TERRITOIRES CONSEILS

Collection
Réunions téléphoniques

RGPD et collectivités et EPCI : comment accélérer sa mise en conformité ?

GROUPE Caisse des Dépôts

TERRITOIRES CONSEILS

Sommaire

RGPD : de quoi s'agit-il ?

RGPD = Règlement général sur la protection des données à caractère personnel

Avant le 25 mai 2018 :

- ➔ La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée en 2004 (Directive 95/46/CE du 24/10/1995) ;
- ➔ Les décisions de la Commission Nationale de l'Informatique et des Libertés (CNIL).

A compter du 25 mai 2018 :

- ➔ Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, 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, et abrogeant la directive 95/46/CE – ou Règlement Général sur la Protection des Données ;
- ➔ La loi Informatique et Libertés modifiée : loi n° 2018-493 du 20 juin 2018 ;
- ➔ Le règlement « eprivacy » : RGPD des communications électroniques, en cours d'élaboration (2018 ou 2019).

RGPD : de quoi s'agit-il ?

Gros apports du RGPD :

- Fin des formalités auprès de la CNIL (déclarations/demandes d'autorisation), mais, contrepartie : obligation de documenter sa conformité ;

- Nomination obligatoire d'un délégué à la protection des données dans le secteur public notamment ;

- Régime fort de sanctions administratives : la CNIL peut prononcer des amendes jusqu'à 20 millions d'euros ou 4% du CA mondial consolidé ;

- Prise en compte de la dimension internationale : procédure particulière en cas de transferts de données ;

- Consécration de nouveaux concepts : portabilité, limitation des données, etc. ;

- Généralisation de l'obligation de notifier les failles de sécurité.

RGPD : de quoi s'agit-il ?

Philosophie de la réglementation :

- Plus de souplesse : on peut tout faire en adaptant la réglementation à son cas – « autorégulation » // Fin des formalités déclaratives auprès de la CNIL ;
- Mais obligation de documenter sa conformité : « accountability » – mesures techniques et organisationnelles à mettre en œuvre et être en capacité de les prouver.

  - Concrètement, gros « classeur » des process à jour, en fonction de ses propres risques, contraintes, spécificités internes…;
  - Actions concrètes à mettre en œuvre.

  → Démarche de conformité ;
  → Principe de responsabilité.

Objectif : protéger les personnes physiques (agents, administrés…) par l'encadrement de l'utilisation de leurs données à caractère personnel.

RGPD : de quoi s'agit-il ?

Principes clefs du RGPD :

- La licéité, la loyauté et la transparence des traitements de données à caractère personnel ;
- La limitation des finalités de ces traitements ;
- La minimisation et l'exactitude des données à caractère personnel ;
- La limitation de la conservation ainsi que l'intégrité et la confidentialité de ces données.

Traitement présumé licite dans deux cas :

- Consentement de la personne ;
- Obligation légale de collecter.

Article 5 et 6 RGPD

RGPD : de quoi s'agit-il ?

A qui s'applique la réglementation ?

- Responsable du traitement : celui qui est à son initiative ;
- Sous-traitant : celui qui utilise et/ou alimente le traitement.

ET

- Etabli en France ou sur le territoire de l'UE ou ;
- En cas de collecte en France ou sur le territoire de l'UE, même via un site internet.

Guide du sous-traitant disponible sur le site de la CNIL.

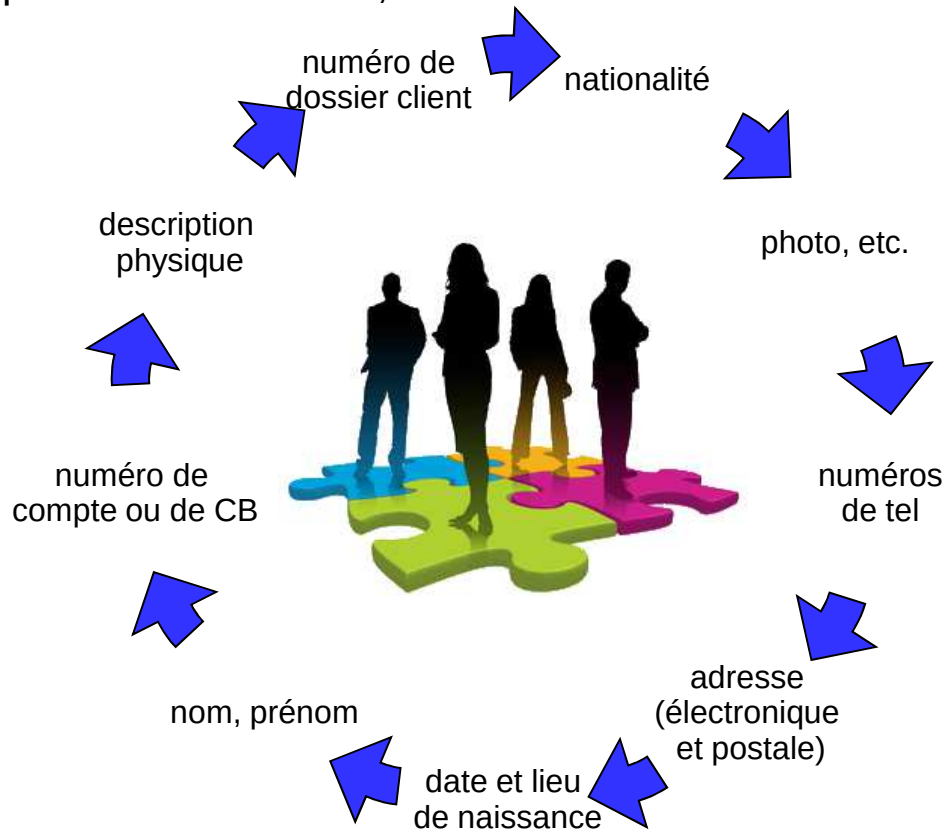
RGPD : de quoi s'agit-il ?

Qu'est-ce qu'une donnée à caractère personnel ?

➔ information qui permet d'identifier ou de reconnaître, directement ou indirectement, une personne, un individu : agent, administré, fournisseur/prestataire personne physique.

Exceptions :

- Données concernant des personnes morales ;
- Données anonymisées



RGPD : de quoi s'agit-il ?

Zoom sur les données interdites :

Sont, en principe, interdites de collecte sauf si la règlementation l'autorise ou oblige à collecter :

- les données relatives à des infractions, condamnations ou mesures de sûreté (sauf pour le service contentieux) ;
- les données sensibles : santé, vie sexuelle, origines raciales ou ethniques, opinions philosophiques, religieuses, politiques ;
- le numéro de sécurité sociale, en raison de risques de fraude (sauf paie).

Distinction :
-données « classiques » : celles qui ne présentent pas de caractère particulièrement sensible, notamment compte tenu de leur nature ;
-et données « sensibles » : celles qui ne peuvent être recueillies qu'avec le consentement explicite de la personne concernée.

RGPD : de quoi s'agit-il ?

A qui s'applique la réglementation ?

- Responsable du traitement : celui qui est à son initiative ;
- Co-responsable du traitement ;
- Sous-traitant : celui qui utilise et/ou alimente le traitement.

ET

- Etabli en France ou sur le territoire de l'UE ou ;
- En cas de collecte en France ou sur le territoire de l'UE, même via un site internet.

Guide du sous-traitant disponible sur le site de la CNIL.

RGPD : de quoi s'agit-il ?

Quels traitements de données sont concernés ?

- **toute opération ou ensemble d'opérations portant sur des données à caractère personnel, quelque soit le procédé utilisé** : collecte, enregistrement, organisation, structuration, conservation, adaptation ou modification, extraction consultation, utilisation, communication par transmission, diffusion, etc. ;

- traitements automatisés et non automatisés (y compris les traitements papier) ;

- exemples :
  - dossiers d'inscription école ;
  - logiciel gestion de la paye des agents ;
  - fichier Excel relatif aux impayés ;
  - etc.

Article 4 RGPD

TERRITOIRES CONSEILS

Sommaire

1. Nommer un délégué à la protection des données : art. 37

- Sa désignation est obligatoire dans le secteur public.

- Le DPO ne peut pas être le responsable de traitements, mais ce peut être un salarié.

- Il peut être :
  -mutualisé au sein d'un groupe ;
  -interne ou externe.

- Il est le successeur naturel du CIL. Il doit être déclaré auprès de la CNIL et son identité et ses coordonnées doivent être communiquées au grand public. Modèle de formulaire de désignation sur le site de la CNIL

- Il veille au respect de la bonne application du RGPD et il est le contact principal des autorités compétentes en cas de contrôle.

2. Créer un registre des traitements : art. 30

- Faire l'inventaire des traitements de données internes et externalisés ;

- Réaliser une cartographie des traitements de données ;

- Rédiger le registre des traitements :
  - Modèle sur le site de la CNIL ;
  - Par exemple, tableur Excel avec un onglet par traitement de données.

- Contenu du registre : s'aider des délibérations de la CNIL (normes simplifiées, autorisations uniques, etc.).

Conseil : reprendre les anciennes déclarations CNIL mais attention, ou le registre tenu par le CIL, le cas échéant.

Attention : si traitement de données « sensibles » ou d'infractions, penser à faire obligatoirement une étude d'impact – article 35 RGPD : possibilité de télécharger un logiciel pour réaliser des PIA sur le site de la CNIL.

3. Rédiger les mentions obligatoires : art. 13 et 14

- Les personnes doivent être informées en cas de collecte directe et indirecte de leurs données ;

- Faire un audit des formulaires de collecte de données, du site internet, des contrats en cours et les modifier en conséquence ;

- Prévoir d'informer les administrés et les agents avec les nouvelles mentions obligatoires, par l'envoi d'un mail dédié par exemple ;

- Prévoir des clauses-type sur le sujet, à insérer dans les modèles de contrats notamment ;

- Eventuellement, prévoir un process pour intégrer les mentions d'information à tout projet incluant un traitement de données.

Conseil : aidez-vous des exemples sur le site de la CNIL en attendant un nouveau simulateur de mentions d'information.

A noter que la CNIL permet une information en plusieurs niveaux et via différents canaux.

4. Créer les procédures d'exercice des droits : art. 15 et s.

Principe : toute demande d'exercice d'un droit prévu par le RGPD doit faire l'objet d'un accueil favorable.

Exceptions : dans certains cas, le RT pourra refuser l'exercice de certains droits, notamment en cas de contentieux par exemple. Une décision motivée devra être transmise par écrit à la personne concernée.

➢ Process à mettre en place pour faciliter les démarches des personnes.

- **Droit d'accès** : *art. 15* : obtenir et vérifier les données qu'un organisme détient sur vous;
- **Droit d'opposition** : *art. 21* : s'opposer, pour des motifs légitimes, à figurer dans un fichier (diffusion, transmission, conservation) ;
- **Droit à la limitation du traitement** : *art. 18* : geler l'utilisation de vos données ;
- **Droit à la portabilité** : *art. 20* : emporter une copie de vos données pour les réutiliser ailleurs ;
- **Droit de modification / rectification** : *art. 16* : rectifier les informations inexactes vous concernant ;
- **Droit de suppression/effacement** // droit à l'oubli : *art. 17* : effacer des données vous concernant.

5. Veiller aux contrats passés avec des tiers : art. 28 et 29

Méthode :

- Revoir les contrats de sous-traitance en cours : négocier l'insertion d'une clause permettant d'engager la responsabilité du prestataire.

- Veiller à l'insertion d'une clause-type dans tous les nouveaux contrats avec des prestataires : mettre en place un process pour que, dans chaque nouveau contrat, un telle clause soit prévue // « privacy by design ».

➔ Veiller à engager la responsabilité du prestataire au moyen d'une clause-type délimitant le rôle de chacun et permettant d'engager la responsabilité du ST.

Exemple de clauses sur le site de la CNIL

Responsabilité du responsable de traitement, du sous-traitant.
Principe de coresponsabilité.

6. Intégrer la sécurité : art. 32

La sécurité doit être **adaptée à la taille et au contexte de l'entreprise**. Elle est une garantie de la non-altération des données de manière involontaire et de leur confidentialité.

Quelques fondamentaux :
- Gestion des accès ;
- Protection du réseau informatique ;
- Procédure de gestion des tiers (engagement de confidentialité) ;
- Mise en place d'une politique d'archivage et de suppression définitive (paye : 5 ans par exemple) ;
- Procédure de gestion des violations de DCP // **obligation de notifier les failles de sécurité à la CNIL** (dans les 72 heures) et, éventuellement, aux personnes concernées (art. 33) – registre des violations de données ;
- Procédure de communication de DCP : transferts vers tiers…

Outils :
-Politique de sécurité ;
-Charte informatique ;
-Formulaire de notification des violations des DCP (sur le site de la CNIL) ;
-Etc.

7. Sensibiliser le personnel

Sensibiliser le personnel de votre collectivité en continu, surtout les personnes qui collectent de la DCP.

- Zone dédiée sur l'intranet avec ressources d'informations (créations, publications CNIL, etc.) ;

- Communication régulière sur les grands principes de la réglementation (proportionnalité, minimisation, etc.) ;

- Éventuellement, formation du personnel qui collecte de la DCP ou qui l'utilise – registre des formations ; attention aux zones de commentaires libres ;

- Réalisation d'audits – entretiens avec les agents concernés…

Conseil : annexer au règlement intérieur une clause sur la confidentialité à destination des salariés.


Mes bonnes pratiques
Ne pas communiquer mon identifiant et mon mot de passe
Ranger mes dossiers quotidiennement dans des armoires fermées
Respecter la charte Informatique et le Règlement Intérieur
Suivre et appliquer les documents explicatifs sur les process
Respecter la confidentialité des données de chacun à l'écrit comme à l'oral
Archiver/purger régulièrement mes dossiers
Ne pas prêter/ donner ma carte d'accès aux locaux
Protéger mon téléphone par un verrouillage
Verrouiller mon poste de travail dès que je m'absente
Ne pas prêter/ donner mon téléphone ou mon ordinateur portable

TERRITOIRES CONSEILS

Sommaire

Les sanctions encourues

Trois types de sanctions :

-Administratives : sanctions prononcées par la CNIL, **jusqu'à 20 millions d'euros** ;

-Pénales : de nombreux délits repris aux art. 226-16 à 226-24 du Code pénal, **jusqu'à 300 000 euros d'amende et 5 ans d'emprisonnement** + de nombreuses contraventions dans la partie réglementaire du Code pénal ;

-Atteinte à l'image de la collectivité : **sanctions publiques** prononcées par la CNIL, reprise par les médias.

En cas de contrôle de la CNIl, coopérez.

TERRITOIRES CONSEILS

Sommaire

Mémo

Avant la mise en œuvre d'un traitement, toujours se poser les questions suivantes :

1) Le RGPD est-il applicable au traitement ?
2) Ma conformité est-elle documentée ?
3) Suis-je certain de respecter les principes de collecte loyale et proportionnée ?
4) Une durée de conservation et des modalités d'archivage ont-elles été définies ?
5) Une politique de sécurité et de confidentialité des données est-elle définie ?
6) Y a t-il des données interdites (sensibles, infractions/condamnations pénales, n° de sécu) ?
7) Y a t-il des transferts de données en dehors de l'Union européenne ?
8) Des procédures ont-elles été définies afin de respecter les droits des personnes fichées ?
9) Des études d'impact doivent-elles être rédigées ? Faut-il consulter la CNIL ?

Service de renseignements téléphoniques

Certaines questions posées par les participants renvoient à des situations très particulières, qui nécessitent une réflexion plus approfondie qui dépasse le cadre de ces réunions. Afin d'obtenir la meilleure réponse possible, contactez le service de renseignements téléphoniques de Territoires Conseils :

- par téléphone au 0970 808 809 □
- par mail sur le site Internet www.caissedesdepotsdesterritoires.fr en cliquant sur APPUI JURIDIQUE ou TÉLÉPHONE. Vous y trouverez également une rubrique «Questions-réponses ».

Dans le cadre des missions d'intérêt général de la Caisse des Dépôts, ce service est accessible gratuitement à toutes les intercommunalités, quels que soient leur taille et leur type, ainsi qu'aux communes de moins de 10 000 habitants.