LexCase FLASH
Lettre d'information de LexCase
PARIS · LYON · MARSEILLE

IP/IT/DATA

Entités publiques et RGPD : vigilance accrue !

Après avoir mis en demeure 22 communes, par décision du 25 avril 2022, d'avoir à désigner un délégué à la protection des données sous 4 mois, la CNIL continue à s'intéresser au secteur public en publiant un guide de la responsabilité des acteurs dans le cadre de la commande publique.



Si vous n'avez que 30 secondes

La Commission Nationale de l'Informatique et des Libertés (CNIL) a publié le 2 juin 2022 un guide afin d'aider les entités publiques à identifier leurs responsabilités et celles des opérateurs économiques dans différents contextes de commande publique.

Le guide vise à accompagner les organismes concernés dans l'identification de leurs qualités et obligations au regard des dispositions du Règlement Général sur la Protection des Données (RGPD).

Les éclairages fournis par la CNIL sont bienvenus, tant la détermination de la qualification de l'entité publique (en tant que responsable de traitement, sous-traitant ou co-responsable de traitement) peut s'avérer difficile dans certains cas.

Or les enjeux sont importants, puisqu'il s'agit également de déterminer la propriété des données personnelles collectées et traitées dans le cadre du traitement, dont l'importance peut être cruciale en raison en particulier de leur volume et valeur économique.

Ce guide pourra donc utilement servir à expliciter aux opérateurs économiques la qualification retenue par l'entité publique, afin d'éviter des discussions stériles et des désaccords sans fin.

Toutefois, ce guide est trop succinct et n'apporte pas toutes les réponses souhaitées.

Enfin, reste à savoir si ce guide serait susceptible d'avoir des effets notables sur les droits ou la situation des entités publiques, et donc de faire l'objet d'un recours pour excès de pouvoir (voir en ce sens la décision du Conseil d'État en date du 8 avril 2022, req. N°452668 pour des questions-réponses).

1. Un peu de contexte

Les entités publiques confient quotidiennement à des opérateurs économiques la mission de répondre à leurs besoins en matière de travaux, fournitures et services, au travers de la conclusion de marchés publics et de contrats de concession définis et régis par le Code de la commande publique.

Par exemple, les collectivités territoriales et leurs groupements délèguent à des tiers, désignés titulaires ou concessionnaires suivant la nature du contrat, tout ou partie de la gestion de services publics relevant de leurs compétences (services périscolaires, eau et assainissement, transports, stationnement, etc.).

Ce faisant, des traitements de données personnelles sont mis en œuvre, concernant par exemple les administrés, usagers ou employés du service public.

Comme le rappelle la CNIL, ces traitements doivent obligatoirement être réalisés dans le respect du RGPD.

Cette question revêt une importance accrue en raison du risque juridique et d'image s'attachant au non-respect des obligations et à la publicité des décisions de la CNIL.

Vingt-deux communes en ont récemment fait les frais, puisque la CNIL a décidé, par délibération du 5 mai 2022, de publier les mises en demeure d'avoir à désigner un délégué à la protection des données qui leur avaient été adressées le 25 avril 2022, au motif notamment que, compte tenu de leurs missions parfois sensibles et de l'exercice de l'autorité publique, ces communes doivent veiller à la protection des données personnelles qui leur sont confiées, notamment au regard de leurs obligations de sécurité.

La CNIL a ainsi estimé nécessaire « *d'informer les administrés des communes concernées sur le manque de prise en compte des problématiques de protection des données de la part de leur commune et sur le fait que l'absence d'un DPD/DPO* [délégué à la protection des données] *les prive d'un interlocuteur dédié à ce sujet* » (Délibération MEDP-2022-001 du 5 mai 2022).

Les communes en question sont les communes d'Achères, d'Auch, de Bastia, de Beaune, de Bruay la Buissière, d'Etampes, de Gagny, de Koungou, de Kourou, de Le Gosier, de Le Robert, de Montmorency, de Montfermeil, de Petit-bourg, de Pierrefitte-sur-Seine, de Saint-André, de Saint-Benoît, de Saint-Dizier, de Sotteville-lès-Rouen, de Villeneuve Saint-Georges et de Vitry-sur-Seine.

2. Dans quels cas une entité publique doit-elle être qualifiée de responsable de traitement ?

Le responsable de traitement est défini comme l'entité qui détermine, seule ou conjointement avec d'autres, les objectifs (finalités) et les moyens du traitement. En d'autres termes, le pourquoi et le comment.

Le guide rappelle que la qualification d'une entité publique en tant que responsable de traitement peut être prescrite par des dispositions législatives ou réglementaires.

En matière de commande publique, il existe ainsi des dispositions propres à des secteurs d'activité qui prescrivent de manière implicite une qualification de responsable de traitement (par exemple dans le secteur eau et assainissement). Il incombe donc à l'entité publique d'interpréter correctement ces dispositions et d'en tirer les conséquences utiles, en termes de qualification ou non en tant que responsable de traitement.

Toutefois, une telle qualification résultera le plus souvent d'une analyse, traitement par traitement, des circonstances juridiques et factuelles dans lesquelles le traitement de données personnelles intervient.

Il appartient donc à l'entité publique de procéder à cette analyse avant la signature du contrat avec l'opérateur économique.

La CNIL considère que l'entité publique pourra être qualifiée comme responsable de traitement lorsqu'elle se sera spécifiquement intéressée à la fois aux objectifs et aux conditions de mise en œuvre du traitement de données personnelles, par exemple lorsque:

- L'objet même du contrat est la mise en œuvre d'un traitement de données dont les caractéristiques sont alors encadrées dans le contrat (exemple: l'objet du contrat est la réalisation d'une campagne publicitaire dont les finalités et les caractéristiques sont définies par l'entité publique);

- L'entité publique a exigé le déploiement du traitement en le visant dans le cahier des charges et en définissant la nature et l'étendue des besoins à satisfaire (exemple: recours imposé par l'entité publique à un dispositif technologique spécifique qui implique une exploitation de données personnelles, tel qu'un système de lecture automatisé des plaques d'immatriculation pour la facturation et le contrôle du stationnement payant);

- L'entité publique a retenu l'innovation technologique par ses critères de sélection des offres, invité les candidats à fournir des précisions quant aux opérations envisagées en matière de données personnelles, et validé les objectifs et conditions de traitement proposés par l'opérateur économique.

Le fait que l'entité publique ait initialement fourni les données à l'opérateur économique pour traitement n'implique pas nécessairement une qualification de responsable de traitement.

En définitive, il ressort des indications de la CNIL que :

- Lorsqu'elle a spécifiquement demandé la mise en œuvre d'un traitement de données dans un objectif déterminé, l'entité publique sera plus facilement qualifiée de responsable de traitement, et ce même si les instructions fournies pour la mise en œuvre du traitement ne couvrent pas l'ensemble des moyens essentiels de mise en œuvre, ou même si elle ne fait qu'endosser les moyens proposés par l'opérateur économique (y compris les moyens essentiels), dont elle a connaissance;

- Le fait que l'opérateur économique ait pu librement déterminer certains moyens dits non essentiels du traitement, d'ordre technique et organisationnel (par exemple: choix d'un type particulier de matériel/logiciel, détail des mesures de sécurité) est sans incidence sur sa qualification de sous-traitant au sens du RGPD, dès lors qu'il n'a pas disposé d'un pouvoir décisionnel s'agissant des buts poursuivis par la mise en œuvre du traitement et des moyens essentiels ;

- Le fait que l'entité publique n'accède pas, au cours de l'exécution du contrat, aux données traitées par l'opérateur économique, est sans incidence sur sa qualification de responsable de traitement, dès lors que l'opérateur économique agit pour son compte et ne poursuit pas de finalité ou d'intérêt propre, se contentant de traiter les données dans le strict cadre défini par l'entité publique;

- Si l'opérateur économique ne fait que se conformer aux directives de l'entité publique, l'entité publique doit être qualifiée de responsable de traitement.

3. Dans quels cas l'entité publique pourrait ne pas être considérée comme responsable de traitement ?

Notamment dans les cas suivants :

- Si l'entité publique n'a pas spécifiquement besoin du traitement de données en cause (qui n'est pas régi par le contrat), par exemple dans le cadre de marchés ou concessions de travaux, de marchés de fournitures ou de petits marchés de services non centrés sur la gestion des données personnelles;

- Si l'entité publique n'a entendu fixer que l'objectif de la prestation dont résultera le traitement, mais pas les moyens;

- Si le contrat a pour objet l'exécution d'une mission de service public, tout particulièrement lorsqu'il a opéré un véritable transfert de la gestion du service à la charge de l'opérateur économique; ce qui implique que l'opérateur économique dispose d'une liberté dans l'organisation de l'exécution du service public.

4. Et quid de la qualification de responsables conjoints ?

La qualification de responsables conjoints de traitement pourrait être fréquente, et concerner prioritairement les traitements d'usagers intervenant dans le cadre de l'exécution de missions de service public.

En effet, l'opérateur économique jouit alors d'une liberté dans la définition des objectifs et conditions de mise en œuvre du traitement de données personnelles.

Dans ce cas, l'entité publique et l'opérateur économique seront considérés ensemble comme étant responsables de traitement, et devront veiller ensemble au respect du RGPD, ce qui leur imposera de déterminer leurs obligations respectives à ce titre.

Les cas cités par la CNIL sont les suivants:

- L'entité publique a précédemment géré le service en régie;

- Les conditions d'exploitation des données collectées et produites revêtent pour l'entité publique des enjeux économiques, politiques ou juridiques importants notamment en raison de la finalité du traitement ou de la nature des informations en cause (par exemple: des données indispensables à l'exécution du service qui doivent être communiquées à l'entité publique sur simple demande notamment pour permettre la préparation d'une nouvelle en concurrence).

5. Quelles conséquences ?

Le choix de l'opérateur économique doit s'accompagner d'une analyse du statut des acteurs au regard des règles du RPGD, en amont de la conclusion des marchés et concessions.

Cette analyse peut être facilitée par les documents d'appels d'offres, qui permettent de déterminer qui, en pratique, a exercé une influence décisive sur les objectifs et les conditions de mise en œuvre du traitement.

www.lexcase.com

LexCase

Paris
17, rue de la Paix
75002 Paris
Tél. +33 (0)1 40 20 22 22
Fax +33 (0)1 56 72 84 99

Lyon
2, rue Pdt Carnot
69002 Lyon
Tél. +33 (0)4 37 23 11 11
Fax +33 (0)4 37 23 11 00

Marseille
38, rue Grignan
13001 Marseille
Tél. +33 (0)4 91 33 22 22
Fax +33 (0)4 91 33 20 85

SELARL d'avocats au capital de 777.760 € immatriculée sous le numéro 512 642 950 RCS Paris

Les documents contractuels doivent nécessairement inclure les clauses requises par le RGPD en fonction de la qualification retenue, sous peine de sanctions administratives prévues par le RGPD.

Enfin, les contrats conclus avant l'entrée en vigueur du RGPD doivent en principe avoir été mis à jour.

À noter toutefois que la CNIL, comme les juridictions, n'est pas liée par les qualifications figurant dans les contrats.

6. Quid d'un recours pour excès de pouvoir ?

Le Conseil d'État a récemment considéré qu'une question-réponse publiée par la CNIL sur son site Internet est susceptible de produire des effets notables sur la situation des opérateurs concernés, eu égard à sa teneur et au fait que la CNIL fait part de son interprétation d'une disposition de la loi n°78-17 du 6 janvier 1978 telle que modifiée (dite « loi Informatique et Libertés »).

Par conséquent, cette question-réponse et la décision de la CNIL ayant refusé de la retirer sont susceptibles de recours pour excès de pouvoir (CE, 8 avril 2022, req. N°452668).

Il est permis de se demander si une telle analyse est transposable au guide de la responsabilité des acteurs dans le cadre de la commande publique, instrument de « soft law ».

En effet, l'on pourrait considérer que le guide fournit, au moins dans certains cas, des réponses précises à des questions précises, notamment au travers des exemples qui y sont mentionnés. Et donc qu'il contient une interprétation par la CNIL de la loi Informatique et Libertés. C'est d'ailleurs tout l'objet de ce type d'instrument de droit souple.

Par ailleurs, le guide sert de doctrine à la CNIL en cas de contrôle, et son non-respect par les entités publiques pourrait donc avoir des conséquences pour les entités publiques (mises en demeure, sanctions, etc.).

L'analyse ne semble toutefois pas totalement évidente, et mérite donc d'être testée.

Affaire à suivre, donc !

L'ÉQUIPE DROIT IT/IP/DATA DE LEXCASE



Iliana BOUBEKEUR
Avocate associée
iboubekeur@lexcase.com



Guillaume BUSSEUIL
Avocat Collaborateur
gbusseuil@lexcase.com



Manon FAUCHER
Avocat Collaborateur
mfaucher@lexcase.com

LexCase FLASH
Lettre d'information de LexCase

L'ÉQUIPE DROIT PUBLIC DE LEXCASE



Alain de BELENET
Avocat associé
adebelenet@lexcase.com



Raphael APELBAUM
Avocat associé
rapelbaum@lexcase.com



Maxime BUSCH
Avocat associé
mbusch@lexcase.com



Freddy LEPRODHOMME
Avocat Collaborateur
fleprodhomme@lexcase.com



Fanny VANDECASTEELE
Avocat Collaborateur
fvandecasteele@lexcase.com



Alexandre LO-CASTO PORTE
Avocat Collaborateur
alocastoporte@lexcase.com



Florent GADRAT
Avocat Collaborateur
fgadrat@lexcase.com



Claire MARTIN
Avocate Collaboratrice
cmartin@lexcase.com



Stefano ARPANTE
Avocat Collaborateur
sarpante@lexcase.com