Guide des bonnes pratiques contractuelles et recommandations

Pour la mise en place d'une gouvernance de la donnée territoriale

AVERTISSEMENTS

La Caisse des dépôts et consignations décline toute responsabilité dans la mise en œuvre par les collectivités territoriales des recommandations formulées dans ce présent guide.

Il est de la responsabilité des collectivités territoriales de rédiger et de mettre à jour leurs documents contractuels avec l'appui d'un conseil juridique.

SOMMAIRE

Rappel des enjeux

Les collectivités territoriales font face aujourd'hui à une multitude d'enjeux (logement, énergie, TEE, mobilité, transition numérique, …). Le sujet de la donnée, et plus particulièrement celui de la donnée territoriale, a pour caractéristique d'être commun et transverse à tous ces enjeux. **Toutes les compétences exercées par les collectivités sont en effet concernées** par le sujet des données : de l'éclairage public à l'arrosage automatique, des services scolaires à l'eau potable, de la vidéoprotection au transport, etc… Ainsi, de **nombreuses données sont produites aujourd'hui sur les territoires**. Ces données sont **générées par une multitude d'acteurs** :

- Les collectivités : par leurs outils métiers et, pour certaines, via un réseau IoT. Sur un même territoire, plusieurs collectivités et EPCI produisent des données (communes, groupements de communes, département et région),
- Les autres acteurs publics : les services déconcentrés et agences de l'Etat, les services départementaux d'incendie et de secours, les services de police et gendarmerie,
- Les acteurs privés : entreprises exerçant sur le territoire (qu'elles soient titulaires de contrats publics ou non), des entreprises collectant des données sur le territoire (GAFAM, Waze…), des associations…
- Les citoyens : informations transmises aux différentes administrations (services scolaires, état civil…), relevés GPS…

Le pouvoir d'action sur le territoire passe par une meilleure maîtrise des données : **leur maitrise devient un enjeu essentiel pour le pilotage des politiques publiques**.
Quelle collectivité peut prétendre définir sa stratégie d'équipements publics, piloter un service public, mettre en place un contrat de délégation de service public ou mettre à jour son PLU sans avoir la maîtrise la plus large possible des données générées sur son territoire à un niveau équivalent à ce que détiennent les acteurs privés opérant sur son territoire ?
Les données constituent ainsi un levier d'action pour les politiques publiques locales : dans la visualisation, le diagnostic, l'aide à la décision, et même le service aux citoyens…

Un autre aspect de ce sujet concerne les obligations de conformité (loi pour une République Numérique, RGPD, …), auxquelles sont soumises les collectivités.
Comme on le voit, les données sont un enjeu majeur pour les collectivités territoriales.

Ainsi, il semble nécessaire que chaque collectivité s'empare de la question en mettant par exemple en place une réflexion stratégique, suivie d'actions concrètes. Ceci reste encore souvent l'apanage des « grandes » villes mais de plus en plus de collectivités souhaitent mettre en place des solutions.

Plusieurs initiatives ont d'ores-et-déjà été mises en place : des collectivités/EPCI ont lancé des marchés de solutions intégrées qui couvrent plusieurs verticales métiers et qui embarquent une dimension « gouvernance de la donnée ».

Différents choix de positionnement s'offrent aux collectivités :

- Inclusion du sujet des données dans le contrat global dans les cas de projets dits « intégrés »,
- Mise en œuvre d'un contrat de plateforme de données territoriales (région Ile-de-France),
- Choix d'une plateforme « open-source » pour traiter les problématiques d'open data, de conformité RGPD, de stratégie data et de smart city,
- Etc.

Malgré les évolutions législatives, les collectivités comme beaucoup d'autres organisations, peinent à s'approprier le sujet dans toutes ses dimensions : souveraineté, sécurité, données personnelles, sobriété…
Le présent document propose ainsi, sur la base du cadre légal et réglementaire actuel, des recommandations et bonnes pratiques contractuelles sous la forme de clauses-types permettant d'aiguiller la collectivité dans la rédaction de ses contrats sur les sujets liés à la souveraineté des données, la protection des données, la transparence des données et des algorithmes, ainsi que les droits de propriété en lien avec les innovations technologiques.
Il convient de le considérer comme une sorte de boîte à outils pour aider les collectivités.

Si l'application de telles clauses semble évidente pour des contrats de solutions innovantes, on notera que, des données étant produites sur toutes les verticales métiers, l'essentiel des contrats signés par les collectivités est concerné, qu'il s'agisse d'un Marché public, d'une délégation de service public, d'une convention…

Il est à noter que pour chaque « clause type » proposée, le document distingue :

- Si la clause reprend les dispositions d'une loi ou d'un règlement,
- Si la clause vient préciser des dispositions légales ou réglementaires, ces dernières étant considérées trop larges ou floues,
- Si les dispositions de la clause vont au-delà de la loi ou du règlement et relèvent de la seule liberté contractuelle.

Nous espérons que cette série d'éléments viendra utilement aider les acteurs publics territoriaux dans leurs réflexions et leurs travaux de mise en place de solutions de gouvernance de la donnée territoriale.

Avertissement et encadré méthodologique

Si le législateur est venu fixer un certain nombre de principes relatifs aux données publiques, force est de constater qu'ils ne se suffisent pas par eux-mêmes et qu'ils doivent faire l'objet d'adaptations.

A cet égard, ces dernières années certains acteurs tels que l'association Opendata France, la CNIL ou encore l'ANSSI sont intervenus pour proposer des « clauses types » au sein des contrats, et plus particulièrement des cahiers de clauses administratives générales, ou des clauses relatives à la protection des données à caractère personnel, ou de sécurité des systèmes d'informations.

Pour l'heure, il n'existe pas de clausier type s'agissant des différents enjeux auxquels sont confrontés les collectivités dans la gestion de leurs données publiques.

Il est néanmoins important d'avoir à l'esprit que le clausier proposé au titre du présent guide sera nécessairement à adapter par les collectivités le moment venu en fonction des attentes locales, de besoins spécifiques, mais aussi des projets qui créeront des situations nouvelles qu'un clausier ne peut anticiper.

Les clauses proposées dans ce guide ne constitueront pas, à elles seules, un contrat et ne se suffiront pas à elles-mêmes pour mettre en place une gouvernance de la donnée dans les territoires.

Etant précisé que les clauses identifiées avec :

- * : découlent directement du domaine de la loi et du règlement ;
- ** : viennent préciser un principe fixé par la loi ;
- *** : prennent des partis pris en faveur d'une meilleure maîtrise des données qui, s'ils ne sont pas nécessairement prévus par la loi, pourront constituer une prochaine étape pour le législateur.

01

Garantir la souveraineté de la collectivité sur ses données

1.1 Définir le statut des Données publiques

Proposition de clause type **

« Les données produites, collectées, traitées ou gérées par la collectivité ou par le Concessionnaire/Titulaire pour son compte dans le cadre de ses activités de service public et en lien avec ses compétences, ont le statut de « données publiques » au sens du code des relations entre le public et l'administration. »

Commentaire juridique

Aux termes de la circulaire modifiée du 26 mai 2011 relative à la création du portail unique des informations publiques de l'Etat « data.gouv.fr » par la mission « Etalab » et l'application des dispositions régissant le droit de réutilisation des informations publiques, les informations publiques ou données publiques correspondent aux informations contenues dans les documents produits ou reçus dans le cadre de la mission de service public des administrations de l'Etat, des collectivités territoriales et des personnes publiques ou privées chargées d'une mission de service public.

En outre, l'article L. 300-2 du code des relations entre le public et l'administration définit la notion de document administratif les données publiques de la manière suivante :

> *« Sont considérés comme documents administratifs, au sens des titres Ier, III et IV du présent livre, quels que soient leur date, leur lieu de conservation, leur forme et leur support, les documents produits ou reçus, dans le cadre de leur mission de service public, par l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission. Constituent de tels documents notamment les dossiers, rapports, études, comptes rendus, procès-verbaux, statistiques, instructions, circulaires, notes et réponses ministérielles, correspondances, avis, prévisions, codes sources et décisions. »*

Aux termes de ces deux textes, il est expressément indiqué que les données de l'ensemble des services publics des administrations en ce compris ceux qui seraient exploités par des opérateurs privés constituent des documents administratifs, des informations publiques ou des données publiques.

Ainsi, et contrairement à ce qui a pu être soutenu par certains opérateurs privés, il ne fait pas de doute pour le législateur que les données publiques incluent les données de l'ensemble des services publics en ceux compris ceux qui seraient exploités par des opérateurs privés. Dès lors, les données des contrats de Concession ou des Marchés publics sont bien des données publiques dans la mesure où elles ont été produites dans le cadre d'une mission de service public.

Bien que ce principe n'ait pas encore été acté au sein de tous les contrats des collectivités, une majorité de métropoles, à l'instar des métropoles de Dijon, de Nantes ou encore de Lyon ont mis en place des clauses s'inspirant du modèle ci-dessus présenté.

1.2 Garantir la Propriété des données

Proposition de clause type***

Pour les Concessions

« Les données produites, collectées, traitées ou gérées par l'Autorité concédante ou par le Concessionnaire pour son compte dans le cadre de ses activités de service public et en lien avec ses compétences en ce qu'elles sont nécessaires au fonctionnement du service public constituent des biens de retour et sont réputées appartenir à l'Autorité concédante dès l'origine.

Le Concessionnaire s'engage à permettre à l'Autorité concédante d'accéder librement à ces données à tout moment de l'exécution du contrat.

A l'issue de la Concession, le Concessionnaire s'engage à remettre gratuitement à l'Autorité concédante toutes les données visées au premier alinéa du présent article et à apporter la preuve de leur destruction. »

Pour les Marchés publics

« Les données produites, collectées, traitées ou gérées par l'Acheteur public ou par le Titulaire pour son compte dans le cadre de ses activités de service public et en lien avec ses compétences en ce qu'elles sont nécessaires au fonctionnement du service public sont réputées appartenir à l'Acheteur public dès l'origine.

Le Titulaire s'engage à permettre à l'Acheteur public d'accéder librement à ces données à tout moment de l'exécution du Marché public.

A l'issue du Marché public, le Titulaire s'engage à remettre gratuitement à l'Acheteur public toutes les données visées au premier alinéa du présent article et à apporter la preuve de leur destruction.

Commentaire juridique

Les textes susvisés définissant la catégorie des documents administratifs/informations publiques/données publiques, ne précisent pas le régime de propriété des données lorsqu'elles sont gérées par les prestataires de l'administration chargés de l'exploitation d'un service public.

Aussi, afin de rendre juridiquement plus robuste le régime de propriété des données au sein d'un contrat de Concession, il est recommandé non seulement de qualifier lesdites données de données publiques comme exposé ci-avant mais également de s'inspirer de la théorie des biens de retour applicable en matière de Concession de service public.

Cette théorie trouve son origine dans les principes régissant les Concessions de service public lesquelles ont globalement pour objet de confier la gestion d'un service public à un opérateur sans que la collectivité ne s'en dessaisisse pour autant.

En application de cette théorie, les biens de retours sont considérés comme les « *biens nécessaires au fonctionnement du service public* » réputés appartenir à la personne publique dès leur réalisation ou leur acquisition.

Toujours selon cette théorie, au terme du contrat, les biens de retour reviennent gratuitement à l'Autorité concédante.

Cette théorie a été transposée par nos soins aux données dans plusieurs contrats de collectivités et notamment des contrats de smart city tels que ceux de Dijon métropole, de la Communauté de commune du Pays Haut Val d'Alzette ou encore de la métropole d'Angers.

Pour les Marchés publics, il est recommandé d'indiquer expressément dans les contrats que **l'ensemble des données collectées** par des opérateurs privés en charge d'un service public constituent des **« biens nécessaires au fonctionnement du service public » réputés appartenir à la personne publique dès leur collecte.**

En outre, il pourrait être également précisé que la collectivité dispose d'un droit d'accès auxdites données tout au long de l'exécution du contrat et qu'au terme de ce dernier, lesdites données reviennent gratuitement à la personne publique et doivent être détruites par l'exploitant.

1.3 Définir les données d'intérêt général

Proposition de clause type***

Il n'existe pas de clause type sur le sujet, voici à titre d'exemple la clause de la charte de la donnée métropolitaine de Nantes :

> *Principe 4 – Données d'intérêt métropolitain*
>
> *Des acteurs divers interviennent dans la vie du territoire métropolitain et sont susceptibles de produire des données qui revêtent un caractère d'intérêt général.*
>
> *Certaines sont produites par des acteurs publics (services de l'Etat, collectivités territoriales, entreprises publiques ou Concessionnaires de l'Etat…). D'autres sont produites par des acteurs privés.*
>
> *Lorsqu'il est de l'intérêt de tous qu'elles soient partagées avec la puissance publique parce qu'elles peuvent contribuer à la mise en œuvre des politiques publiques du territoire, la collectivité propose un cadre de dialogue avec les acteurs concernés pour créer les conditions d'un accès à ces données respectueux des droits de tous.*
>
> *Ces données sont d'intérêt métropolitain.*

Commentaire juridique

Initialement proposée dans le rapport n° 3399 déposé le 15 janvier 2016 par le député Luc Belot, la notion de donnée d'intérêt général était plus large que celle actuellement en vigueur dans la Loi pour une République numérique.

En effet, comme le rappelait le rapporteur du projet de loi, le Député Luc Belot :

> *Nous créons également une nouvelle catégorie juridique, les « données d'intérêt général.*

En effet, certains jeux de données ne sont ni purement publics, au sens où ils seraient produits par des administrations, ni complètement personnels, rattachés à des individus, ni entièrement privés ou commerciaux, même s'ils le sont peut-être au départ. Il est pourtant de l'intérêt de tous que ces jeux de données soient partagés avec la puissance publique, dans la mesure où leur contrôle par les seules entreprises privées qui ont signé des contrats avec l'État – sous forme de convention ou de délégation de service public… – ne permet pas qu'ils soient utilisés de façon optimale. »

Ainsi, à l'origine, la notion de donnée d'intérêt général ne visait pas que les données des contrats de Concession. Elle couvrait l'ensemble des données d'origine publique ou privée pour lesquelles il est de « *l'intérêt de tous qu'elles soient partagées avec la puissance publique* ».

Or, dans la version actuellement en vigueur du texte de la loi pour une république numérique, la notion de données d'intérêt général fait l'objet d'une section dédiée (la section 2 du chapitre 1 « Economie de la donnée »), comprenant 8 articles.

Sur ces huit articles, un seul d'entre eux traite des contrats de l'administration, et plus précisément des seuls contrats de Concession.

Ainsi, l'article 17 de la loi république numérique a modifié l'ordonnance n° 2016-65 du 29 janvier 2016 relative aux contrats de Concession en la complétant par un article 53-1 ainsi rédigé :

> *« Art. 53-1. - Lorsque la gestion d'un service public est déléguée, le concessionnaire fournit à l'Autorité concédante, sous format électronique, dans un standard ouvert librement réutilisable et exploitable par un système de traitement automatisé, les données et les bases de données collectées ou produites à l'occasion de l'exploitation du service public faisant l'objet du contrat et qui sont indispensables à son exécution. L'Autorité concédante ou un tiers désigné par celle-ci peut extraire et exploiter librement tout ou partie de ces données et bases de données, notamment en vue de leur mise à disposition à titre gratuit à des fins de réutilisation à titre gratuit ou onéreux.*
>
> *« La mise à disposition ou la publication des données et bases de données fournies par le concessionnaire se fait dans le respect des articles L. 311-5 à L. 311-7 du code des relations entre le public et l'administration.*
>
> *« L'Autorité concédante peut, dès la conclusion du contrat ou au cours de son exécution, exempter le concessionnaire de tout ou partie des obligations prévues au présent article par une décision motivée fondée sur des motifs d'intérêt général et rendue publique. » ;*

En outre, l'article 78 de l'ordonnance est complété par un alinéa ainsi rédigé :

> *« L'article 53-1 s'applique aux contrats de concession délégant un service public pour lesquels une consultation est engagée ou un avis de concession est envoyé à la publication à compter de la date d'entrée en vigueur de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. Pour les contrats de concession délégant un service public pour lesquels une consultation a été engagée ou un avis de concession a été envoyé à la publication avant la date d'entrée en vigueur de cette même loi, les Autorités concédantes ne peuvent exiger du concessionnaire la transmission des données et des bases de données qu'à la seule fin de préparer le renouvellement du contrat. »*

Certaines collectivités ont décidé de revenir à cet esprit initial. À l'instar de Nantes métropole qui au principe n°4 de sa Charte métropolitaine de la donnée a créé la notion de « données d'intérêt métropolitain » afin de pouvoir accéder aux données utiles au territoire, et notamment aux données des nouveaux acteurs de la ville (waze, uber, etc.).

En se réappropriant la notion de données d'intérêt général Nantes métropole a ainsi institué un cadre de dialogue innovant pour engager des discussions avec les acteurs concernés.

Etant précisé que le principe de données d'intérêt général devra être décliné le moment venu dans les contrats de la métropole ce que cette dernière est en train de mettre en œuvre.

En tout état de cause, pour l'heure et à notre connaissance, il n'existe pas à ce jour de contrat déclinant ce nouveau concept de données d'intérêt général ou d'intérêt « territorial » en dehors de la charte métropolitaine de la donnée précitée.

1.4 Contrôler l'hébergement et les conditions de stockage des données publiques

Proposition de clause type

Face aux enjeux de sécurité et de souveraineté des données liées à l'objet du Marché public / de la Concession, l'Acheteur public/l'Autorité concédante fixe les règles d'hébergement de ses données.

Afin de garantir la sécurité des données à caractère personnel, l'Acheteur public/l'Autorité concédante impose :

- *Option n°1* : leur hébergement dans l'Union Européenne [solution conforme au RGPD et au nouveau règlement sur la libre circulation des données non personnelles adopté le 21 juin 2018] ;*
- *Option n°2** : leur hébergement sur le territoire français [option susceptible de porter atteinte au principe de libre concurrence] ;*
- *Option n°3*** : leur hébergement dans le data center local de proximité XX [acceptable si des solutions de stockage sont offertes à tous les opérateurs sans distinction et donc sans distorsion de concurrence].*

Commentaire juridique

Le fait d'imposer des règles strictes imposant le stockage des données en France répond aux enjeux de souveraineté mais soulève deux difficultés juridiques.

La question de sa compatibilité avec le règlement sur la libre circulation des données non personnelles adopté le 21 juin 2018 par le Parlement européen se pose dans la mesure où ce dernier est entré en vigueur le 21 décembre 2018 et qu'il est d'effet direct dans les Etats membres.

Ce règlement fait suite à un accord politique conclu en juin 2018 sur un nouveau principe qui supprime les exigences en matière de localisation des données tout en garantissant que les autorités compétentes puissent accéder aux données à des fins de contrôle réglementaire.

Toutefois, des exceptions permettront de maintenir une localisation des données sur le territoire national. Ce sera notamment le cas pour des raisons de sécurité nationale ou s'il s'agit de données « mixtes » à caractère personnel et non personnel.

Par ailleurs, ces principes pourront être contestés au regard du **droit de la concurrence**.

En effet imposer des règles strictes liées au stockage des données en France, voire sur le territoire métropolitain, peut être de nature à constituer une barrière à l'entrée pour certains opérateurs.

Il conviendra donc d'utiliser ces critères de façon habile dans la commande publique.

Le choix d'outils utilisant un stockage de type cloud ou local est légitime pour nombre d'applications.

Imposer un stockage local peut être acceptable si des solutions de stockage sont offertes à tous les opérateurs sans distinction et donc sans distorsion de concurrence (ex : mise à disposition d'un espace de stockage dans un data center de proximité).

Tel est le cas en Bretagne ou des data centers locaux de proximité ont été implantés ou sont en cours d'implantation. Cela permet ainsi à certaines collectivités bretonnes de proposer des solutions de stockage local des données du contrat et ce sans distorsion de concurrence.

En outre, de plus en plus d'opérateurs intègrent aujourd'hui le stockage en France comme une option (parfois payante).

02

Protéger les données

2.1 Protéger les données à caractère personnel

Proposition de clause type**

1. Gestion des données à caractère personnel

Dès lors que l'Acheteur public/l'Autorité Concédante détermine les finalités et les moyens de mise en œuvre de traitement des données du service et notamment des données à caractère personnel des usagers dudit service, il sera considéré comme responsable du traitement correspondant et assumera à ce titre l'ensemble des obligations prescrites par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après « loi Informatique et Libertés ») telle que modifiée par 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 (ci-après « RGPD »).

Dans l'hypothèse où l'Acheteur public/l'Autorité Concédante est considéré comme responsable du traitement, il reviendra au Titulaire/Concessionnaire, en qualité de sous-traitant, d'assurer la confidentialité et la sécurité des données du service pour la couverture des risques résiduels.

Les deux premiers alinéas du présent article n'ont ni pour objet, ni pour effet de conférer au Titulaire/Concessionnaire un quelconque droit de propriété sur lesdites données à caractère personnel

Le Titulaire/Concessionnaire s'interdit, à l'expiration du présent Contrat de conserver les données visées au présent article. Le Titulaire/Concessionnaire devra apporter la preuve de leur destruction à l'Acheteur public/l'Autorité Concédante.

La répartition précise des responsabilités entre le responsable de traitement et le sous-traitant est indiquée en annexe X du présent Contrat.

2. Protection des données à caractère personnel

Chaque partie est tenue au respect des règles relatives à la protection des données à caractère personnel, auxquelles elle a accès pour les besoins de l'exécution du Marché/de la Concession notamment les dispositions de la loi modifiée n°78-17 du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés.

Le Titulaire/Concessionnaire prend toute mesure nécessaire pour préserver et faire respecter l'intégrité et la confidentialité des données à caractère personnel. Le Titulaire/Concessionnaire s'engage notamment à mettre en place les mesures techniques et organisationnelles permettant d'assurer, compte tenu de l'état des règles de l'art, un niveau de sécurité et de confidentialité approprié au regard des risques présentés par le traitement et la nature des données à caractère personnel traitées pour le compte de l'Acheteur public/l'Autorité concédante.

En cas d'évolution de la législation sur la protection des données à caractère personnel en cours d'exécution du Marché/de la Concession, les modifications éventuelles demandées par l'Acheteur public/l'Autorité concédante, afin de se conformer aux règles nouvelles, donnent lieu à un accord préalable des parties.

La répartition précise des responsabilités entre le responsable de traitement et le sous-traitant est indiquée en annexe X du présent Contrat.

Commentaire juridique

Pour rappel, la notion de responsable de traitement désigne aux termes de l'article 3 de la Loi Informatique et Libertés : « *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* ».

Or, c'est bien la collectivité qui détermine les finalités et les moyens des données de ses propres services publics et a fortiori des données à caractère personnel, c'est-à-dire :

- pour la CNIL « l'objectif et la façon de le réaliser »[1] ;
- ou encore pour la commission européenne il s'agit de déterminer « «pourquoi» et «comment» les données à caractère personnel devraient être traitées »[2] ;
- ou enfin pour le Conseil d'Etat constitue un « faisceau d'indice » le fait pour l'organisme de décider de la nature des données collectées, de déterminer les droits d'accès, la durée de la conservation et d'apporter des correctifs au traitement[3].

Ainsi, force est de constater que ce n'est pas parce que la collectivité a confié via une Concession ou un Marché public le traitement des données à caractère personnel des usagers de ses propres services publics qu'elle n'est plus responsable de traitement.

Ceci s'inscrit d'ailleurs dans la logique de la CNIL qui elle-même a reconnu dans son guide de sensibilisation du RGPD à destination des collectivités que ces dernières étaient responsables du traitement des données à caractère personnel collectées dans le cadre des services publics dont elle**s** ont la gestion sans instituer d'autres critères d'appréciation[4]

Ceci étant rappelé, s'agissant de l'utilisation de cette clause, il convient de relever deux éléments :

- d'une part, elle permet aux collectivités de conserver la responsabilité du traitement pour deux raisons :
  - dès lors que la qualité de responsable ou co-responsable de traitement sera reconnue au profit du Titulaire ou du Concessionnaire, il existera un risque juridique à ce que ces derniers se considèrent, au terme d'une lecture, certes extensive, comme seul propriétaire voire co-propriétaire(s) des données à caractère personnel en question.

  - dès lors que la qualité de responsable ou de co-responsable de traitement est reconnue à un Concessionnaire ou au Titulaire d'un Marché, il est arrivé que ces derniers refusent de transmettre à la collectivité lesdites données à caractère personnel au terme normal du contrat. S'estimant être les seuls responsables du traitement de ces données au sens de la Loi informatique et libertés modifiée, certains opérateurs en sont même venus à conserver ces données après le terme normal du contrat ce qui n'a pas été sans susciter des difficultés majeures lors de la procédure de renouvellement dudit contrat…

[1] https://www.cnil.fr/fr/definition/responsable-de-traitement
[2] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_fr
[3] Conseil d'Etat, 12 mars 2014, n°354629.
[4] https://www.cnil.fr/sites/default/files/atoms/files/cnil-guide-collectivite-territoriale.pdf : voir page 40

- d'autre part, il est recommandé pour une meilleure lisibilité du contrat de créer une annexe au contrat, inspirée directement des clauses types proposées par la CNIL, et d'y renvoyer par la mention suivante : « La répartition précise des responsabilités entre le responsable de traitement et le sous-traitant est indiquée en annexe X du présent CCAP/Concession. »

A cet égard, ladite annexe devra reprendre les mentions suivantes :

- Description des traitements de données mis en place, de leurs finalités et des données à caractère personnel concernée ;
- les mesures prises pour respecter les obligations incombant au sous-traitant au titre de la Loi Informatique et libertés et du RGPD.

  Il s'agit notamment de :

  - l'obligation du sous-traitant de respecter la finalité du traitement déterminé par la collectivité ;
  - le respect des droits reconnus aux personnes dont les données sont collectées. A cet égard, le sous-traitant devra a minima coopérer avec le responsable de traitement pour l'aider à satisfaire aux éventuelles demandes desdites personnes. Alternativement, le sous-traitant peut être chargé de répondre au nom du responsable de traitements aux demandes desdites personnes ;
  - la mise en place de mesures de sécurité appropriées au regard des données collectées et de la finalité du traitement. A cet égard, le RGPD dresse la liste de mesures de sécurité générales toutefois, les mesures particulières mise en place sont listées dans ladite annexe ;
  - la notification sous 72 heures de toute violation de données personnelles constatée par le responsable de traitement. Etant précisé que le format de cette notification est précisé par l'annexe afin de permettre à l'Acheteur public de notifier ladite violation à la CNIL avec toutes les informations utiles ;
  - le respect des restrictions de tout transfert des données hors de l'union européenne conformément au texte précité ;
  - l'encadrement du sort des données la fin du traitement. Le sous-traitant détruit ou restitue les données collectées au responsable de traitement ;
  - la mise en place d'un droit d'audit au bénéfice du responsable de traitement afin de constater le respect par le sous-traitant de ses obligations.

Etant précise qu'il est recommandé d'insérer une obligation générale du sous-traitant à coopérer avec le responsable de traitement pour respecter ses obligations au titre des textes précités.

Ladite annexe est jointe en annexe du présent guide.

A la différence des précédentes clauses relatives au stockage ou encore à la propriété des données, les clauses relatives à la protection des données à caractère personnel ainsi que l'annexe précitées sont d'ores et déjà très répandues dans les territoires.

Etant précisé que la spécificité de la clause proposée ci-dessus est de confier à la collectivité la responsabilité du traitement des données à caractère personnel. Si les raisons justifiant un tel choix ont été exposées ci-avant, nous ne sommes pas sans ignorer que ce choix peut être lourd de conséquences pour les collectivités dans la mesure où il nécessite de disposer de l'organisation adaptée pour pouvoir assurer la responsabilité du traitement.

Néanmoins et comme exposé par la CNIL dans les clauses types précitées, il est tout à fait possible de mettre à la charge du sous-traitant davantage d'obligations dans la mesure où c'est bien ce dernier qui est en prise directe avec la collecte et le traitement des différentes données à caractère personnel du Marché ou de la Concession.

Là encore et dans la mesure ou les nouveaux contrats de smart city ou projets autour des données nécessitent de prendre en compte le sujet de la responsabilité du traitement des données à caractère personnel, les métropoles de Dijon, Angers, Nantes, Lyon ou encore la CARENE ou la CCPHVA n'ont pas hésité à prendre la responsabilité du traitement des données à caractère personnel.

2.2 Garantir la sécurité des systèmes d'information

Proposition de clause type*

Le sujet des clauses de sécurité informatique est vaste et figure en annexe du présent guide de bonnes pratiques.

Cette annexe, directement inspirée du travail réalisé par l'ANSSI et décrit ci-après, comporte les obligations à mettre à la charge du Titulaire d'un Marché public ou du Concessionnaire, à savoir :

- La description de la politique de sécurité mise en place par la collectivité ;
- Les modalités de contrôle et d'audits qui pourront être réalisés par la collectivité ;
- La documentation associée ;
- Les conditions de maintien en condition de sécurité ;
- Les modalités d'hébergement des données ;
- Les conditions de recours à la sous-traitance ;
- Les labels et certificats ;
- Les modalités de règlement des différends ;
- La mise en conformité avec les standards et référentiels.

Commentaire juridique

De nombreuses réflexions sont actuellement en cours en France afin de tenter de parvenir à la rédaction de clauses types sur ce sujet.

A ce jour, et s'agissant des recommandations les plus actuelles, il est recommandé de se référer à l'arrêté en date du 8 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité lequel contient un certain nombre de clauses auquel l'acheteur public ou l'Autorité concédante peut décider de se soumettre volontairement.

Est donc joint en annexe du présent guide, une annexe à intégrer aux contrats de Marchés publics ou de Concession et relative à la sécurité des systèmes d'information.

De nombreuses études ont été lancées en 2020 par différents partenaires institutionnels des territoires sur le sujet de la cybersécurité et plus largement de la sécurité des réseaux des collectivités. Il est donc envisageable que de nouveaux textes de loi ou règlementaire interviennent sur ce sujet.

2.3 S'engager en faveur de la sobriété dans la collecte et la conservation des données

Proposition de clause type* : Sobriété dans la collecte et la conservation des données**

« *La collectivité impose à son Titulaire/Concessionnaire l'application d'un principe de sobriété dans la collecte et la conservation des données. La Collectivité ainsi que le Titulaire/Concessionnaire s'engagent à collecter les seules données nécessaires à l'accomplissement des missions de service public et en limitent le stockage.*

Le Titulaire/Concessionnaire évalue annuellement les impacts de l'application de ce principe de sobriété.

A cet égard, le Titulaire/Concessionnaire présente chaque année un rapport public qui dresse un état des lieux de la mise en œuvre de ce principe.

Ce rapport détaille notamment les modalités de conservation des données et plus particulièrement des données à caractère personnel.

[Etant précisé que la durée de conservation de toutes les données, personnelles ou non, devra être déterminée en fonction de leur nature et de l'objectif poursuivi (à l'exception des données conservées et archivées à des fins de recherche scientifique ou historique).] »

Commentaire juridique

Dans un souci de répondre à de nouvelles préoccupations environnementales liés à un usage de plus important du numérique et de la potentielle prolifération de « big data territorial », certaines collectivités font le choix de recourir à des clauses de « sobriété dans la collecte et la conservation des données ».

C’est pour cette raison que la clause susvisée est proposée.

Elle a pour objectif de répondre à une demande de certains territoires souhaitant s’engager plus fortement dans la réduction des consommations d’énergie et qui anticipent les difficultés que pourraient générer à terme la collecte et le stockage d’un volume important de données.

03

Garantir la transparence

3.1 Mettre en œuvre l'open data des données publiques

Proposition de clause type* : Ouverture des données

L'Acheteur public / Autorité concédante s'est engagé(e) dans une politique pour l'innovation et le développement numérique faisant une place prioritaire à la réutilisation des données publiques conformément au code des relations entre le public et l'administration concernant la réutilisation des informations du secteur public.

Pour cela, l' Acheteur public / Autorité concédante permet aujourd'hui à des tiers de réutiliser librement les données publiques diffusées sur sa plate-forme accessible à l'adresse suivante : [A COMPLETER.]

Sont expressément exclues de cette démarche les données à caractère personnel ainsi que celles sur lesquelles des tiers détiendraient des droits de propriété intellectuelle.

L'Acheteur public / Autorité concédante se réserve la possibilité de publier sous une licence de réutilisation publique, qui précise les droits et les obligations rattachés aux données, les données issues de l'exécution de la présente Convention.

A cette fin, le Délégataire/Titulaire met à disposition gratuitement sous format ouvert (c'est-à-dire, tout protocole de communication, d'interconnexion ou d'échange et tout format de données interopérable et dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre) toutes les données non couvertes par des droits de propriété intellectuelle et relative à l'exécution de la Convention.

A défaut, en vue de la mise à disposition à titre gratuit des informations publiques, le Délégataire fournira les outils permettant d'extraire et d'exploiter librement tout ou partie des données et bases de données.

Le Délégataire/Titulaire apporte une attention particulière à documenter les opérations d'accès. Il accorde également les autorisations afin que les services de l'Acheteur public / Autorité concédante puissent exploiter les données à la fréquence de leur production.

Le Délégataire/Titulaire précise dans la description des données mises à disposition, le contenu des évolutions et corrections et le rythme de production des mises à jour.

Le Délégataire/Titulaire doit assurer une ressource support pour répondre aux questions des réutilisateurs de données, que l'espace d'échanges soit mis en place par l'Acheteur public / l'Autorité concédante ou le Délégataire/Titulaire.

Commentaire juridique

S'agissant des conditions d'accès aux documents administratifs, il est prévu, aux termes de l'article L311-1 que :

> *« les administrations mentionnées à l'article L. 300-2 [c'est-à-dire l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission] sont tenues de publier en ligne ou de communiquer les documents administratifs qu'elles détiennent aux personnes qui en font la demande, dans les conditions prévues par le présent livre. »*

S'agissant des conditions de réutilisation, il est prévu, aux termes de l'article L. 321-1 du code des relations entre le public et l'administration :

> *« Les informations publiques figurant dans des documents communiqués ou publiés par les administrations mentionnées au premier alinéa de l'article L. 300-2 peuvent être utilisées par toute personne qui le souhaite à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus.*
>
> *Les limites et conditions de cette réutilisation sont régies par le présent titre ».*

En outre, aux termes de l'article L. 324-1 du code des relations entre le public et l'administration :

> *« La réutilisation d'informations publiques est gratuite. »*

Les données mises à la disposition du public excluent les données protégées par la Loi (données personnelles, données d'entreprises relevant du secret industriel ou commercial, données couvertes par des droits d'auteur).

Il convient de rappeler que par décret n° 2018-1117 du 10 décembre 2018 relatif aux catégories de documents administratifs pouvant être rendus publics sans faire l'objet d'un processus d'anonymisation, le gouvernement est venu lister des catégories de documents pouvant être publiés sans faire l'objet d'une anonymisation préalable.

Le décret incorporé à l'article D. 312-1-3 du code des relations entre le public et l'administration précise notamment, pour les documents administratifs communicables ou accessibles à toute personne, les catégories de documents pouvant être rendus publics par les administrations sans faire l'objet d'un traitement rendant impossible l'identification des personnes.

Aux termes des dispositions de l'article D. 312-1-3 du code des relations entre le public et l'administration précité, il s'agit des catégories suivantes :

> « *1° Les documents nécessaires à l'information du public relatifs aux conditions d'organisation de l'administration, notamment les organigrammes, les annuaires des administrations et la liste des personnes inscrites à un tableau d'avancement ou sur une liste d'aptitude pour l'accès à un échelon, un grade ou un corps ou cadre d'emplois de la fonction publique ;*
>
> *2° Les documents nécessaires à l'information du public relatifs aux conditions d'organisation de la vie économique, associative et culturelle, notamment le répertoire national des associations et le répertoire des entreprises et de leurs établissements ;*

3° Les documents nécessaires à l'information du public relatifs aux conditions d'organisation et d'exercice des professions réglementées et des activités professionnelles soumises à la règlementation, notamment celles relatives à l'exercice des professions de notaire, avocat, huissier de justice et architecte ;

4° Les documents nécessaires à l'information du public relatifs à l'enseignement et la recherche et notamment les résultats obtenus par les candidats aux examens et concours administratifs ou conduisant à la délivrance des diplômes nationaux ;

5° Les documents nécessaires à l'information du public relatifs aux conditions d'organisation et d'exercice des activités sportives ;

6° Les documents nécessaires à l'information du public relatifs aux conditions d'organisation et d'exercice de la vie politique, notamment le répertoire des élus, à l'exception des informations prévues au 2° du I de l'article 5 du décret n° 2014-1479 du 9 décembre 2014 relatif à la mise en œuvre de deux traitements automatisés de données à caractère personnel dénommés "Application élection" et "Répertoire national des élus" ;

7° Les documents nécessaires à l'information du public relatifs aux conditions d'organisation et d'exercice des activités touristiques ;

8° Les documents nécessaires à l'information du public relatifs aux activités soumises à des formalités prévues par des dispositions législatives ou réglementaires notamment, en matière d'urbanisme, d'occupation du domaine public et de protection des données à caractère personnel ;

9° Les documents administratifs conservés par les services publics d'archives et les autres organismes chargés d'une mission de service public d'archivage :

a) lorsqu'ils sont librement communicables en application des articles L. 213-1 et L. 213-2 du code du patrimoine, sauf lorsqu'ils comportent des données mentionnées au I de l'article 8 de la loi n° 78-17 du 6 janvier 1978 ou des données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes au sens de l'article 9 de la même loi ;

b) lorsqu'ils comportent des données mentionnées au I de l'article 8 de la loi n° 78-17 du 6 janvier 1978 ou des données à caractère personnel relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes au sens de l'article 9 de la même loi, à l'expiration d'un délai de 100 ans calculé à compter de la date des documents, sauf si le délai de communicabilité fixé par le code du patrimoine est plus long. Dans ce cas, c'est ce dernier délai qui s'applique ;

c) lorsqu'ils sont librement communicables en application des articles L. 213-1 et L. 213-2 du code du patrimoine, les instruments de recherche décrivant les fonds d'archives, sauf s'ils comportent des données à caractère personnel relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes au sens de l'article 9 de la loi du 6 janvier 1978 précitée. Dans ce cas, ils peuvent être publiés à l'issue d'un délai de 100 ans à compter de la date des documents décrits par l'instrument de recherche.

Les archives publiques et les instruments de recherche qui les décrivent peuvent être publiés avant l'expiration des délais ci-dessus sur autorisation de la Commission nationale de l'informatique et des libertés. »

Ce décret est pris pour l'application de l'article L. 312-1-2 du code des relations entre le public et l'administration, dans sa version résultant de l'article 6 de la loi pour une République numérique. Ce texte est entré en vigueur le lendemain de sa publication.

La collectivité privilégie l'utilisation d'une licence d'utilisation des données qui permet l'usage le plus large des données ouvertes. La collectivité se réserve néanmoins le droit d'appliquer des restrictions pour protéger l'intérêt général et limiter des utilisations de données qui iraient à l'encontre des politiques publiques du territoire.

Plus précisément, il sera rappelé qu'afin d'éviter la prolifération des licences, la loi pour une République numérique précitée a prévu la création d'une liste, fixée par décret (et incorporée à l'article D.323-2-1 du code des relations entre le public et l'administration (CRPA)), de licences qui peuvent être utilisées par les administrations pour la réutilisation à titre gratuit de leurs informations publiques.

Deux types de licences peuvent être utilisées par les administrations, les licences prévues à l'article précité D.323-2-1 du code des relations entre le public et l'administration (CRPA) **(i)** et celles qui n'y sont pas prévues et qui devront faire l'objet d'une homologation **(ii)**.

(i) Deux licences sont prévues à l'article D.323-1 du CRPA :

- la licence ouverte d'Etalab, dite licence « libre » ou licence « française » qui permet la réutilisation la plus large des données publiques ;
- La licence « Open DataBase License (ODBL) » qui fixe des critères de réutilisation plus restrictifs.

(ii) Les administrations souhaitant recourir à une licence ne figurant pas dans le paragraphe précédent doivent auparavant en obtenir l'homologation dans les conditions prévues à l'article D.323-2-2 du CRPA.

Pour être prononcée, une homologation doit suivre une procédure particulière. L'administration (services de l'État, collectivité, établissement public…) doit pour cela contacter la mission Etalab (homologation.licence@data.gouv.fr).

La demande d'homologation doit comporter :

1. La description des informations publiques (données, logiciel…) dont la réutilisation doit être spécialement encadrée,
2. Les raisons motivées de cette volonté d'encadrement spécifique,
3. Les explications montrant l'inadéquation des licences proposées,
4. Le texte de la licence souhaitée,
5. La synthèse de la concertation menée auprès des réutilisateurs.

Une fois homologuée, la licence s'applique aux seules informations publiques (données, logiciels…) concernées par la demande originale.

La liste ci-dessous présente les licences homologuées, le périmètre et la durée de l'homologation :

- La « licence d'utilisation à titre gratuit » de l'institut national géographique et forestier (IGN) ;
- La licence du produit gratuit issu de la Base Adresse Nationale (BAN) ;
- La licence « Creative Commons Attribution - Partage dans les mêmes conditions (CC-BY-SA) 4.0 » ;
- La licence de réutilisation des informations de l'institut National de la Propriété Industrielle (INPI) ;
- La licence de réutilisation des informations de l'institut National de la Propriété Industrielle (INPI).

Si le principe d'une clause relative à l'open data ne figure pas toujours dans les contrats des collectivités, force est de constater qu'à ce jour de nombreuses collectivités et la quasi-totalité des métropoles disposent d'une plateforme d'open data.

Cette clause a pu là encore, figurer dans des contrats de collectivités pionnières, c'est-à-dire qui s'étaient spontanément soumises à des obligations d'open data avant la loi pour une république numérique (tel était le cas de Nantes, Rennes et Lyon, notamment), afin que les données soient mises en ligne dans le cadre de l'exécution du contrat.

3.2 Développer l'open data des algorithmes

Proposition de clause type* : Ouverture des algorithmes

« Pour mettre en œuvre ses missions de service public, la collectivité utilise des traitements automatisés de données relatifs à [à compléter] que le Titulaire/le Délégataire met en œuvre pour le compte de la collectivité.

La Collectivité s'engage à publier les règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement des missions de service public.

*Le responsable du traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, **en détail et sous une forme intelligible**, à la personne concernée, la manière dont le traitement a été mis en œuvre à son égard.*

Option : modèle d'information sur l'utilisation d'un traitement algorithmique devant être obligatoirement mentionnée dans la décision elle-même et selon le modèle fourni par Etalab :

La présente décision a été prise sur le fondement d'un traitement algorithmique. Ce traitement permet de [mentionner la finalité, ex : calculer le montant de l'impôt dû] et dont les règles sont définies ici [Lien vers les règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement des missions de l'administration lorsqu'ils fondent des décisions individuelles cf. art. L. 312-1-3 du CRPA].

En application de l'article R. 311-3-1-1 et R. 311-3-1-2 du code des relations entre le public et l'administration, vous pouvez demander la communication des règles définissant ce traitement et leur mise en œuvre dans votre cas auprès de [Nom de l'administration, modalités de contact]*. En cas d'absence de réponse dans un délai d'un mois à la suite de la réception de votre demande par nos services, vous disposez d'un délai de deux mois pour saisir la Commission d'accès aux documents administratifs (CADA) selon les modalités décrites sur le site web www.cada.fr. »*

Commentaire juridique

La transparence algorithmique a été introduite dans le Code des relations entre le public et l'administration (CRPA) part la loi du 7 octobre 2016 pour une République numérique.

L'article L. 311-3-1 oblige toute administration (et par conséquent tout partenaire de l'administration[5]) ayant recours à un procédé algorithmique pour des décisions individuelles à en faire explicitement mention.

En outre, si une personne intéressée en fait la demande, l'administration est tenue de lui communiquer « *les règles de mise en œuvre définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre* ».

L'article L. 311-3-1-2 précise la nature des éléments qui doivent être communiqués à la demande d'une personne intéressée :

> *« sous une forme intelligible et sous réserve de ne pas porter atteinte à des secrets protégés par la loi, les informations suivantes :*
>
> *1° Le degré et le mode de contribution du traitement algorithmique à la prise de décision ;*
>
> *2° Les données traitées et leurs sources ;*
>
> *3° Les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé ;*
>
> *4° Les opérations effectuées par le traitement. »*

En complément et **y compris en l'absence de demande individuelle**, l'article L. 312-1-3 précise que toutes les administrations concernées par les obligations d'open data (plus de 3500 hab et 50 agents ETP) :

> « *publient en ligne les règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles* »

Point d'attention :

La loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles a introduit dans l'article 10 de la loi Informatique et libertés une obligation supplémentaire concernant les traitements automatisés (c'est à dire sans intervention humaine).

A compter du 1er juillet 2020, tout traitement automatisé devra comporter, à peine de nullité, l'obligation de mention explicite.

Par ailleurs le même article 10 précise que :

[5] Dans l'hypothèse où la thèse précédemment exposée selon laquelle les administrations sont les seules et uniques gestionnaires des données publiques est retenue, par extension, les algorithmes ayant produit lesdites données publiques sont considérés comme des éléments composant les données publiques et soumis aux mêmes principes de transparence.

> « *le responsable du traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer,* ***en détail et sous une forme intelligible****, à la personne concernée, la manière dont le traitement a été mis en œuvre à son égard* ».

Enfin, rappelons que l'article 39 de la loi Informatique et Libertés précisait déjà que :

> « *toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement à caractère personnel en vue d'obtenir (...) 5° les informations permettant de* ***connaître et de contester*** *la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé* ».

En s’inscrivant dans le principe général énoncé par l’article L. 312-1-3 et en anticipant d’éventuelles demandes individuelles au titre des articles L. 311-3-1 et 311-3-1-2, une collectivité pourrait faire preuve d’exemplarité en insérant la clause proposée ci-dessus.

Pour l’heure seule la charte nantaise précitée se rapproche, à notre connaissance de la clause ci-dessus.

04

Favoriser des nouveaux usages

4.1 Encadrer les droits de propriété intellectuelle sur les innovations technologiques

Proposition de clause type* : droits de propriété intellectuelle

Option n°1 : la cession de droits à titre exclusif

« *Les Parties reconnaissent que les résultats ont été développés grâce aux efforts et investissements exclusif de l'Acheteur public/ l'Autorité concédante sous l'égide du présent Contrat.*

Dès lors, les Parties conviennent ce qui suit :

- *Le Titulaire / Concessionnaire entend céder à l'Acheteur public/ l'Autorité concédante, à titre exclusif, sur [l'ensemble du territoire français / le monde entier] et pour une durée indéterminée, les droits de propriété intellectuelle sur les Résultats.*
- *Le prix de la cession est inclus dans le prix du Contrat et le Titulaire/Concessionnaire ne peut en aucun cas solliciter de rémunération supplémentaire.* »

Option n°2 : la cession de droits à titre non exclusif

« *Les Parties reconnaissent que les résultats ont été développés grâce aux efforts et investissements conjoints de l'Acheteur public/ l'Autorité concédante et du Titulaire/Concessionnaire sous l'égide du présent Contrat.*

Dès lors, les Parties conviennent ce qui suit :

- *Le Titulaire / Concessionnaire entend céder à l'Acheteur public/ l'Autorité concédante, à titre non exclusif, sur [l'ensemble du territoire français / le monde entier et pour une durée indéterminée, les droits de propriété intellectuelle sur les Résultats.*
- *Réciproquement l'Acheteur public/le Concédant accepte que les Résultats soient exploités librement par le Titulaire/Concessionnaire, en dehors de [l'ensemble du territoire français / le monde entier.*
- *[Option à négocier : En contrepartie de l'investissement humain et financier de l'Acheteur public// l'Autorité concédante dans la recherche et le développement des Résultats, le Titulaire/Concessionnaire s'engage à faire bénéficier l'Acheteur public// l'Autorité concédante, à titre gracieux sous la forme d'une concession non-exclusive à durée indéterminée de tous perfectionnements et améliorations que le Titulaire / Concessionnaire aurait réalisé ou fait réaliser à partir de Résultats.]*
- *Le prix de la cession est inclus dans le prix du Contrat et le Titulaire/Concessionnaire ne peut en aucun cas solliciter de rémunération supplémentaire.* »

Option n°3 : l'octroi d'une licence ou d'un droit d'usage par le Titulaire ou le Concessionnaire à l'Acheteur public / à l'Autorité concédante

Le Titulaire/Concessionnaire consent à faire bénéficier l'Acheteur public/ l'Autorité concédante, d'une licence d'utilisation des droits de propriété intellectuelle dont il est titulaire, cessionnaire ou licencié et sans contrepartie financière, sur les éléments issus de l'exécution du présent Contrat.

Le transfert ainsi consenti sur ces éléments comprend notamment au bénéfice de l'Acheteur public / l'Autorité concédante :

- *Le droit de reproduire, en tout ou partie, sur tout support, en un nombre illimité d'exemplaires par tout procédé de fixation,*
- *Le droit de représenter, par tout procédé de communication au public,*
- *Le droit d'adapter / modifier en vue de permettre l'exploitation des éléments transférés et leur évolution aux besoins de l'exploitation du service.*
  L'Acheteur public / l'Autorité concédante se réserve la possibilité de sous-licencier ou concéder tout ou partie des droits transférés par les titulaires au profit de tout tiers de son choix associé – ou non – à l'exploitation du service public objet du Contrat.

  Cette licence ne vaut que pour les besoins et la durée du présent Contrat.

Commentaire juridique

Le sujet de la répartition des droits de propriété intellectuelle détenus notamment sur les résultats d'un projet co-construit entre une ou plusieurs collectivités et un ou plusieurs opérateurs privés est un sujet crucial dès lors que le projet a pour objectif la mise en place d'une innovation technologique voire une « plateforme smart city ».

Ce sujet de la propriété intellectuelle semble détaché du sujet des données alors qu'il lui est directement lié :

- Déjà parce que, de manière générale, le droit de la propriété intellectuelle ne prévoit pas de protection spécifique sur les données en tant que telles mais surtout sur les bases de données. En d'autres termes, en droit de la propriété intellectuelle, on tend à protéger davantage le contenant (via la protection spécifique octroyée aux bases de données) que le contenu (aucune protection spécifique n'étant directement accordé aux données en tant que telles dans le code de la propriété intellectuelle) ;
- Ensuite parce que, là encore, l'absence de clauses relatives aux droits de propriété intellectuelle pourrait générer des difficultés en cours ou au terme normal ou anticipé du contrat lorsque la collectivité souhaitera récupérer les données qui y sont logées.

Il apparaît donc nécessaire de fixer ces règles de répartition dans une clause dédiée afin de palier tout risque juridique sur ce sujet.

La rédaction de clauses relatives aux droits de propriété intellectuelle nécessitera d'être adaptée selon la nature des projets.

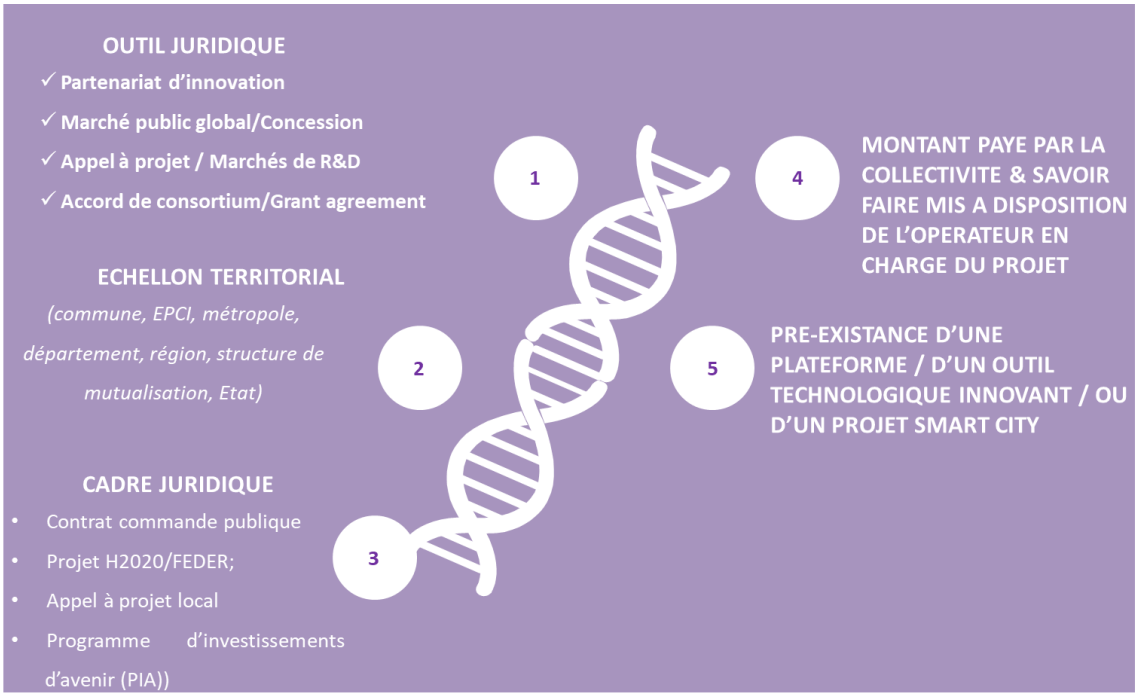
En sus desdites clauses de propriété intellectuelle, des contrats de partage desdits droits de propriété intellectuelle devraient être conclus dans les 6 mois précédant le terme normal du contrat.

Le « rapport de force » entre les parties à la négociation ne sera pas le même selon :

- L'outil juridique utilisé (marché public, appel à projet, accord de consortium…) ;
- L'échelon territorial et les possibilités d'essaimage de l'innovation technologique en question ;
- Le cadre juridique (contrat de la commande publique, FEDER, H2020, PIA, …) ;
- Le montant payé par la collectivité pour la réalisation de ladite innovation technologique mais également le savoir-faire mis à disposition par la collectivité ;
- Ou encore selon qu'il préexiste ou non une plateforme, un outil technologique innovant ou encore un projet de smart city.

Etant précisé qu'il existera également des différences selon les types de contrats : dans un partenariat d'innovation par exemple le sujet de la propriété intellectuelle est un sujet majeur et précisément régi par le code de la commande publique.

Dans la mesure où il existe autant d'exemple de clauses que de cas particuliers en matière de droits de propriété intellectuelle, le schéma ci-dessous représente au regard de nos retours d'expérience les différents types de variables à prendre en compte sur le sujet des droits de propriété intellectuelle :



4.2 Garantir la réversibilité des outils technologiques

Proposition de clause type : Réversibilité des outils technologiques**

« Aux termes du présent Contrat, la réversibilité intervient lorsque la relation contractuelle cesse à son terme normal ou anticipé qu'elle que soit la cause de ce terme.

La réversibilité a pour objectif de permettre à l'Acheteur public/ l'Autorité concédante de récupérer l'ensemble des données et informations contenues dans les solutions développées par le Titulaire / Concessionnaire et ce dans les meilleures conditions et de poursuivre, dans le respect du principe de continuité du service public, les prestations qu'il avait confiées au Titulaire du Marché/Concessionnaire.

Ainsi, en cas de cessation de la relation contractuelle, quelle qu'en soit la cause, le Titulaire/Concessionnaire s'engage à restituer gratuitement, à la première demande de l'Acheteur public formulée par lettre recommandée avec accusé de réception et dans un délai de 48 heures à la date de réception de cette demande, l'ensemble des données visées à l'article de la présente convention sous un format aisément réutilisable dans un environnement équivalent.

Le Titulaire/Concessionnaire s'engage à ce que l'Acheteur public puisse poursuivre l'exploitation des données visées à l'article sans rupture, directement ou avec l'assistance d'un autre prestataire selon des modalités décrites dans un plan de réversibilité (qui décrira la durée et les conditions de mise en œuvre de la réversibilité ou de la transférabilité) qui devra être fourni par le Titulaire/Concessionnaire à l'Acheteur public/l'Autorité concédante. »

Commentaire juridique

Aux termes des dispositions de l'article 31.4. du CCAG TIC :

> « *La « réversibilité » désigne l'opération de retour de responsabilité technique, par lequel l'Acheteur public reprend les prestations qu'il avait confiées au Titulaire du Marché d'infogérance arrivant à terme.*
>
> *La « transférabilité » désigne l'opération de transfert de responsabilité technique, par lequel l'Acheteur public fait reprendre par un nouveau Titulaire les prestations qu'il avait confiées au Titulaire du Marché d'infogérance arrivant à terme.*
>
> *La période de réversibilité ou de transférabilité est la période couvrant le retour ou le transfert de responsabilité technique précédemment définis.*
>
> *Le « plan de réversibilité » ou « de transférabilité » est le document annexé au cahier des clauses administratives particulières qui décrit la durée et les conditions de mise en œuvre de la réversibilité ou de la transférabilité.* »

Si cette clause du CCAG TIC définit précisément le concept de réversibilité, elle reste insuffisante pour pallier les difficultés rencontrées par les collectivités en fin de contrat pour récupérer non seulement des informations sur le logiciel déployé par l'opérateur mais également des données qui y étaient contenues.

De nombreuses expériences passées, notamment sur des plateformes de dématérialisation ont démontré le réel problème de l'absence de clauses de réversibilité et par conséquent l'enjeux que représente une telle clause pour les collectivités.

Cet enjeu est d'autant plus important lorsque la collectivité prévoit de mettre en place « sa propre plateforme smart city ». Il serait regrettable que la collectivité ne soit plus en mesure d'exploiter ladite plateforme en fin de contrat, faute de réversibilité. La CCPHVA en décidant de co-construire une plateforme smart city « sur mesure » pour son territoire a été confrontée à ces enjeux forts de réversibilité. Des clauses renforcées ont été insérées dans le contrat afin que la collectivité puisse librement confier via une nouvelle procédure de mise en concurrence l'exploitation de cette plateforme à un nouveau Titulaire.

De telles clauses ont également vocation à protéger les collectivités dans les contrats qu'elles pourraient être amenées à conclure avec de jeunes entreprises innovantes ou start up dans l'hypothèse où ces dernières viendraient soit à disparaître soit à être rachetée par un tiers.

De telles clauses de réversibilité ont notamment pu être introduites dans le cadre de contrats issus de l'expérimentation relative aux « achats innovants » (tels qu'introduits par le décret n° 2018-1225 du 24 décembre 2018 portant diverses mesures relatives aux contrats de la commande publique), auxquels certaines collectivités ont pu recourir avec des start up ou des PME locales pour le déploiement de projets innovants.

05

Annexes

LEXIQUE

ANSSI

Agence Nationale de Sécurité des Systèmes d'Information

Autorité concédante

Désigne l'entité en charge de confier l'exécution du service public au Concessionnaire.

CGCT

Code général des collectivités territoriales.

Concession

Définis à l'article L.1120-1 du code de la commande publique, les contrats de concession sont regroupés dans un régime commun : les contrats de concession de travaux, les contrats de concession de services, et les contrats de concession de défense ou de sécurité. Etant précisé que les contrats de concession de services se divisent en contrats de concession de service public ou délégation de service public pour les collectivités territoriales et en contrat de concession de services simples.

Concessionnaire

Désigne l'entité en charge de l'exécution de la Concession.

CNIL

Commission Nationale de l'Informatique et des Libertés

CRPA

Code des relations entre le public et l'administration

Loi informatique et libertés

Loi modifiée n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Loi pour une République numérique

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique dite également « Loi Lemaire ».

Loi VALTER

Loi n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public

Marchés publics ou « Marché »

Définis à l'article L.1110-1, la notion de « marché public » recouvre les marchés classiques, les marchés de partenariat et les marchés de défense ou de sécurité.

RGS

Référentiel Général de Sécurité de l'ANSSI

Titulaire

Désigne l'entité en charge de l'exécution du Marché public.

MODELE D'ANNEXE RELATIVE AU DISPOSITIF DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Objet

La présente annexe a pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 entré en vigueur le 25 mai 2018 (ci-après, « ***le règlement européen sur la protection des données*** »).

Description du traitement faisant l'objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) **[A COMPLETER]**

La nature des opérations réalisées sur les données est **[A COMPLETER]** **[*Conseil : mettre la définition la plus exhaustive du traitement*]**

La ou les finalité(s) du traitement sont **[A COMPLETER]** **[*Conseil : à compléter si cela est possible*]**

Les données à caractère personnel traitées sont **[A COMPLETER]**. **[*Conseil : à compléter si cela est possible*]**

Les catégories de personnes concernées sont **[A COMPLETER]**. **[*Conseil : à compléter si cela est possible*]**

Pour l'exécution du service objet du contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes **[A COMPLETER]**. **[*Conseil : à compléter si cela est possible*]**

Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. Traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet de la sous-traitance

2. Traiter les données **conformément aux instructions** du responsable de traitement. Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en **informe immédiatement** le responsable de traitement.

En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis,

il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public

3. Garantir la **confidentialité** des données à caractère personnel traitées dans le cadre du contrat.

4. Veiller à ce que les **personnes autorisées à traiter les données à caractère personnel** en vertu du contrat :

- S'engagent à respecter la **confidentialité** ou soient soumises à une obligation légale appropriée de confidentialité
- Reçoivent la **formation** nécessaire en matière de protection des données à caractère personnel

5. Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de **protection des données dès la conception** et de **protection des données par défaut**

6. Tenir compte de la nature du traitement, aider le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III du règlement européen sur la protection des données ;

7. Aider le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36 du règlement européen sur la protection des données, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;

8. Supprimer toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel ;

9. Mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au règlement européen sur la protection des données et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits ;

Dans ce cadre, le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

10. Sous-traitance

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « **le sous-traitant ultérieur** ») pour mener des activités de traitement spécifiques.

Dans cette hypothèse, le sous-traitant se conforme aux conditions visées aux paragraphes 2 et 4 de l'article 28 du règlement européen sur la protection des données.

Il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le responsable de traitement dispose d'un délai minium de **[A COMPLETER]** à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance

ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations de la présente annexe pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

11. Droit d'information des personnes concernées

Le sous-traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise. La formulation et le format de l'information doit être convenue avec le responsable de traitement avant la collecte de données.

12. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Le sous-traitant doit répondre, au nom et pour le compte du responsable de traitement et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d'exercice de leurs droits, s'agissant des données faisant l'objet de la sous-traitance prévue par la présente annexe.

13. Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 24 heures après en avoir pris connaissance et par le moyen suivant **[A COMPLETER]**. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Après accord du responsable de traitement, le sous-traitant notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

La notification contient au moins :

- La description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- La description des conséquences probables de la violation de données à caractère personnel ;

- La description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

- La description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- La description des conséquences probables de la violation de données à caractère personnel ;
- La description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

14. Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations

Le sous-traitant assiste le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le sous-traitant assiste le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

15. Mesures de sécurité

Généralités

Conformément à l'article 32 du règlement européen sur la protection des données, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 du règlement européen sur la protection des données peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

Mesure de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

[Décrire les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque]

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité prévues par **[Viser le code de conduite édicté].**

[L'article 32 du règlement européen sur la protection des données prévoit que la mise en œuvre des mesures de sécurité incombe au responsable du traitement et au sous-traitant, il est recommandé de déterminer précisément les responsabilités de chacune des parties au regard des mesures à mettre en œuvre] **[Ce partage de responsabilité sera à affiner en fonction des options choisies].**

16. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à :

Au choix des parties :

- Détruire toutes les données à caractère personnel ou
- A renvoyer toutes les données à caractère personnel au responsable de traitement ou
- A renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

17. Délégué à la protection des données

Le sous-traitant communique au responsable de traitement **le nom et les coordonnées de son délégué à la protection des données**, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données

18. Registre des catégories d'activités de traitement

Le sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement comprenant :

- Le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- Les catégories de traitements effectués pour le compte du responsable du traitement ;
- Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :

  - La pseudonymisation et le chiffrement des données à caractère personnel ;
  - Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
  - Des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
  - Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

19. Documentation

Le sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s’engage à :

1. Fournir au sous-traitant les données visées au II de la présente annexe

2. Documenter par écrit toute instruction concernant le traitement des données par le sous-traitant

3. Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant

4. Superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant

MODELE D'ANNEXE RELATIVE A LA SECURITE DES SYSTEMES D'INFORMATION

Article 1 : Champ d'application

La présente annexe a pour vocation d'assurer un premier cadre de sécurisation des systèmes d'information et des données associées du présent Marché.

Article 2 : Politiques de sécurité

Le Titulaire/Concessionnaire est tenu de respecter les prescriptions de la politique de sécurité des systèmes d'information (PSSI) de l'Acheteur public/Autorité concédante.

Article 3 : Contrôles et audits

L'Acheteur public/Autorité concédante peut conduire ou mandater des contrôles et audits de sécurité informatique des fournitures, prestations, moyens utilisés et services proposés par le Titulaire/Concessionnaire, et de ses sous-traitants.

Les contrôles et audits peuvent être réalisés sans accord préalable dès lors que les tests et sondes respectent les conventions techniques d'usage permettant de les identifier.

Article 4 : Documentations

4.1. Dans le cadre de la revue formelle de sécurité de l'Acheteur public/Autorité concédante, le Titulaire/Concessionnaire fournit, à première demande, l'ensemble de la documentation et les réponses nécessaires à l'analyse des risques résiduels en matière de confidentialité, d'authentification, de traçabilité, d'intégrité, de disponibilité et de résilience.

4.2. Le Titulaire/Concessionnaire est responsable de l'identification des traitements de données à caractère personnel ou de données sensibles, et de leurs signalements au Pouvoir adjudicateur/Autorité concédante. Le Titulaire/Concessionnaire s'assure de la conformité desdits traitements au regard des normes juridiques en vigueur, sous réserve des dispositions spéciales du présent Marché.

Le Titulaire/Concessionnaire fournit au Pouvoir adjudicateur/Autorité concédante l'aide nécessaire à la réalisation d'analyses d'impact relatives à la protection des données à caractère personnel, et à la consultation préalable des autorités de contrôle.

4.3. Le Titulaire/Concessionnaire fournit à première demande la documentation nécessaire au Pouvoir adjudicateur/Autorité concédante pour :

- la sécurisation de son système d'information ;
- la protection de ses données ;
- la démonstration du respect de ses obligations issues des normes juridiques en vigueur.

4.4. La documentation fournie par le Titulaire/Concessionnaire permet l'identification de tous les flux échangés (entrants et sortants, applicatif mais aussi de maintenance, de statistiques, de mise à jour, d'administration distante, etc), et des dispositifs de contrôle d'accès et de maintien en condition de sécurité.

4.5. Le Titulaire/Concessionnaire porte à la connaissance de l'Acheteur public/Autorité concédante toutes les actions particulières nécessaires à un emploi sécurisé du produit, fourniture ou service du présent contrat.

Lesdites actions particulières font l'objet d'un avenant au présent contrat.

Article 5 : Maintien en condition de sécurité

5.1. Le Titulaire/Concessionnaire assure les mises à jour des composants logiciels du présent contrat vers des versions supportées par l'éditeur ou communauté Open Source qui les produisent.

Une vérification d'aptitude au bon fonctionnement (VABF) ou au service régulier (VSR) est refusée si des composants ne sont pas à jours des correctifs de failles de sécurité.

5.2. La responsabilité du maintien en condition de sécurité du Titulaire/Concessionnaire comprend les composants et services développés en propre, ainsi que ses composants et dépendances amont (librairies, cadriciels, environnement d'exploitation, API tierces) ou sous-traités.

5.3. Le Titulaire/Concessionnaire ne peut conditionner la garantie du bon fonctionnement des fournitures ou de prestations du présent contrat à l'emploi de composants dans une version non supportée, sauf à démontrer une contrainte supérieure et proposer à ses frais des moyens de cantonner les risques, ou à démontrer que les risques sont négligeables dans le contexte d'emploi.

5.4. Dans le cadre du présent contrat, les unités d'œuvre portant le maintien en condition opérationnelle (MCO), mais aussi tierce maintenance applicative (TMA) ou simplement hébergement, incluent le maintien en condition de sécurité et la mise en œuvre des correctifs de failles de sécurité.

Article 6 : Signalements de sécurité

6.1. Dans le cadre du contrat, le Titulaire/Concessionnaire met à la disposition de l'Acheteur public/Autorité concédante des canaux publics d'information par abonnement (flux RSS, liste de diffusion par courriel) ou tout autre dispositif d'information dédié à la sécurité informatique.

Lesdits canaux assurent l'information continue de l'Acheteur public/Autorité concédante quant aux événements et changements impactant la sécurité (Annonce de correctif, attaque en cours, nouvelle configuration à appliquer, violation de données à caractère personnel, etc)

Ces canaux d'information sont distincts des flux commerciaux et marketing.

6.2. Les outils numériques compris dans l'objet du présent contrat permettent de signaler directement au Titulaire/Concessionnaire les éventuelles failles ou détournements des dispositifs de sécurité.

Les conventions d'usage en cybersécurité sont respectées (security.txt, abuse@) afin d'assurer l'efficacité desdits signalements.

Le Titulaire/Concessionnaire s'assure de la facilité d'accès au point d'entrée du signalement lequel doit être accessible en moins d'une minute.

6.3. Après analyse partagée et vérification, le Titulaire/Concessionnaire se conforme aux obligations d'enregistrements des failles auprès des autorités compétentes en suivant les normes en vigueur.

À défaut d'action sous trois (3) mois, l'Acheteur public/Autorité concédante à la faculté de se substituer au Titulaire/Concessionnaire dans les actions précédentes, ou de pratiquer une divulgation responsable, soit l'annonce de la faille avec embargo pendant au moins quatre-vingt-dix (90) jours sur les détails techniques.

Article 7 : Hébergement de données

À première demande, le Titulaire/Concessionnaire identifie tous les prestataires techniques hébergeant ou stockant les données et leurs copies, utilisées ou échangées au cours du contrat ainsi que leur localisation.

Cette déclaration est exhaustive. Par exception, peuvent être exclus de ladite déclaration les prestataires dépositaires de copies chiffrées sous réserve que l'algorithme soit sans faille connue et que lesdits prestataires ne soient pas en possession des clés cryptographiques.

Article 8 : Sous-traitances

8.1. Les clauses de la présente annexe s'appliquent à tous les sous-traitants du Titulaire/Concessionnaire. Le Titulaire/Concessionnaire est responsable du respect par ses sous-traitants de la présente annexe.

Sont à la charge du Titulaire/Concessionnaire, les contrôles et les éventuelles actions de remédiation en cas de défaut, y compris jusqu'au remplacement du sous-traitant défaillant.

Article 9 : Labels et certificats

9.1. Le Titulaire/Concessionnaire pour attester du niveau de sécurité des composants impliqués dans le présent contrat, peut présenter des labels et certificats au Pouvoir adjudicateur.

À ce titre, peuvent être présentés notamment :

- les qualifications globales de type ISO27000 ou équivalent ;
- les qualifications partielles de type référentiel en Tier 1 à 4 en matière d'hébergement ;
- les qualifications très ponctuelles de type rapports de test de l'état de l'art sur des interfaces spécifiques.

Article 10 : Défauts et règlement des différends

10.1. Le Titulaire/Concessionnaire est soumis à un devoir d'information de l'Acheteur public/Autorité concédante. Le Titulaire/Concessionnaire dès qu'il en a connaissance, transmet au Pouvoir adjudicateur les non-conformités à la politique de sécurité et les défauts de sécurisation constatés.

10.2. L'Acheteur public/Autorité concédante apprécie l'importance du défaut constaté eu égard à la sensibilité des données manipulées, de leurs volumes, et des conséquences prévisibles si le défaut persiste.

L'Acheteur public/Autorité concédante a la faculté de sanctionner lesdits défauts, en fonction de l'importance, par :

- la non-validation d'aptitude au service régulier ;
- l'application de pénalités de retard ;
- l'ajournement, la suspension ;
- la résiliation des bons de commandes.

10.3. Le règlement des éventuelles contestations sur des décisions de l'Acheteur public/Autorité concédante fait l'objet d'un règlement amiable par la constitution d'un comité consultatif dédié.

Ledit comité consultatif est composé de membres qualifiés et habilités pour cette fonction, désignés au préalable, ou choisis conjointement.

Article 11 : États de l'art

11.1. Il appartient au Titulaire/Concessionnaire de se mettre en conformité avec les standards et référentiels qui concernent les services qu'il propose, utilise ou met à disposition.

À titre d'information, certains de ces référentiels sont publiés sur :
www.economie.gouv.fr/hfds/cybersecurite-et-politique-ministerielle-ssi

11.2. À première demande, le Titulaire/Concessionnaire fournit la conformité à ces référentiels pour les services et objets numériques inclus dans l'objet du présent contrat. Le Titulaire/Concessionnaire précise les domaines concernés (interfaces web et courriels), les objets et bases d'information concernées (appareils connectés, sauvegardes de données, consoles d'administration).

11.3. Constituent l'état de l'art pour les Interfaces web, les points suivants :

- Interfaces utilisables par des navigateurs à l'état de l'art (part de marché cumulée supérieure à 50%), sans générer d'alerte de sécurité.
- sans module d'extension.
- dans leur mode Grand public le plus protecteur (souvent appelé navigation Incognito).
- et en exploitant les techniques de protections associées.
- connexion TLS (https) pour authentifier la source et chiffrer les communications.
- marquage approprié des cookies ou jetons de session pour se protéger des vols ou exploitation de sessions déjà ouvertes.
- politique de sécurité des contenus pour se protéger contre les injections de contenus actifs malicieux.
- activation des protections des navigateurs par l'emploi d'entêtes de sécurité.
- Publication d'un point de contact via le fichier /.well-known/security.txt pour permettre des signalements directement auprès des bonnes équipes techniques.

Le présent résumé est sans préjudice du détail dudit référentiel accessible via le lien suivant : www.economie.gouv.fr/hfds/cybersecurite-et-politique-ministerielle-ssi

11.4. Constituent l'état de l'art pour les Services de courriels, les points suivants :

- Authenticité des émetteurs garantie par l'émission de messages depuis des serveurs associés publiquement aux domaines, signature numérique par domaine et une politique publique liant le tout.
- Identification claire du statut des comptes émetteurs de courriels, par exemple en ajoutant un suffixe à ceux fournis aux personnels qui ne sont pas agents ou salariés directs.
- Intégrité des messages par leur signature numérique.
- Confidentialité des échanges de machines en machines, confidentialité compatible avec les obligations d'interceptions légales.
- Analyse des rapports d'anomalies via DMARC ou abuse@.

Le présent résumé est sans préjudice du détail dudit référentiel accessible via le lien suivant : www.economie.gouv.fr/hfds/cybersecurite-et-politique-ministerielle-ssi

11.5. Constituent l'état de l'art pour les appareils connectés, les points suivants :

- Dispositif de lutte contre les logiciels malveillants (anti-virus, ou système de vérification et détection à base de signatures ou condensats des logiciels autorisés).
- Dispositif de mise à jour sécurisé.
- Limitation de l'exposition via les réseaux en réduisant les ports acceptant des connexions entrantes et en authentifiant les accès distants, sans faille connue (ceci exclut les connexions non chiffrées TELNET, HTTP/SMTP sans TLS, et l'emploi de mots de passe génériques ou faciles à découvrir, par exemple du fait d'un hachage insuffisant).

Le présent résumé est sans préjudice du détail dudit référentiel accessible via le lien suivant : www.economie.gouv.fr/hfds/cybersecurite-et-politique-ministerielle-ssi

11.6. Constitue l'état de l'art pour les sauvegardes des données stockées, les sauvegardes 3-2-1 (3 copies, 2 technologies, 1 exemplaire hors site principal, donc avec chiffrement) pour se protéger des rançongiciels, des erreurs de manipulations ou des défaillances de matériels.

Le présent résumé est sans préjudice du détail dudit référentiel accessible via le lien suivant : www.economie.gouv.fr/hfds/cybersecurite-et-politique-ministerielle-ssi

11.7. Constituent l'état de l'art pour l'administration des systèmes d'information, les points suivants :

- Consoles dédiées à l'exploitation et l'administration, et au minimum isolées des réseaux bureautiques et d'Internet, web et courriel notamment.
- Connexions aux machines administrées par des protocoles chiffrés, authentifiants et sans faille connue et bien configurés (VPN IPsec, TLS, ssh, RDP avec NLA).

Le présent résumé est sans préjudice du détail dudit référentiel accessible via le lien suivant : www.economie.gouv.fr/hfds/cybersecurite-et-politique-ministerielle-ssi

REMERCIEMENTS

Ce guide a été rédigé pour le compte de la Banque des Territoires en association avec Schéhérazade Abboub, Avocat associée chez Parme Avocats.

■ Banque des Territoires

Didier Célisse
Lucas Griffaton-Sonnet
Emmanuel Passilly
Mathieu Prot

■ Parme Avocats

Schéhérazade Abboub

PARME Avocats est un cabinet dédié aux projets des collectivités. Crée il y a plus de 20 ans, il regroupe 28 avocats, dont 8 associés, hautement qualifiés, disposant d'une expertise éprouvée et reconnue dans l'ensemble des champs d'intervention des collectivités. PARME Avocats se positionne en tant qu'acteur majeur dans de nouveaux domaines d'intervention tels que les données publiques et les villes intelligentes (Smart Cities).

BANQUE des TERRITOIRES

Caisse des Dépôts GROUPE

banquedesterritoires.fr

@BanqueDesTerr

Direction de la communication du groupe Caisse des Dépôts - Septembre 2020 - 20-211-BDT - Imprimerie Caisse des Dépôts