usager la révocabilité de son consentement
- Communication sur le RGPD (site, magazine…)
- Adaptation aux nouvelles exigences d'information des notices d'information, mentions légales des sites internet et formulaires de contact
- Intégration du principe de co-responsabilité du Responsable de traitement et des sous-traitants dans le dispositif de la commande publique : refonte des clauses des cahiers des charges (marchés publics) pour prise en compte des nouvelles modalités de mise en conformité (registre des traitements, étude d'impact sur la vie privée lors de nouveaux outils informatique par exemple)

Plan d'action RGPD
Commune de Mogneneins 2/2

- Définition et mise en place des processus internes et outils de bonne gestion des données personnelles et des modalités de saisine par les agents en interne et par les citoyens

- **Désignation du DPO Data Protection Officer (DPO),** un délégué à la protection des données (Art 37. RGPD : obligatoire)
  > Délibération 2018.07.03 – Mogneneins – RGPD : nomination d'un délégué de la protection des données

  > Ses principales missions sont de contrôler le respect du règlement, de conseiller le responsable des traitements sur son application et de constituer le point de contact avec l'autorité de contrôle, de répondre aux sollicitations de personnes qui souhaitent exercer leurs droits.

Mogneneins

Sources du document au 6/11/2018 :
- CNIL – http://www.cnil.fr
- Le CLUSIF https://clusif.fr/workgroup/synergie-partenariat-entre-rssi-dpo/
- Amabis : https://www.amabis.com/rgpd-gdpr-mise-en-conformite-solution/

Auteur : Nathalie Vernus-Prost – Mogneneins – novembre 2018