Service public fédéral Intérieur
Direction générale Institutions et Population
*Registre national*
*Relations extérieures*

3153668

Aux utilisateurs du Registre national

**Votre correspondant**
Sophie Boulanger
Vincent Vandenkerckhoven

T
02 518 20 61
02 518 22 74

**E-mail**
sophie.boulanger@rrn.fgov.be
Vincent.Vandenkerckhoven@rrn.fgov.be

F
02 518 29 61

**Votre référence**

**Notre référence**

**Annexes**

**Bruxelles**
7 -08- 2017

**Mise en oeuvre du Règlement (UE) 2016/679 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**

**(RGPD ou Règlement Général sur la Protection des Données)**

Mesdames,

Messieurs,

A plusieurs reprises j'ai attiré l'attention sur les obligations imposées en application des lois des 8 août 1983 organisant un registre national des personnes physiques et 8 décembre 1992 relative à la protection de la vie privée (transposant la Directive 95/46 UE) incombant aux responsables de traitement au sein des autorités et organismes légalement habilités à accéder au RN ainsi qu'aux mesures en vue de garantir la sécurité des données.

Il me parait nécessaire, au regard de la prochaine entrée en vigueur le 25 mai 2018 du Règlement européen 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 (RGPD), d'attirer l'attention des autorités et organismes susmentionnés sur la nécessité de prendre la mesure des obligations imposées par le RGPD[1].

Le RGPD s'axe sur une logique globale de **responsabilisation de l'ensemble des acteurs**. On assiste à un allègement considérable des obligations en matière de formalités préalables, puisque le régime déclaratif (dont étaient néanmoins exemptés les registres de population) est totalement supprimé, pour entrer dans un système de « Gestion » des données personnelles. On passe en effet d'une logique de contrôle a priori à une logique de responsabilisation en continu des responsables de traitement. Cela signifie que la **conformité au RGPD devra être permanente et dynamique.** Il conviendra d'adopter et d'actualiser des mesures techniques et

[1] Les grands principes déjà présents dans la loi sur la protection de la vie privée ne changent pas mais le RGPD **renforce les obligations en matière de transparence des traitements** et de **respect des droits des personnes** et conforte le rôle de l'autorité de contrôle (Commission pour la protection de la vie privée) en **renforçant considérablement son pouvoir de sanction**. Ainsi, outre des avertissements publics, elle pourra prononcer de lourdes amendes administratives. Il conviendra d'intégrer un nouveau principe de **protection des données dès la conception** (Privacy by design) du traitement et **par défaut** (Privacy by default). Il faudra ainsi tenir compte le plus en amont possible, dès la phase de conception du produit, du service ou du traitement, des paramétrages par défaut et des principes essentiels de la protection des données. Il s'agira en particulier de minimiser l'impact sur la vie privée du traitement effectué comme par exemple *restreindre au maximum les droits d'accès aux données et les opérations susceptibles d'être réalisées.*

organisationnelles permettant de s'assurer et de démontrer à tout instant qu'un niveau optimal de protection aux données traitées est réellement offert. Les responsables de traitement seront ainsi appelés à tenir un **registre de leurs activités de traitement.**

Les organismes publics et privés auxquels les communes **sous-traitent** la mise en œuvre de tout ou partie de leurs traitements (ex. : prestataires de service hébergeant des données) devront obligatoirement participer à la démarche de mise en conformité, en aidant celles-ci à satisfaire à leurs diverses obligations, sous peine de sanctions.

Cette note n'a pas pour objectif de procéder à une analyse exhaustive des actions à mener par les communes ou les firmes informatiques pour se conformer au RGPD. Le RGPD va au-delà du champ de compétence du département au sein des communes. Vous traitez en effet chaque jour de nombreuses données personnelles, que ce soit pour assurer la gestion administrative de votre structure (fichiers de ressources humaines), la sécurisation de vos locaux (contrôle d'accès par badge, vidéosurveillance) ou la gestion des différents services publics et activités dont vous avez la charge : gestion des registres de population, gestion de l'état civil, listes électorales, développement de téléservices, etc. Le département n'a pas à s'immiscer dans cette gestion. Cependant il me parait nécessaire d'aider nos partenaires à se préparer et anticiper les changements liés à l'entrée en application du RGPD.

Aussi, le département vous propose-t-il une méthodologie en 5 étapes pour ce faire :

- Étape 1 : La désignation d'un pilote : le Délégué à la protection des données (DPO)
- Étape 2 : L'élaboration d'un Registre des traitements (RT)
- Etape 3 : L'analyse critique du RT
- Etape 4 : La réévaluation des processus internes
- Etape 5 : La documentation de la conformité

La réalisation des étapes 3, 4 et 5 sont tributaires du timing qu'impose la future réforme de la loi sur la protection de la vie privée du 8 décembre 1992 par le SPF Justice ainsi qu'une mise à jour consécutive de nos propres règlementations : il convient dès lors d'attendre le nouveau cadre légal en matière de protection des données personnelles. Néanmoins il est nécessaire d'entamer dès à présent le travail de mise en conformité par la mise en route des 2 premières étapes.

Parc Atrium
Rue des Colonies 11
1000 Bruxelles

T 02 518 21 31
F 02 518 26 31

callcenter.rrn@rrn.fgov.be
www.ibz.rrn.fgov.be

## I. Etape 1 : La désignation d'un pilote : le DPO

A compter du 25 mai 2018, la désignation d'un délégué à la protection des données (*Data Privacy Officer*) sera obligatoire pour les organismes et autorités publiques, et donc pour les communes[2].

La question du cumul de fonction entre le conseiller en sécurité et le DPO se pose. La CPVP souligne dans sa **Recommandation 04/2017**[3] du 24 mai 2017 que *l'on ne peut conclure que dans tous les cas, le conseiller en sécurité en fonction à l'heure actuelle peut de façon automatique être le délégué à la protection des données de demain...() c'est désormais à l'aune de la fonction telle que décrite par le RGPD que cet aspect doit être examiné.*
*Le RGPD indique que le délégué est désigné sur la base de ses qualités professionnelles, et en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données et de sa capacité à accomplir les missions visées à l'article 39 lesquelles dépassent la seule mise en oeuvre d'une sécurité adéquate et les obligations relatives à l'obligation de sécurité.*

Le délégué aura **pour principales missions** :

- *Informer, former et conseiller* le responsable du traitement et les sous-traitants ainsi que le personnel ;
- *Contrôler* la conformité des traitements au RGPD et autres dispositions analogues;
- *Etre le point de contact* de l'autorité de contrôle sur les questions liées au traitement de données à caractère personnel.

Dans l'exercice de ces missions, le délégué devra être à l'abri des conflits d'intérêts, rendre compte directement au niveau le plus élevé de la hiérarchie et bénéficier d'une liberté certaine dans les actions qu'il décidera d'entreprendre.

**Expertise et moyens**

Il conviendra de s'assurer que le DPO dispose **d'un niveau d'expertise et de moyens suffisants pour exercer son rôle de façon efficace.** Ainsi, le délégué devra :

- être désigné sur la base de ses connaissances spécialisées du droit et des pratiques en matière de protection des données ;
- être associé en temps utile et de manière appropriée à l'ensemble des questions relevant de ses missions ;
- bénéficier des ressources et formations nécessaires pour mener à bien ses missions.

[2] En ce qui concerne les organismes privés je renvoie aux dispositions spécifiques du RGPD
[3] https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_04_2017.pdf

Dans ce contexte, pour les communes qui ont des préoccupations identiques, la désignation d'un seul DPO n'est pas exclue de même qu'un DPO externe.

Enfin, sans aller jusqu'au « partage » du DPO, ces mêmes communes peuvent opportunément travailler ensemble pour se préparer au mieux aux nouvelles obligations posées par le RGPD : identification des besoins des uns et des autres, définition d'un plan d'action comprenant différentes étapes, développement d'un outil commun d'information et de partage de connaissances, etc.

## II. Étape 2 : L'élaboration d'un Registre des traitements

Il s'agit d'une étape fondamentale : la réalisation de l'inventaire de la totalité des fichiers de données personnelles traitées au sein de votre organisation.

Il y a lieu de se référer tout d'abord à la **Recommandation 06/2017 du 14 juin 2017 de la CPVP**[4] concernant la tenue d'un registre des activités de traitements dont le rôle est d'identifier les manques et de décrire les actions à mener pour se conformer aux obligations actuelles et à venir au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées. Le Registre doit contenir certaines informations :

1. Etablir la liste des traitements par finalité principale (et non par outil ou applicatif utilisé) et les types de données traitées ;
2. Identifier les sous-traitants qui interviennent sur chaque traitement ;
3. Déterminer à qui et où les données sont transmises ;
4. Déterminer où sont stockées vos donnéhttps://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitementes et back up;
5. Déterminer combien de temps ces données sont conservées ;
6. Inventorier les mesures de sécurité.

Le format de ce registre importe peu si l'ensemble des informations demandées par le RGPD s'y retrouve. Toutefois, vous pouvez utilement vous inspirer du document de la Commission Vie privée via le lien suivant:

https://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement

[4] https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_06_2017_0.pdf

## III. Etape 3 : Analyse critique des traitements

L'analyse critique du Registre des traitements va vous permettre d'identifier vos manques et de décrire les actions à mener pour se conformer aux obligations actuelles et à venir au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées. Il conviendra de :

1. Vérifier que **seules les données strictement nécessaires** à la poursuite des objectifs sont collectées et traitées.
2. Vérifier **la base juridique** sur laquelle se fonde le traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale) (art 6).
3. Compléter les **mentions d'information** (art. 12, 13 et 14 du GDPR).
4. Vérifier que vos **sous-traitants** connaissent leurs nouvelles obligations et leurs responsabilités grâce à l'existence de clauses contractuelles rappelant leurs obligations en matière de sécurité, de confidentialité et de protection des données personnelles traitées.
5. Vérifier que les modalités d'exercice des **droits des personnes** concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...) sont effectives et les adapter le cas échéant.
6. Vérifier et adapter les **mesures de sécurité** mises en place.

NB : pour certains traitements à risque il sera peut-être nécessaire d'adopter des mesures particulières telles que :

- Une étude d'impact sur la protection des données (PIA),
- Une information renforcée,
- Un recueil du consentement,
- Une autorisation préalable,
- Des clauses contractuelles.

## IV. Etape 4 : Réévaluer les processus internes

Il conviendra de mettre en place des procédures internes qui garantissent la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire) pour **que les réflexes de protection des données personnelles soient acquis chez tous y compris en cas d'incident.**

Parc Atrium
Rue des Colonies 11 T 02 518 21 31 callcenter.rrn@rrn.fgov.be
1000 Bruxelles F 02 518 26 31 www.ibz.rrn.fgov.be

V. Etape 5 : Documenter la conformité

Votre documentation doit démontrer que vous respectez les obligations prévues par le RGPD. Les actions et documents réalisés à chaque étape doivent être **actualisés** régulièrement pour assurer une protection des données en continu. Le dossier à tenir à la disposition de l'Autorité de contrôle doit contenir :

- **Le registre des traitements** (pour les responsables de traitements) ou des catégories d'activités de traitements (pour les sous-traitants) ;
- **Les analyses d'impact sur la protection des données** (PIA) pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes ;
- **L'encadrement des transferts** de données hors de l'Union européenne (notamment, les clauses contractuelles types, les BCR et certifications) ;**Les mentions d'information** ;Les modèles de **recueil du consentement des personnes concernées** :Les procédures mises en place pour **l'exercice des droits** ;**Les contrats avec les sous-traitants** ;Les procédures internes **en cas de violations de données** ;

* * *

**L'application du RGPD est donc un processus global dépassant le seul Registre national et, à cet égard, pour tout renseignement complémentaire vous pouvez utilement consulter le site de la Commission sur la protection de la vie privée (https://www.privacycommission.be/fr/reglement-general-sur-la-protection-des-donnees-0) pour toutes vos questions en la matière.**

Nous espérons que ces informations vous seront utiles et de vous avoir convaincu de l'importance de la mise en œuvre du RGPD au sein de vos organisations que nous vous invitons à réaliser dans le respect des droits et obligations des différents acteurs.

Jacques WIRTZ
Directeur général

Parc Atrium
Rue des Colonies 11
1000 Bruxelles

T 02 518 21 31
F 02 518 26 31

callcenter.rrn@rrn.fgov.be
www.ibz.rrn.fgov.be