Cahier détachable - Mars 2018 - N°321 - **www.courrierdesmaires.fr**

LE COURRIER DES MAIRES **et des élus locaux**

Les nouvelles règles relatives à la protection des données personnelles

Principal actionnaire : Info Services Holding. **Société éditrice :** Groupe Moniteur SAS au capital de 333 900 euros. **Siège social :** Antony Parc 2 - 10, place du Général de Gaulle - La Croix de Berny - BP 20156 - 92186 Antony Cedex. **RCS :** Paris 403 080 823. **Numéro de commission paritaire :** 1008 T 83807. **ISSN :** 0769-3508. **Président-directeur de la publication :** Julien Elmaleh. **Impression :** Imprimerie de Champagne, ZI Les Franchises, 52200 Langres. **Dépôt légal :** à parution.

Les références

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) applicable à compter du 25 mai 2018

Directive (UE) 2016/680 du 27 avril 2016

relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales,

Loi n° 2016-1321 du 7 octobre 2016

pour une République numérique dite loi « Lemaire »

Loi n° 2015-991 du 7 août 2015

portant nouvelle organisation territoriale de la République, dite loi « Notre »

Loi n° 78-17 du 6 janvier 1978

relative à l'informatique, aux fichiers et aux libertés

Arrêté du 4 juillet 2013

autorisant la mise en œuvre par les collectivités territoriales, les EPCI, les syndicats mixtes, les établissements publics locaux qui leur sont rattachés ainsi que les groupements d'intérêt public et les sociétés publiques locales dont ils sont membres de traitements automatisés de données à caractère personnel ayant pour objet la mise à disposition des usagers d'un ou de plusieurs téléservices de l'administration électronique.

Code des relations entre le public et l'administration (CRPA),

art. L. 312-1-1, L. 311-5 et L. 311-6

Projet de loi relatif à la protection des données personnelles, n° 490,

déposé le 13 décembre 2017 au bureau de l'Assemblée nationale

Conseil d'Etat, avis du 7 décembre 2017

sur le projet de loi relatif à la protection des données personnelles, NOR : JUSC1732261L

Charte de déontologie du délégué à la protection des données personnelles,

réalisée par l'Association française des correspondants à la protection des données à caractère personnel (AFCDP)

Les sites à consulter

afcdp.net

cada.fr

Cnil.fr/fr/collectivites-territoriales

Lexique

Commission nationale de l'informatique et des libertés (Cnil)

Autorité administrative indépendante composée d'un collège pluraliste de 17 commissaires (4 parlementaires, 2 membres du Conseil économique, social et environnemental, 6 représentants des hautes juridictions, 5 personnalités qualifiées désignées par le président de l'Assemblée nationale (1), le président du Sénat (1), le conseil des ministres (3). Le mandat de ses membres est de cinq ans.

Correspondant « informatique et libertés » (CIL)

Le correspondant «informatique et libertés» (CIL) veille à la sécurité juridique et informatique de son organisme. Il bénéficie d'un service dédié de la Cnil pour l'accompagner dans l'exercice de ses missions.

DPO et DPD

« Data protection officer » ou Délégué à la protection des données.

Donnée personnelle

Toute information identifiant directement ou indirectement une personne physique, comme le nom, les numéros d'immatriculation et de téléphone, les photographies, la date de naissance, la commune de résidence, l'empreinte digitale, etc.

Responsable de traitement

Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

Traitement de données à caractère personnel

Toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé : collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, etc.

Protection des données personnelles : les nouvelles règles à respecter

Le 25 mai prochain, de nouvelles règles d'utilisation et de diffusion des données personnelles issues du règlement européen sur la protection des données (RGPD) entreront en vigueur, renforçant fortement les contraintes de l'open data et les éventuelles sanctions.
Si ce règlement européen laisse une certaine marge de manœuvre aux Etats – laquelle se concrétise, en France, par le dépôt, par le gouvernement, d'un projet de loi relatif à la protection des données personnelles –, les acteurs publics locaux devront faire face à des injonctions parfois difficiles à concilier.

Philosophie rénovée. D'ores et déjà, les collectivités locales doivent se préparer en intégrant les nouvelles règles en vigueur. La nouvelle philosophie du traitement de leurs données repose sur le principe de la responsabilisation et sur la désignation en leur sein d'un «data protection officer» (DPO). Déjà, les répercussions pour les acteurs publics locaux apparaissent : obligations de recourir à des sous-traitants, articulation de la protection des données avec le dispositif des lanceurs d'alerte, conformité des données à vérifier, analyses d'impact à mener…
Et les collectivités vont devoir articuler ces nouvelles obligations avec celle de l'open data et de l'utilisation des données. Décryptage de ce nouveau cadre juridique de l'ouverture des données publiques.

Par Elise Humbert, Alexandra Aderno et Aloïs Ramel, avocats à la cour, SCP Seban et associés

1

Quels textes régissent la nouvelle réglementation sur la protection des données personnelles ?

Cette nouvelle réglementation correspond au 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, applicable à compter du 25 mai 2018, et à la directive (UE) 2016/680 du 27 avril 2016 relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, qui doit être transposée d'ici le 6 mai 2018.
En droit national, le projet de loi relatif à la protection des données personnelles du 13 décembre 2017, en cours d'examen, transpose la directive précitée et modifie la loi du 6 janvier 1978 pour la mettre en conformité avec ces nouveaux textes et en préciser les conditions d'application.

2

Quels sont les objectifs de cette nouvelle réglementation ?

Le règlement général sur la protection des données (RGPD), tel que le prévoit son article 1er, vise à :
– définir une réglementation européenne unique, adaptée à l'évolution des technologies, applicable à toutes les entreprises basées en Europe mais aussi à celles basées hors de l'Union européenne qui proposent des services en Europe ;
– protéger les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des **données à caractère personnel** ;
– garantir parallèlement la libre circulation des données à caractère personnel au sein de l'Union.
Cette nouvelle réglementation était d'autant plus nécessaire que la directive 95/46/CE du 24 octobre 1995 qui prévalait jusqu'alors, et qui sera abrogée dès l'entrée en application du RGPD, soit le 25 mai 2018, était devenue particulièrement désuète.

3

Quelles en sont les principales mesures ?

La principale innovation portée par le RGPD consiste en l'inversion de la logique de contrôle. Alors que la directive 95/46/CE sur la protection des données reposait en grande partie sur la notion de « formalités préalables » (régime déclaratif et d'autorisation), le nouveau règlement européen substitue à ce contrôle a priori une logique de responsabilisation.
Parmi les 99 articles qui composent le RGPD, on peut également retenir l'obligation pour les entreprises victimes de fuite de données de signaler leur cas aux régulateurs nationaux sous trois jours, le renforcement des sanctions encourues, la portabilité des données ou le droit à l'oubli, qui permettra aux utilisateurs de demander le transfert de leurs données d'une plateforme vers une autre.

4

Qui est concerné par le RGPD ?

Cette nouvelle réglementation renforce les garanties en matière de protection des données personnelles de toute personne physique, indépendamment de sa nationalité ou de son lieu de résidence, qui fait l'objet d'un traitement de ses données personnelles par un organisme basé sur le territoire de l'Union européenne (UE) ou hors de l'UE lorsqu'il propose des services dans l'UE. Elle est donc susceptible de concerner un champ de personnes physiques très large.
Protectrice, cette nouvelle réglementation est également prescriptive pour un grand nombre de personnes morales parmi lesquelles les collectivités territoriales, quelle que soit leur taille.
Si certaines des obligations issues de ces textes ne sont pas applicables en deçà de certains seuils (tenue d'un registre des activités de traitement), d'autres sont en revanche communes à tous les organismes publics (désignation d'un délégué à la protection des données).

5

A quel traitement de données le RGPD s'applique-t-il ou non ?

D'un point de vue matériel, le règlement s'applique à tous **traitements de données à caractère personnel** complètement ou partiellement automatisés et à ceux non automatisés contenus dans un fichier. D'un point de vue territorial, il s'applique à tout traitement effectué par un **responsable de traitement** ou un sous-traitant installé dans l'UE ou qui propose des biens et services dans l'UE.
A contrario donc, cette nouvelle réglementation ne s'applique pas aux traitements d'informations ne concernant pas une personne physique identifiée ou identifiable. Elle ne s'applique pas davantage aux traitements de données effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, ni encore aux traitements de données concernant des activités qui ne relèvent pas du champ d'application du droit de l'UE, telles que la sécurité nationale.

6

A quoi correspond la nouvelle logique de responsabilisation issue du RGPD ?

Ainsi que le synthétise le Conseil d'Etat dans son avis du 7 décembre 2017 sur le projet de loi relatif à la protection des données personnelles, si la directive de 1995 harmonisait jusqu'alors les pratiques nationales par des « prohibitions absolues, tempérées par un système de formalités préalables allant de la déclaration du traitement, jusqu'à son autorisation sous de strictes contraintes de procédure et de fond, proportionnées au degré d'atteinte portée par le traitement aux libertés […], le nouveau régime opère un renversement complet des logiques antérieures ». Avec le RGPD, la charge de la conformité d'un traitement repose essentiellement sur son responsable, lequel est tenu de mettre en œuvre des mesures appropriées et effectives de nature à démontrer à tout moment sa régularité.

7

Cette logique a-t-elle pour conséquence la suppression de toutes les formalités préalables requises jusqu'alors ?

Oui, cette nouvelle logique de responsabilisation a pour conséquence notoire la suppression de la très grande majorité des formalités préalables à un traitement de données appliquées jusqu'alors.
L'article 9 du projet de loi sur la protection des données personnelles prévoit la suppression du régime de déclaration préalable instauré par les articles 22 à 24 de la loi du 6 janvier 1978, du régime d'autorisation de l'article 25 de la loi du 6 janvier 1978 ainsi que les formalités préalables prévues à l'article 27, à savoir un régime d'autorisation par décret en Conseil d'Etat pris après avis motivé et publié de la **Cnil** a2, à l'exception des traitements mis en œuvre pour le compte de l'Etat agissant dans l'exercice de ses prérogatives de puissance publique, qui portent sur des données génétiques ou des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.

8

Dans quels cas la Cnil pourra cependant être saisie préalablement à un traitement de données à caractère personnel ?

Comme le RGPD laisse aux Etats membres la possibilité de le faire, la France s'apprête à créer une formalité préalable particulière liée au caractère sensible de certaines données. Celle-ci concernera, en l'occurrence, les traitements qui nécessitent l'utilisation du numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, lesquels devraient être autorisés préalablement par un décret cadre pris après avis motivé et publié de la Cnil. Le règlement prévoit en outre, de façon générale, que si au terme de l'étude d'impact diligentée par un responsable de traitement, il apparaît que les opérations de traitement des données comportent un risque élevé que ledit responsable ne peut atténuer en prenant des mesures appropriées compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre, il devra consulter l'autorité de contrôle avant que le traitement n'ait lieu.

9

Comment vont s'articuler de façon théorique le RGPD et la loi en cours d'examen ?

D'application directe à compter du 25 mai 2018, le RGPD prévoit cependant de nombreuses marges de manœuvre permettant aux Etats de préciser certaines dispositions ou d'accroître certaines garanties.
C'est donc pour partie l'objet du projet de loi examiné actuellement. A noter que le gouvernement a fait le choix de conserver, au niveau national, la loi du 6 janvier 1978 en raison de sa valeur symbolique et par conséquent de procéder à sa mise en conformité au RGPD. Certaines dispositions de la loi du 6 janvier 1978 devraient ainsi être abrogées, d'autres réécrites. Ce projet de loi maintient cependant pour certaines dispositions un simple renvoi au RGPD.
De sorte que le Conseil d'Etat a relevé un manque de lisibilité du droit positif. Aussi, a été ajoutée une disposition à ce projet habilitant le gouvernement à prendre, dans un délai de six mois, une ordonnance pour procéder à une réécriture de l'ensemble de la loi du 6 janvier 1978.

10

Quelles sont les principales dispositions figurant aujourd'hui dans ce projet de loi ?

Outre les dispositions dédiées à la transposition de la directive (UE) 2016/680 figurant au titre III du projet de loi, affectant moins directement les collectivités territoriales, le projet de loi est articulé autour de deux titres principaux.
Le premier est consacré à la définition des moyens et des conditions de fonctionnement de la Cnil, autorité de contrôle nationale.
Le second traite des marges de manœuvre permises par le règlement et procède, notamment, à la simplification des formalités préalables à la mise en œuvre des traitements conformément à la nouvelle logique de responsabilisation, à la définition d'une réglementation spécifique applicable à certaines catégories particulières de traitement (à l'instar des traitements effectués dans le domaine de la santé) ou encore à la détermination du champ des personnes publiques susceptibles d'être destinataires d'une amende administrative.

11

De quel délai les collectivités territoriales disposent-elles pour se mettre en conformité avec le RGPD ?

Elles ont théoriquement jusqu'au 25 mai 2018, puisque le RGPD sera opposable à partir de cette date.
Cependant, la tardivité de l'examen du projet de loi relatif à la protection des données, lequel a vocation à préciser de façon substantielle les conditions d'application du RGPD, conduira nécessairement à une entrée en application progressive de ces dispositions.
Dans un entretien accordé à la revue en ligne Contexte, le 19 juin 2017, Isabelle Falque-Pierrotin, présidente de la Cnil, indiquait elle-même qu'il ne fallait pas voir « le RGPD comme un couperet en 2018 » et qu'il fallait « déconstruire cette idée qu'il y aura un coup de tonnerre en mai 2018 et que, comme des petits soldats, les entreprises devront être prêtes à 100 % ».

12

Quelles sont les principales obligations auxquelles les collectivités territoriales doivent répondre au plus tôt ?

La première des obligations des collectivités territoriales et la plus tangible est la désignation d'un délégué à la protection des données personnelles (voir questions 15 à 29). Une fois ces « pilotes » désignés et avec leur concours, les collectivités devront procéder à un recensement de l'ensemble des traitements de données auxquels elles ont recours. Elles pourront pour cela saisir la Cnil d'une demande portant sur l'ensemble des traitements lui ayant été déclarés. Ceci, en vue d'établir un registre permettant de satisfaire à leur nouvelle obligation de transparence. Les collectivités devront ensuite déterminer les principales actions à diligenter pour assurer la conformité de ces traitements de données avec les nouveaux droits de leurs administrés, procéder aux modifications contractuelles requises par les obligations de leurs sous-traitants et définir des processus internes de gestion des risques.

13

Quelles sont les sanctions prévues à l'encontre des collectivités qui méconnaissaient cette réglementation ?

Les articles 58 et 83 du RGPD confèrent aux autorités de contrôle des Etats membres de larges prérogatives pour garantir le respect de cette nouvelle réglementation. Les moyens d'investigation et de sanctions dévolus à la Cnil devraient être précisés par les articles 45 à 48 de la loi du 6 janvier 1978.
De façon générale, la Cnil pourra adresser à une collectivité territoriale un rappel à l'ordre, une injonction de mise en conformité, une limitation temporaire ou définitive du traitement ou encore un retrait de certification. En cas d'atteinte aux droits et libertés, la Cnil pourra également agir en urgence et prendre des mesures conservatoires.
Enfin et sauf évolution, les collectivités n'étant pas expressément concernées par l'exonération dont bénéficie l'Etat de se voir infliger des amendes administratives, elles pourront recevoir de telles sanctions.

14

De quelles ressources disposent les collectivités pour faciliter la mise en œuvre de ces nouvelles obligations ?

En conformité avec le RGPD, la Cnil pourra adopter de nouveaux instruments de droit souple (lignes directrices, référentiels, codes de conduite, dispositifs de certification). Ces outils, auxquels elle avait déjà recours, devraient permettre de clarifier ce qui est attendu des collectivités territoriales sur chaque type de fichier. Dans l'attente, la Cnil diffuse, sur son site, différents « documents pratiques » permettant de mieux appréhender les changements en cours. Elle s'est d'ailleurs engagée avec la Commission d'accès aux documents administratifs (Cada) à produire un pack de conformité sur l'open data visant à recenser les données communicables et la mise en œuvre conforme au RGPD de leur diffusion.
A ce stade donc, on peut légitimement considérer qu'il est exigé des collectivités territoriales qu'elles effectuent les premières démarches en vue de cette mise en conformité et notamment de la désignation d'un **DPO**.

15

La désignation d'un « data protection officer » (DPO) est-elle obligatoire pour toutes les collectivités territoriales ?

Oui, du moins si la collectivité gère des traitements de données personnelles mais on voit mal comment il serait possible que ce ne soit pas le cas. L'article 37 § 1.a) du RGPD précise en effet qu'un DPO doit être désigné lorsque « le traitement est effectué par une autorité publique ou un organisme public ». Partant, les EPCI et autres établissements publics locaux seront tout autant assujettis à cette obligation. En revanche, le G29* a formulé des précisions concernant les DPO au sein de ses lignes directrices adoptées le 13 décembre 2016 et révisées le 5 avril 2017. Ainsi, les personnes privées, mêmes lorsqu'elles sont structurellement liées aux personnes publiques et qu'elles gèrent des services publics locaux, ne doivent pas être considérées comme des organismes publics au sens de cette disposition.

* Groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationales de l'Union européenne.

16

Une société concessionnaire de service public local doit-elle désigner un DPO ?

Si les gestionnaires privés de services publics ne sont pas assujettis à cette obligation au titre de l'article 37 § 1.a) du RGPD, ils pourraient néanmoins y être tenus au titre de l'article 37 § 1.b). En effet, celui-ci dispose qu'un organisme privé dont les activités de base consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées, doit désigner un DPO.
Si cette définition n'est pas immédiatement intelligible, les lignes directrices du G29 donnent notamment l'exemple de l'activité hospitalière et des transports. On peut dès lors imaginer que la plupart des concessionnaires de services publics locaux soient soumis à une obligation comparable. En toute hypothèse, lorsque la désignation d'un DPO n'est pas obligatoire, elle est fortement conseillée par le G29.

17

Quel est le rôle du DPO ?

Le DPO (ou, en français, **DPD** pour délégué à la protection des données), qualifié de véritable pierre angulaire du régime de responsabilité prévu par le RGPD par le G29, a pour rôle de faciliter le respect des règles de traitement des données par la mise en œuvre d'outils de responsabilité et d'agir comme intermédiaire entre l'organisme, les personnes physiques concernées et l'autorité de contrôle (la Cnil).
Plus précisément, d'après l'article 39 du RGPD, le DPO informe et conseille le responsable du traitement et les employés sur les obligations en matière de traitement de données, contrôle le respect du RGPD, préconise toute analyse d'impact nécessaire, coopère avec l'autorité de contrôle en lui facilitant l'accès aux données et fait office de point de contact avec celle-ci.

18

De quels moyens dispose-t-il pour agir ?

Le responsable du traitement doit aider le DPO à exercer ses missions en lui fournissant les « ressources nécessaires » (article 38 § 2 du RGPD). Concrètement, la direction de l'organisme doit faire preuve d'un soutien actif pour la fonction de DPO (en termes de communication interne et externe, notamment), lui ménager les conditions matérielles nécessaires à l'exercice de sa fonction (temps nécessaire, formation, ressources financières, composition d'une équipe calibrée), lui permettre d'agir de façon indépendante (absence de toute sanction), lui faciliter l'accès aux données et aux opérations de traitement et, enfin, participer à la prévention des conflits d'intérêts.

19

Quelles sont les différences entre le correspondant informatique et libertés (CIL) et le DPO ?

Le DPO est le successeur naturel du **correspondant informatique et libertés (CIL)**, car leurs missions sont comparables. Néanmoins, les prérogatives du DPO sont renforcées, notamment en ce qui concerne le rôle de conseil et de sensibilisation sur les obligations relatives à la protection des données personnelles. A cet égard, le fait que le RGPD implique dorénavant une logique de responsabilité (sans déclaration ni autorisation préalables) est de nature à renforcer considérablement l'importance du DPO par rapport au CIL. Par ailleurs, des exigences accrues sur la qualification du DPO sont posées. Les ressources dont le DPO doit bénéficier sont encore mieux garanties. Surtout, la nomination d'un DPO est parfois obligatoire (elle l'est toujours pour les personnes publiques), là où l'existence d'un CIL n'était que recommandée.

20

Qui peut être DPO ?

Le DPO doit réunir des compétences particulières, comme le précise l'article 37 § 5 du RGPD. Il doit d'abord avoir les qualités professionnelles requises : une expertise sur la législation et les pratiques en matière de protection des données, une bonne connaissance du secteur d'activité et de l'organisation de l'organisme (opérations de traitement, systèmes d'information utilisés, besoins). Cette qualification suppose une adaptation permanente et une formation continue.

Le DPO doit ensuite jouir d'un positionnement efficace s'il est désigné en interne, afin de pouvoir dialoguer directement avec le niveau le plus élevé de l'organisation et d'animer une équipe d'experts. Enfin, le DPO devra être en capacité de communiquer efficacement et d'exercer ses fonctions en toute indépendance, en se prémunissant de tout conflit d'intérêts.

21

Dans quel cas le DPO pourrait-il être en conflit d'intérêts ?

Le risque de conflit d'intérêts surviendra plus souvent lorsque le DPO est interne à l'organisme. En effet, il est permis à celui-ci d'exercer d'autres fonctions en son sein. Dans ce cas, il faudra veiller à ce que ces fonctions ne l'amènent pas à participer à la détermination des finalités et des moyens du traitement. En règle générale, cela conduit à écarter toutes les fonctions d'encadrement supérieur, ainsi que d'autres fonctions plus subalternes si elles ont conduit la personne à déterminer ces finalités et moyens. En cas de DPO externe, il y aura également conflit d'intérêts si celui-ci est appelé à représenter le responsable du traitement devant les juridictions pour des affaires en lien avec la question de la protection des données.

22

Quelles sont les sanctions encourues par le DPO dans l'exercice de ses fonctions ?

Le DPO ne peut pas être tenu pour responsable de l'absence de conformité des traitements qu'il a pour mission de contrôler. Seul le responsable du traitement (ou son sous-traitant) peut, aux termes du RGPD, être tenu responsable de la non-conformité des traitements de données à caractère personnel. Cette responsabilité ne peut, au demeurant, être transférée par voie de délégation au DPO. Cela ne saurait néanmoins empêcher d'éventuelles poursuites pénales si le DPO se rendait intentionnellement complice d'une infraction aux règles de protection en vigueur.

Par ailleurs, le DPO doit agir en toute indépendance et ne peut être exposé à des sanctions par l'organisme au titre de l'exercice de ses fonctions. Toute forme de sanction est ainsi strictement interdite à son égard (par exemple, tout frein à l'avancement de carrière, une absence de promotion ou un refus d'octroi d'avantages).

23

Quels sont les avantages et inconvénients à désigner un DPO en interne ?

Les avantages à nommer un DPO interne sont nombreux. En premier lieu, il connaît parfaitement l'organisme public et en maîtrise le fonctionnement et les rouages. En général, il utilise lui-même depuis longtemps les systèmes d'information et les traitements qu'il faut commencer par auditer, ce qui permet de gagner du temps et d'avoir une compréhension immédiate des finalités et du contenu des traitements, tout en étant sûr qu'il y a peu de risques qu'un traitement échappe à sa vigilance.
Toutefois, les inconvénients sont, eux aussi, marqués. Le lien hiérarchique fort existant dans la plupart des administrations peut grandement conditionner l'exercice par le DPO de ses fonctions et porter préjudice à sa nécessaire indépendance. Un certain manque de recul, affectant son objectivité, pourrait aussi nuire au parfait exercice de ses missions.

24

Quels sont les avantages et inconvénients à désigner un DPO en externe ?

La désignation d'un DPO externe aura pour principaux avantages la garantie d'indépendance et du niveau d'expertise, puisque celui-ci aura pu être choisi après une mise en concurrence et une comparaison des références et degrés de qualification. En outre, les préconisations des conseils externes sont parfois prises plus au sérieux que les consignes internes n'émanant pas de la direction générale.
Parmi les inconvénients, le DPO externe ne maîtrisera pas aussi bien, au moins dans les premiers temps de sa mission, le fonctionnement de l'organisme et le contenu opérationnel de ses missions. Son travail d'audit initial peut également être vécu comme une intrusion par le personnel, ce qui peut se traduire par un défaut de fluidité de l'information et compliquer l'accomplissement de ses missions.

25

Un DPO peut-il être commun à plusieurs administrations ?

Oui. Cette pratique est autorisée par l'article 37 § 3 du RGPD, qui indique qu'un seul DPO peut être désigné par plusieurs autorités publiques « compte tenu de leur structure organisationnelle et de leur taille ».
On peut imaginer que le RGPD entend par là imposer la même condition qu'il pose dans les situations analogues concernant des entreprises : il faut, en toute hypothèse, que le DPO reste facilement joignable par chaque organisme. Cela signifie que la mutualisation des fonctions de DPO ne doit pas nuire au bon exercice de l'une de ses missions essentielles, soit la disponibilité qu'il doit avoir pour les personnes concernées, l'autorité de contrôle et le personnel interne de l'organisme. Sous cette réserve, rien n'empêche différentes collectivités de mutualiser leur DPO ou de faire appel au même prestataire pour exercer ces fonctions.

26

Comment est formalisée la désignation d'un DPO en interne ?

La Cnil publiera d'ici le 25 mai 2018 un formulaire de désignation en ligne du DPO. Une fois le DPO interne désigné et ce formulaire rempli, l'article 37 § 7 du RGPD impose au responsable du traitement de publier les coordonnées du délégué et de les communiquer à l'autorité de contrôle. Comme l'expliquent les lignes directrices du G29 concernant les délégués à la protection des données dans leur dernière version du 5 avril 2017, ces exigences visent à garantir que les personnes concernées (en interne comme en externe) et l'autorité de contrôle puissent aisément prendre contact avec le DPO, sans devoir s'adresser à un autre service de l'organisme, dans l'optique de garantir une confidentialité optimale.

27

Comment est formalisée la désignation d'un DPO en externe ?

Les mêmes formalités que pour les DPO internes sont à respecter. En outre, comme pour tout marché de prestation de service, le choix d'un DPO externe par une collectivité territoriale ou un établissement public devra respecter les obligations habituelles de publicité et de mise en concurrence lorsque la valeur des prestations excédera 25 000 € HT.

28

Qu'est-ce que la charte de déontologie du délégué à la protection des données personnelles ?

L'Association française des correspondants à la protection des données à caractère personnel (AFCDP) a publié cette charte le 28 décembre 2017. Elle contribue à la bonne application du RGPD et de ses lignes directrices. Y sont formulées les règles de conduite devant régir l'action des DPO. Tous, qu'ils soient internes, externes ou mutualisés, peuvent adhérer à cette charte. Elle garantit le bon exercice des fonctions de ces DPO et peut être invoquée à l'encontre des responsables de traitement, sous-traitants, employeurs, partenaires internes et externes des organismes, de la Cnil, d'autres DPO ainsi qu'aux personnes concernées.

29

Quels conseils pratiques préconiser dans le choix du DPO ?

Il peut être judicieux pour les personnes publiques de désigner initialement un DPO externe pour les premières années d'application du RGPD. Cela permet d'être certain de s'entourer de professionnels avisés, qui vont pouvoir dégrossir le travail de recensement et procéder aux révisions les plus urgentes.
Néanmoins, les collectivités les plus importantes, fortement dotées en personnel, une fois cette première phase de quelques années écoulée, éprouveront vraisemblablement l'envie de désigner un DPO interne. En outre, des filières de formation spécialement dédiées au sujet ont vocation à se développer ; elles pourront bénéficier aux agents de la fonction publique. Une prestation de soutien externe pourra néanmoins être conservée pour les cas les plus épineux, ce qui permettra à l'organisme de bénéficier des avantages respectifs des deux possibilités.

30

Quelles grandes orientations peuvent affecter les collectivités territoriales ?

Les collectivités seront désormais soumises à la logique générale de responsabilisation. Elles n'auront plus à réaliser de formalités en amont de la mise en place de leur traitement de données. Cette responsabilisation s'accompagne de la nécessaire mise en place de mesures techniques et organisationnelles pour démontrer en permanence qu'elles offrent un niveau optimal de protection aux données traitées. Cela nécessite qu'elles soient bien documentées sur les actions menées pour démontrer la conformité des traitements et qu'elles soient bien organisées, en procédant, par exemple, à l'élaboration de registres.
Partant, les collectivités sont responsables, dès la conception, du traitement de leurs données, et par défaut. Cela signifie qu'elles doivent tenir compte des règles de protection des données dès la phase de conception du produit, du service ou du traitement, et dès qu'elles définissent les outils utilisés et les paramétrages par défaut.

31

Le RGPD entraîne-t-il une « révolution culturelle » pour les collectivités ?

Si les collectivités seront soumises à une logique inversée en matière de gestion des données personnelles et si elles devront obligatoirement désigner un délégué à la protection des données pour se conformer au RGPD, en revanche, la loi « informatique et libertés » du 6 janvier 1978 leur est toujours applicable. Par conséquent, elles doivent toujours respecter les grands principes, énumérés par cette loi, lors de la collecte, du traitement et de la conservation des données. Ainsi, les collectivités continuent d'appliquer :
– le principe de finalité,
– le principe de proportionnalité,
– le principe d'une durée limitée de conservation des données,
– le principe de sécurité et de confidentialité des informations,
– le principe du respect des droits des personnes.

32

Quelles sont les conséquences du RGPD pour les sous-traitants des collectivités ?

Les sous-traitants des collectivités territoriales doivent obligatoirement participer à la démarche de mise en conformité des traitements de données, en les aidant à satisfaire leurs diverses obligations. Sont concernés les prestataires de services informatiques, les agences de communication et, de façon générale, tout organisme offrant un service impliquant un **traitement de données à caractère personnel** A-Z.
Partant, à compter du 25 mai 2018, ils ne pourront plus se contenter de suivre les instructions des collectivités responsables du traitement pour protéger la sécurité et la confidentialité des données. Ils devront adopter une démarche active auprès des responsables de traitement dès lors qu'ils sont eux aussi concernés par la logique de responsabilisation. Ils ont ainsi une obligation de conseil et d'assistance dans le cadre de la réalisation des analyses d'impact, doivent participer à la destruction des données et contribuer aux audits.

33

Quelles obligations incombent aux sous-traitants ?

Les sous-traitants ont tout d'abord une obligation de transparence et de traçabilité. Celle-ci doit les conduire à mettre à la disposition des collectivités territoriales les informations nécessaires pour démontrer le respect de leurs obligations et à tenir un registre qui recense et décrit les traitements effectués. En outre, s'ils sont sélectionnés pour la conception de traitement de données, ils doivent garantir le respect des principes de protection de données dès la conception et par défaut.
Ils doivent garantir la sécurité des données traitées notamment au regard des principes de l'obligation de confidentialité imposée à leurs salariés.
Ils ont enfin une obligation d'assistance, d'alerte et de conseil qui doit les conduire à alerter les collectivités territoriales si leurs instructions violent des règles en matière de protection de données, à les assister pour répondre aux demandes d'exercice des droits de rectification, opposition ou portabilité des données.

34

Quelles sont les modifications des clauses de marchés publics conclus avec les sous-traitants à envisager ?

A compter du 25 mai 2018, les marchés publics conclus avec des sous-traitants devront comprendre les clauses obligatoires prévues par le RGPD. A cet égard, des avenants aux contrats, qui peuvent d'ores et déjà être préparés, procéderont à ces ajouts. Ces clauses doivent permettre de fixer précisément les obligations et la responsabilité du sous-traitant à l'égard du responsable de traitement.
Les clauses devront également détailler les modalités d'information des personnes concernées par les opérations de traitement au moment de la collecte des données.
Les modalités de transmission des demandes d'exercice des droits des personnes concernées par les traitements de données ainsi que les obligations des sous-traitants pour intervenir en la matière seront fixées. La méthode de notification des violations de données à caractère personnel sera également décrite.

35

Comment assurer la conformité du dispositif de lanceur d'alerte au RGPD ?

L'autorisation unique AU-004 a vocation à encadrer les traitements de données à caractère personnel dans le cadre des dispositifs d'alertes professionnelles. Les organismes qui mettent en place un traitement de données dans le cadre de ce dispositif peuvent donc procéder auprès de la Cnil à une déclaration simplifiée de conformité à l'AU-004, si leur dispositif correspond bien à ce qui est prévu dans cette autorisation.
Quand bien même il n'apparaît pas, à ce jour, que la Cnil effectue par ce biais un exercice de vérification sur place de la conformité du dispositif à l'AU-004, cette autorisation unique conservera toute son utilité à compter du 25 mai 2018, puisqu'elle expose de quelle façon les risques relatifs au traitement de données à caractère personnel pour les personnes concernées peuvent et doivent être minimisés.

36

Quelles garanties le label gouvernance informatique et libertés offre-t-il ?

Le label « gouvernance informatique et libertés » est délivré par la Cnil qui procède à un examen de conformité de l'organisme candidat à vingt-cinq exigences fixées par un référentiel. Toute collectivité territoriale, dès lors qu'elle a désigné un correspondant informatique et libertés, peut solliciter la délivrance du label. Ce label permet d'attester de la qualité des procédures en place.
Le référentiel a récemment été modifié en prévision de l'entrée en vigueur du RGPD. Une délibération n° 2017-219 du 13 juillet 2017 l'a fait évoluer pour prendre en compte les exigences du RGPD. Par conséquent, le label délivré depuis garantit la conformité aux règles applicables en matière de protection des données.

37

Quels points de vigilance sont à respecter en matière de vidéosurveillance ?

Devant l'enchevêtrement des dispositions applicables en matière de vidéoprotection (loi « informatique et libertés » et/ou code de la sécurité intérieure), il est parfois difficile pour les collectivités de respecter l'ensemble des règles édictées en matière de protection de la vie privée et de réaliser les démarches correspondant aux systèmes de caméras mis en place (autorisation préfectorale, autorisation Cnil ou déclaration). Jusqu'à présent, les contrôles sur place de la Cnil sont rares.
Néanmoins, à compter du 25 mai 2018, les contrôles seront plus fréquents et les sanctions plus lourdes. Il est donc préférable, pour les collectivités doutant de la conformité de leur dispositif aux règles de protection des données, de saisir dès à présent la Cnil pour avis et de vérifier que les démarches préalables ont été respectées.

38

Quels sont les points de vigilance s'agissant de la décentralisation du stationnement payant ?

La réforme du stationnement payant, en vigueur depuis le 1er janvier 2018, a conduit les collectivités territoriales à recourir à de nouveaux services impliquant le traitement de données personnelles, telles que la lecture automatisée de plaques d'immatriculation (Lapi). Ce service implique la collecte du numéro de plaque d'immatriculation des véhicules en stationnement. Il appartient aux collectivités de s'assurer de la conformité de leur dispositif au RGPD. Elles peuvent tout d'abord suivre les recommandations de la Cnil qui régissent les modalités de captation des plaques d'immatriculation, à l'exclusion de toute autre donnée à caractère personnel. Celles-ci prévoient que ce dispositif ne constitue qu'un précontrôle qui nécessité ensuite de diligenter sur place des agents assermentés. Toutefois, dès lors que des interrogations en la matière subsistent, la réalisation d'une analyse d'impact peut permettre de lever certains doutes.

39

Comment assurer la conformité des téléservices publics locaux au RGPD ?

L'arrêté du 4 juillet 2003 encadre les traitements automatisés de données à caractère personnel mis en œuvre par les collectivités responsables de téléservices publics locaux. Ces téléservices permettent aux administrés d'effectuer en ligne certaines démarches administratives. Leur mise en œuvre est subordonnée à une déclaration de conformité à l'acte réglementaire unique RU-030. Comme pour les dispositifs de lanceur d'alerte, toute collectivité territoriale mettant en place un téléservice peut procéder auprès de la Cnil à un engagement de conformité à ce RU-030.
A compter du 25 mai 2018, l'engagement à ce RU garantit la conformité du traitement des données collectées dans le cadre des téléservices. A plus forte raison, ces services à distance devront être audités afin de garantir un paramétrage par défaut pour limiter le nombre et la nature des données collectées. Il peut s'agir d'utiliser des menus déroulants et de favoriser les caches à cocher.

40

Comment assurer la conformité de transfert de données consécutif à un transfert de compétences ?

Les transferts de compétences entérinés par la loi «Notre» du 7 août 2015 ou les délégations de compétences fondées sur l'article L. 1111-8 du code général des collectivités territoriales (CGCT) peuvent donner lieu à la redistribution de données personnelles entre les différents niveaux de collectivités territoriales concernées. Afin de garantir la bonne gestion des données personnelles au regard du RGPD, les collectivités qui vont recevoir ces données doivent rapidement garantir leur sécurité. Elles doivent ainsi mettre en place des mesures techniques et organisationnelles pour assurer les accès distants de données, mettre à jour les dossiers de sécurité des téléservices et prononcer leur homologation. Ce lourd travail peut s'accompagner d'une étude d'impact sur la vie privée. Le rôle du DPO sera ici déterminant.

41

Dans quel cas recourir à une analyse d'impact relative à la protection des données (DPIA) ?

Dès lors que le traitement de données personnelles est susceptible d'engendrer des risques élevés pour la vie privée des administrés, les collectivités territoriales devront effectuer des analyses d'impact. Ces Data Privacy Impact Assessment (DPIA) doivent leur permettre de mettre en place des traitements de données respectueux de la vie privée.
Le DPIA est obligatoire quand le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Les traitements qui remplissent ces critères concernent la surveillance systématique de zones accessibles au public (télésurveillance), la collecte de données sensibles ou à large échelle, le traitement de données biométriques ou de données relatives à des infractions ou des condamnations pénales.

42

Quels sont les documents constituant le registre de conformité ?

Etre en conformité avec la loi «informatique et libertés» ne suffit pas, encore faut-il pouvoir démontrer cette conformité. C'est l'élaboration et la mise à jour du registre de traitements qui peut constituer la preuve de cette conformité. La collectivité doit donc, en premier lieu, disposer d'un registre qui liste les traitements qui ont eu lieu sous sa responsabilité. Y sera joint la description des procédures et moyens adaptés pour la sécurité des traitements, les procédures internes en cas de violation de données, les informations sur le DPO, les modèles de recueil du consentement et les procédures mises en place pour l'exercice des droits.
Le DPIA pourra compléter, le cas échéant, cette documentation. Le sous-traitant de la collectivité devra également tenir son propre registre d'activités.

43

Comment assurer la conformité de la gestion des fichiers des administrés ?

Le maire ou le président de la collectivité territoriale qui met en place le traitement de données à caractère personnel est le responsable de traitement. Par conséquent, l'exécutif est responsable dans l'hypothèse où un élu local ferait un mauvais usage des fichiers créés. A cet égard, avant l'entrée en vigueur du RGPD, qui renforce les sanctions en cas de non-conformité, il apparaît judicieux de mettre en place des formations au profit des élus visant à rappeler les règles d'utilisation des fichiers d'administrés. Parmi ces règles, rappelons que les registres d'état civil ne peuvent être utilisés à des fins de communication politique ou encore que les données recueillies à l'occasion du recensement ne peuvent être utilisées pour alimenter des fichiers d'administrés.

44

Quelles précautions prendre pour assurer la conformité de l'open data ?

Certains des documents soumis à l'obligation de publicité contiennent des données personnelles ou des données qui, sans être personnelles, permettent, par le recoupement d'informations, d'identifier une personne. Or, la collectivité territoriale doit empêcher que les données transmises puissent, par leur utilisation, porter atteinte à la vie privée d'administrés.
Plusieurs mesures peuvent donc être mises en œuvre pour éviter de contrevenir au RGPD lors de la publication de ces informations. En amont, cela nécessite d'auditer les documents d'ores et déjà publiés. Les techniques d'anonymisation de données, si elles sont chronophages, peuvent permettre de réduire les risques d'atteinte à la vie privée sans retirer tout intérêt à l'open data.

45

A quelles obligations d'open data les collectivités sont-elles soumises ?

Conformément à l'article L. 312-1-1 du code des relations entre le public et l'administration (CRA) issu de la loi n° 2016-1321 du 7 octobre 2016, dite loi «Lemaire», les collectivités territoriales de plus de 3500 habitants comptant plus de 50 agents sont tenues, lorsque ces documents sont disponibles sous format numérique, de publier en ligne les documents suivants :
– les documents communicables (en principe depuis le 7 avril 2017)
– les documents figurant au répertoire tenu par les administrations des principaux documents contenant des informations publiques (en principe depuis le 7 octobre 2017)
– les bases de données, mises à jour de façon régulière, qu'elles produisent ou qu'elles reçoivent (d'ici le 7 octobre 2018)
– les données, mises à jour de façon régulière, dont la publication présente un intérêt économique, social, sanitaire ou environnemental (d'ici le 7 octobre 2018).

46

Quelles sont les sanctions encourues en cas de méconnaissance par une collectivité de ces nouvelles obligations ?

Lorsqu'une collectivité ne procède pas spontanément à mise en ligne d'un document soumis à une obligation «open data», un administré peut saisir la Cada de ce refus de publication (article L. 342-1 du CRPA).
La procédure est ensuite la même que celle actuellement suivie pour une demande de communication de documents administratifs. De sorte qu'en cas de non-soumission de l'administration à cette nouvelle obligation de diffusion de données, celle-ci pourrait y être contrainte au terme d'une procédure contentieuse devant les juridictions administratives, dont la recevabilité sera cependant conditionnée à la saisine préalable pour avis de la Cada.

47

Dans quelles hypothèses l'open data doit être concilié avec la protection des données personnelles ?

La grande majorité des documents soumis à une obligation de mise en ligne ne comporte aucune **donnée personnelle** et n'a donc pas vocation à donner lieu à des exigences complémentaires liées à l'entrée en application du RGPD.
L'article L. 312-1-1 du CRPA impose cependant aux collectivités, d'ici le 7 octobre 2018, la mise en ligne des bases de données qu'elles produisent ou qu'elles reçoivent ainsi que les données dont la publication présente un intérêt économique, social, sanitaire ou environnemental, dans le respect des limites définies aux articles L. 311-5 et L. 311-6 dudit code et par suite de la protection de la vie privée.
C'est donc dans le cadre de la mise en ligne de ce type de documents susceptibles de comporter des données personnelles, que les collectivités s'interrogent aujourd'hui légitimement sur la conciliation de ces deux nouvelles réglementations.

48

Quelles préconisations respecter en cas de mise en ligne d'un document comportant des données personnelles ?

Lors d'une journée d'étude le 16 octobre 2017, Alice de La Mure, juriste à la Cnil, a souligné que la conciliation des exigences de transparence et de protection des données personnelles devait conduire les collectivités à faire preuve de pragmatisme, formulant à leur égard une double recommandation :
– parvenir à un niveau d'anonymisation qui, à défaut d'être parfait, soit a minima satisfaisant au regard de l'avis rendu par les Cnil européennes le 10 avril 2014 ;
– proscrire dans le même temps toute réutilisation des données ayant pour objet ou effet d'identifier de nouveau les personnes physiques initialement concernées par les informations diffusées.
La Cnil n'a pas manqué cependant de relever le caractère complexe de l'exercice et l'utilité du pack de conformité annoncé pour ce début d'année 2018, aux fins de clarifier les attendus.

49

En quoi ces deux réglementations peuvent conduire les collectivités à engager une réflexion politique globale ?

Moins de 5 % des 4 500 collectivités territoriales concernées par la loi open data pratiquent aujourd'hui l'open data. Or, l'entrée en application du RGPD, lequel apparaît davantage prescriptif car assorti de sanctions plus lourdes, va conduire les collectivités territoriales à s'interroger sur l'échelle pertinente de gouvernance et l'organisation interne optimale pour la gestion et la protection des données des administrés.
A cette occasion pourrait être menée, en cohérence, une réflexion plus globale sur la politique de la data à engager par la collectivité territoriale.

50

Quels seraient les différents scénarios possibles ?

Schématiquement, on peut distinguer trois options principales :
– celle de rejoindre les collectivités pionnières de l'open data et de s'astreindre parallèlement à l'obtention d'une certification permettant d'être vertueux quant à la protection des données personnelles (le DPO serait alors « haut placé » dans la hiérarchie administrative) ;
– l'option « juridique », soit l'application la plus rigoureuse possible des textes privilégiant éventuellement un accompagnement externe temporaire et tendant à l'obtention d'un label Cnil (le DPO désigné serait alors probablement le directeur juridique ou en externe un cabinet d'avocats) ;
– l'option « technique », garantissant une connaissance précise des outils de traitement des données et de leur potentialité et une politique de transparente restreinte à l'essentiel (le DPO désigné serait alors probablement le directeur des services informatiques).

JOURNÉE D'ÉTUDE

Technical Circle

JEUDI 5 AVRIL 2018 – PARIS

Réseaux d'eau intelligents

SMART WATER ET NOUVELLES TECHNOLOGIES : COMMENT OPTIMISER SA GESTION DE L'EAU

Les données issues des réseaux d'eau et centralisées dans le Smart water network ouvrent de nouvelles perspectives de gestion et de services. Comment orchestrer normalisation, interopérabilité, mutualisation des équipements et optimisation des coûts.

- Smart Water : des réseaux d'eau de plus en plus intelligents pour une meilleure gestion des flux hydrauliques
- Comment choisir aujourd'hui une technologie du télérelevé adaptée aux besoins de demain
- Analyse du contexte normatif. Quel niveau d'interopérabilité peut-on en attendre
- Comment mettre en oeuvre une mutualisation des équipements avec les autres services et d'autres acteurs du territoire
- Quels sont les équipements et services proposés par les opérateurs au travers de retours d'expériences

Journée animée par Joël GRANDGUILLOT,
DGST S.A, communauté d'agglomération

INSCRIVEZ-VOUS DÈS MAINTENANT !

Programme complet et inscription sur :
conferences.lesechos.fr/conferences.com
Rubrique « Conférences », journée d'étude « Réseaux d'eau intelligents »

Elodie BOULET
elodie.boulet@leops-digital.com
01 77 98 93 36

Un partenariat avec :

suez

Fluksaqua

Avec le soutien de :

afnor

AITF

amf